Interested in learning more about security?

SANS Institute InfoSec Reading Room

How Secure are the Root DNS Servers?

On October 21, 2002, the Internet was the target of a Distributed Denial of Service (DDoS) attack. The extent and scope of the impact has been the subject of several forums. Primarily, these discussions have centered on how vulnerable are the "venerable" root name servers that are at the top of the Internet hierarchy. This attack impacted 9 of the 13 root name servers. This paper is meant to provide the reader with insight into what the root server is and how the root name servers system operates; the threats to which ...

Global Information Assurance Certification

Security Essentials Practical

How Secure are the Root DNS Servers?

Version 1
Submitted by

Susan Baranowski

March, 2003

HOW SECURE ARE THE ROOT DNS SERVERS? 1

ABSTRACT 1

THE ROOT NAME SERVER SYSTEM 1

ROOT NAME SERVERS 1
THE ROLE OF THE ROOT NAME SERVER 1
THE ROOT ZONE FILE 2
ZONE TRANSFERS 3
DOMAIN NAME SYSTEM 3
Steps in the Root Name Server System Process *4*
CORE APPLICATION SOFTWARE ON THE ROOT SERVERS 5
Berkeley Internet Name Daemon (BIND) *5*
Network Time Protocol (NTP) *5*
Syslog *5*
Secured Shell (SSH) *5*
MANAGEMENT OF THE ROOT SERVERS AND DNS 6

WHAT ARE THE CONCERNS AND PROBLEMS (THREATS AND VULNERABILITIES)? 6

THE CURRENT PROTECTION METHODS – COUNTERMEASURES 8
Personnel Practices *8*
Physical Protection *8*
Hardware Redundancy *8*
Y2K Validation *9*
System Protection *9*
Root Name Servers *9*
Master Root Name Server "A" *9*
Root Zone File *9*
Core Application Software *10*
EMERGING COUNTERMEASURES 10
ICANN'S ACTIONS 10
DEFENSE IN DEPTH 10

SUMMARY: OCTOBER 21, 2003 11

WHAT THEY'RE SAYING: INDUSTRY COMMENTS 12

SUMMARY: EVALUATION 14

Confidentiality *14*
Integrity *14*
Availability *14*
Due Diligence *14*

DEFINITIONS 15

APPENDIX A ROOT NAME SERVER OPERATORS AND LOCATIONS 17

APPENDIX B STEPS IN THE ROOT NAME SERVER SYSTEM PROCESS 18

END NOTES 19

REFERENCES 20

How Secure are the Root DNS Servers?

Susan Baranowski
March 3, 2002

Abstract

On October 21, 2002, the Internet was the target of a Distributed Denial of Service (DDoS) attack. The extent and scope of the impact has been the subject of several forums. Primarily, these discussions have centered on how vulnerable are the "venerable" root name servers that are at the top of the Internet hierarchy. This attack impacted 9 of the 13 root name servers. This paper is meant to provide the reader with insight into what the root server is and how the root name servers system operates; the threats to which the root servers are vulnerable, what countermeasures have been implemented for protection; a summary of the October 21, 2002 incident; and industry analysis of the root name server system. This paper is intended as an overview for a general audience. References and links are provided for those who want more technical insight. The purpose is to provide the current state of the root name server system and its operation. The reader will be left to do a final evaluation of the confidentiality, availability and integrity strength of the root name servers and the root name server system.

The Root Name Server System

The overall operation of the root name server is referred to as the "The Root Name Server System" and is comprised of three major functions plus the core application software used in the operation:

- Root Name Servers
- Root Zone file
- Domain Name System (DNS) protocol
- Core Application Software

Root Name Servers

Root name servers exist to provide Internet Protocol (IP) addresses for the worldwide multitude of Internet users who traverse the global Internet. The root name server layer consists of a group of 13 domain name system (DNS) servers in operation throughout the world today, ten within the United States and three outside of the US. These root name servers, operated by a variety of government, commercial, research and educational organizations around the world, represent the top layer in the Internet Domain Name System (DNS) hierarchy. Due to protocol limitations, the number of these machines is currently limited to 13, although efforts are underway to remove this limitation.[1] The current 13 servers are named "A" through "M", a.root-servers.net – m.root-servers.net. A complete list of these root servers can be found in Appendix A.

The Role of the Root Name Server

Root name servers are the machines that provide access to IP addresses through the "root zone file" for proper navigation on the World Wide Web. At the top of the hierarchy of the 13 root name servers is the "A" root server, which generates a critical "root" zone file every 12 hours that tells the other 12 root name servers what Internet domains exist and where they can be found.[2]

This process was established in order for each root name server always to contain the same data. From the inception of the DNS, its fundamental design goal has been to provide a consistent name space that will be used for referring to resources. [3]

Just below the root name servers in the Internet hierarchy are those domain name servers that house the actual Internet domains, the top level DNS (tlDNS) name servers. The tlDNS include both the generic DNS (gDNS) and country code DNS (ccDNS) such as: .com, .net, .org, .biz, .info, .name, .edu .uk, etc. These tlDNS are the official databases for all web sites that register an official domain name on the Internet. The root name server and DNS system can be described as a distributed Internet directory service that provides information assistance. An analogy can be referring to a phone book that has both names and phone numbers. The root name server provides the phone number (IP address) for the domain word names (phone book name) and the tlDNS handles the translation between the domain names and these IP numeric addresses. Each of the root name servers maintains this list which allows a request to look up domain names in each of these top level DNS (tlDNS).

As this paper is focused on the root name server, a reader who is interested in learning more about the tlDNS and their operation can go to the following URL: http://www.icann.org/tlds/

The Root Zone File

Each root name server contains the same database divided into sections called zones. The zones represent how data is partitioned in the DNS hierarchy. These zones are distributed as root zone files among the tlDNS primary name servers. The primary and subsequently the secondary level DNS name servers are the repositories of these zone files that make up the overall domain database.

A root zone file:

- represents a section or zone of the overall Internet "domain" database and stores sub-domain information
- represents either a single organization or a whole domain within the DNS hierarchy or could be a group of domains
- is maintained on the primary tlDNS and secondary name servers that are now the "authority" for distribution within their zones.

Currently, the master root zone file, the authoritative list of the top-level domain registries and the master name servers for each, is maintained by Network Solutions Incorporated of Herndon, Virginia, US and is available publicly through the 12 secondary root servers "B – M" from the primary "A" root server.[4] This root zone file is made available to the other 12 root name servers in either of two ways:

- *In-band* via the DNS protocol itself through zone transfers as described in Request for Comments (RFC) 1034: **ftp://ftp.rfc-editor.org/in-notes/rfc1034.txt**
- *Out-of-band* via FTP as described in RFC 952: **ftp://ftp.rfc-editor.org/in-notes/rfc952.txt**

Zone Transfers

Given the relatively small size of the root zone, most updates of the root zone file are propagated via zone transfers.[5] The zone files are distributed to the tlDNS primary name servers. Then afterward, the other non-master or secondary servers for the zone periodically check for changes (at a selectable interval) and obtain new zone copies when changes have been made. [6] This is known as a "zone transfer". As part of standard system administration operating procedures, each DNS name server backs up a copy of its zone file for security and redundancy.

Domain Name System

The domain name system (DNS) is a distributed database arranged hierarchically with the root name servers at the top of the hierarchy and the tlDNS primary name servers and secondary level name servers below. A domain name server is said to be an authority for those sections or zones of the overall domain name space for which it has the complete information. The distribution of the root zone files in this hierarchy ensures, as shown in the previous section, that not all the information is in one place.

The actual combination of the second-level and top-level domain name server is what is commonly referred to as the domain name. Entities who wish to set up and manage a domain must select a top-level domain name system, tlDNS, to register with and create a unique second-level name. Then, they need to register this domain name with either the tlDNS directly or with a recognized authority, a registrar that oversees this tlDNS name space. In the example, www.sans.org, "sans" is the sub domain (second-level) and probably has its own domain name server. It has been registered to the tlDNS "org".

The distributed database can be put in perspective when one understands that a DNS server in a totally different part of the world can manage a separate level in the same domain name string. Take for example the URL "www.nokia.com". The sub domain "nokia" is probably managed on a DNS name server at the site of the company headquarters in Helsinki, Finland. The primary domain ".com" is managed by Verisign, Inc. which manages the tlDNS primary name servers in Herndon, VA.

For more information on the DNS, go to http://www.dns.net/dnsrd/ or to the RFC 1034 identified above.

DNS Protocol

Every time users submit a URL request they need the DNS protocol for their requests to find their destination on the Internet. The DNS protocol provides a service that does not depend on just one root name server for communication. The DNS protocol is the method that translates a URL request, the domain word string, into its corresponding IP address. As part of their zone file, each level of the DNS name server hierarchy has a listing of the names and IP addresses of all 13 of the Internet root servers. Each DNS server can therefore be configured to redirect requests to another root name server if the original root name server machine stops functioning.

It is important to understand that most Internet traffic is in fact handled by the primary and secondary domain name servers that cache frequently requested URL addresses and eliminate the need to query the root name servers. DNS servers and ISP providers have made it easy to retain this IP address information for repeated and continued use through the use of "caching" for a specified amount of time. ISP providers also retain this information for individual users who "bookmark" URL addresses.

Steps in the Root Name Server System Process

The root name server acts like a "facilitator" or "traffic cop" at the top of the hierarchy by keeping track of URL requests and directing them to their destinations. The root name server routes a request from the DNS name servers and their subsequent lower level DNS name servers in the hierarchy to the corresponding master tlDNS primary name server when they receive a request.

The following table describes the steps that a request for a common URL address uses when it takes the Internet superhighway to a web site. When the browser tries to reach a site such as www.sans.org it may or may not need to eventually ask the root name server at the top of the hierarchy to locate the IP address.

Step	Action	What is happening
1	A user types in the URL request.	The PC must find the IP address for the hostname: www.sans.org
2	The web browser sends this request to the "**Resolver**" which is a computer program/process that runs in the background of any PC connected to the Internet.	The **Resolver's** task is to provide domain name resolution. It checks its internal host tables for stored or cached IP addresses. If the URL requested is available it returns this to the user. If not, it goes on to **Step 3**.
3	The **Resolver** checks its configuration for the IP address of the local DNS name server to send the query to.	This request is made to the DNS server at the company site or ISP. It also has another name in the Internet world: **Recursive** server. If this DNS **Recursive** server cannot resolve and return the response to the **Resolver**, (because it does not have it in its file or cache), it proceeds to **Step 4**.
4	The DNS **Recursive** server sends its query to the root name server.	The DNS **Recursive** servers have a file containing a list of the 13 Internet root name servers and use this file to direct the query.

Step	Action	What is happening
5	The root name server tells the DNS **Recursive** servers where to go for more information.	The root name server provides a "referral" to the **Recursive** server query for the tlDNS **Authoritative** named servers needed to answer the request. For example, if an "***.org***" URL is requested, the root server sends the request to the DNS **Authoritative** server for ***org.***
6	The **Recursive** server queries the **Authoritative** servers directly and asks about their full IP address request.	The **Authoritative** server checks its registries and returns the domain name response to the **Recursive** server.
7	The **Recursive** server returns the request to the **Resolver**.	The **Recursive** server, usually the local DNS name server, caches the domain address information when it returns the query.
8	The **Resolver** has the information it needs and sends the IP address to the Internet and establishes a connection.	The user is connected to www.sans.org. *Think of this process the next time you put in an unknown URL request – simple enough?*

Primary source courtesy of: http://support.dyndns.org/support/kb/

Note: At each step of the process, the answers being received about the URL request are cached in all the DNS name servers for a specified time.

Readers who would like to see these steps visually can refer to a diagram of this process in Appendix B.

Core Application Software on the Root Servers

The root name servers utilize the following software: [7]

Berkeley Internet Name Daemon (BIND)

This software handles the context of root name service. It is the most common DNS software of the Internet. Ported to every platform of Unix and Windows NT, the BIND source code is maintained by the Internet Software Consortium.

Network Time Protocol (NTP)

Provides clock synchronization, insuring machine clocks are quite closely aligned with standard time sources. (*Note: BIND makes no use of the system clock itself*.)

Syslog

Used to log system messages thus *no direct impact* would be made on name server operation.

Secured Shell (SSH)

Provides remote access to the root name server. Failure of this application simply means remote access to the root name server is impacted; there is *no impact* on the operation of the name server software itself.

Management of the Root Servers and DNS

The Internet Corporation for Assigned Names and Numbers (ICANN) was created in 1998, to assume the following key responsibilities from the Internet Assigned Numbers Authority (IANA). The mission of ICANN is to coordinate the stable operation of the Internet's unique identifier systems. In particular, ICANN coordinates the: [8]

- allocation and assignment of three sets of unique identifiers for the Internet:
    - domain names (forming a system referred to as "DNS");
    - Internet protocol (IP) addresses and autonomous system (AS) numbers; and
    - protocol port and parameter numbers.
- operation and evolution of the DNS's root name server system.

What are the Concerns and Problems (Threats and Vulnerabilities)?

A reality of today's global environment is that most Internet services are dependent on the DNS to operate. If the DNS experiences failure, users are not able to complete URL requests or send email. Since the DNS was designed with one master database, this could potentially represent a single point of failure. An analysis of the more common concerns and problems is listed below. Links are provided for readers who would like to obtain further information:

- It would be possible to change where the root servers are simply by having the relatively small group of people who control who can change routing tables set up new routes, so that those queries go to new servers.

  http://www.templetons.com/brad/dns/howworks.html

- If terrorists were to direct a worm to attack root name servers, they could make the Internet inaccessible to the average person, who would have to know the numerical address IP address rather than an easy-to-remember name, www.sans.org in order to reach a Web site. (Unless the local DNS already has this in the file or has cached the IP address).

  http://www.washingtonpost.com/ac2/wp-dyn?pagename=article&node=&contentId=A38036-2001Sep27&notFound=true

- In information security, one of the things that that has been acknowledged about the Internet is that diversity improves the resistance of the overall system. "The number of machines that are DNS roots servers and tlDNS servers is relatively small and predictable." http://www.cavebear.com/rw/steps-to-protect-dns.htm

- There is not a great deal of software diversity at the upper layers of the DNS - to a large degree the same software is used: BIND running on Unix. This means that many of these servers may be vulnerable to the same kind of attack. http://www.cavebear.com/rw/steps-to-protect-dns.htm

- The root server system can also be vulnerable to DDoS (distributed denial of service) attacks and related software-based threats. In a recent address to ICANN, the following statement was made "Protection against DDoS attacks is problematic under current network architectures, requiring a shift in focus to detection and rapid recovery." http://www.icann.org/committees/security/dns-security-update-1.htm

- Concern over root name server security led to an Internet Engineering Task Force best-practices memo last year, which stressed that physical and electronic security must be paramount. A malcontent who breached a root server could spoof domain names, forge websites and disrupt the Internet for millions of people. http://www.names4ever.com/services/domain-news-11-13-01.html

The following table presents a summary of some of the commonly recognized threats and vulnerabilities that face the root server name system:

Threat	Vulnerability	Type of Attacks
Confidentiality	• Administration and operator error; misconfigurations • Authentication and non-repudiation	• Unauthorized access • Elevation of privilege
Integrity	• Corruption of key address lists in the root zone file	• Unauthorized access • Elevation of privilege

Threat	Vulnerability	Type of Attacks
Availability	Network and Host System: • Misconfigurations • Intrusions Physical: • Power grid failures, • Telecom infrastructure failure • Cooling system failures	• Distributed Denial of Service (DDoS) • Spoofing • Unauthenticated zone transfers • ICMP Packets • Man-made or natural disasters

The Current Protection Methods – Countermeasures

A conscious effort has been made to diversify the administration of the 13 machines in several areas: diverse organizations, locations, types of operators, operating environments, etc. Diversity provides one level of protection making it more difficult to attack all thirteen roots servers with a uniform approach. [9]

Personnel Practices

Beyond the software and hardware, the operators of the 13 authoritative root name servers mirror the diversity of the system itself, bringing different personalities and different organizational settings to the mix. Nevertheless, they have developed a strong social network of trust, and make use of well-established encrypted communication channels to share information. Each root name server operator has multi-level system administration personnel and support with internally defined escalation procedures.[10]

Additionally, should disruption occur, a summary of the standard set of procedures for the operation of the root name server is further defined in RFC 2870.

Procedurally, the root name server operators have all taken steps to minimize susceptibility to disruption, and to enable rapid detection and recovery. Each root name server site: [11]

- keeps backup copies of zone files, thus should a disruption occur in the generation or transmission of the root zone file, the root servers can make use of backup copies until the situation is resolved.
- has contact information (in hard copy) for all other operators, thus should an issue be detected, the root name server operators can get in contact with each other.

Physical Protection

Hardware Redundancy

The specification for root name server performance detailed in RFC 2870 specifies that the root name servers have physical security "in a manner expected of data centers critical to a major enterprise."

Each root name server has redundant hardware available to it. The hardware is in the form of either a: [12]

- *Hot spare*—able to be made operational with human intervention.
- *Live spare*—able to take on the full load of serving the root zone without human intervention should there be a hardware failure.

All 13 root name servers have some "hardening" with respect to environmental contingencies. This hardening includes: [13]

- The use of controlled physical access, protection against power grid and cooling failures with UPS protected power with local generator capacity for extended outages.
- Diverse Internet connectivity in three levels: Physical, Data Link, Network

Y2K Validation

The root name servers underwent a comprehensive evaluation for Y2K sustainability, and it was established that all the root name servers would not encounter significant events on January 1, 2000. The full review can be obtained at URL: http://www.icann.org/committees/dns-root/y2k-statement.htm

System Protection

Root Name Servers

All of the root name servers use some variant of the Unix operating system, however both the hardware base and the vendors' Unix variants are relatively diverse: of the 13 root servers, there are seven different hardware platforms running eight different operating system versions from five different vendors. [14]

It has been estimated, that, with the amount of traffic each individual root name server receives, root name service can function with little or no disruption when 40% of the name servers are offline, thus should a significant catastrophe or attack occur, the diversity of location will permit the root name server system to continue operation while the disrupted name servers are restored. [15]

Master Root Name Server "A"

The Master Root "A", as previously stated, is managed by Verisign's Network Solutions and, at the top of the Internet hierarchy, it is the most valuable name server in the DNS. The following security precautions have been taken to safeguard this server: [16]

- biometric-verified access to server rooms
- backup power supplies, redundancy
- different types of hardware and software
- multiple Internet links

Root Zone File

Once generated, the master zone file is replicated to a disaster recovery site, with backups stored at off-site locations. Changes to the zone file are subjected to an elaborate system of review and verification, including human scrutiny of the file before it is published.[17] The change control of this file is held by the Internet Assigned Numbers Authority (IANA).

Core Application Software

The root DNS name servers have implemented BIND, version 8 or higher. BIND v9 is the most recent version and has incorporated stronger functionality to further security. As the root name servers run recent versions of BIND, the 13 operators are able to share experience and troubleshooting tips.[18]

Emerging Countermeasures

With the guidance of IETF, the organizations that operate the root name servers have started working on the following security enhancements:

- The use of a dedicated primary server for distribution of zone file updates.
- A set of security-enhancing tools, known collectively as DNS security (DNSSEC). DNSSEC essentially uses public key cryptography techniques to verify the validity of DNS data. In other words, DNSSEC is a mechanism to assure the authenticity and integrity of DNS data. DNSSEC facilitates a chain of trust that starts with the root name servers and proceeds through the hierarchical resolution of a domain name. At each level in the DNS, the signature of the upper level zone is verified using an associated public encryption key. [19]

ICANN's Actions

The Security and Stability Advisory Committee was formed by ICANN in 2002 following the ICANN meeting in November 2001 that focused on DNS security.

In light of recent attack, the Committee has focused on:

- Analysis of the October 2002 Distributed Denial of Service Attacks.
- Making recommendations for addressing operational procedures.

Full details can be obtained on: http://www.icann.org/committees/dns-root/

As a result of the ICANN meeting in January, 2003, the Security Committee is tasked to coordinate these following assessments across the internet community: [20]

1. Perform a comprehensive *threat/risk analysis*
2. Establish an on-going *audit* capability to assess protection, detection and recovery capabilities.
3. Include assessments of the *length of time* that it is acceptable for particular services to be unavailable.

Defense in Depth

A basic principle of security protection, defense in depth (DiD), asserts that at every point on the Internet superhighway where there is transmission, processing or storage of data there is room for a security breach. Organizations at every level of the DNS should be taking precautions to maintain confidentiality, integrity and availability of data.

"The Internet does not run on root name servers alone…ensuring the safety and stability of the Internet depends on every member of the Internet community, business, individuals, and governments, all fulfilling their respective duties on the global, regional, and national levels."[21]

Summary: October 21, 2003

Type of Attack: Distributed Denial of Service

Attack Method: The attack, over a period of one hour, was done via Internet control message protocol (ICMP) requests to the root servers. These requests were high-volume and high frequency ICMP data packets sent to the root name servers. The term for this is ”ping-flooding”.

Impact: Nine of the 13 servers were impacted.

Mitigation: ICMP data is not essential to network administration and many servers, and the routers that direct data to its destination, tend to block the protocol. That is precisely what administrators did during the recent attack to stop the flood of data from reaching the DNS root servers. Indeed, October's attack may not have been as serious as previously claimed.[22]

What They're Saying: Industry Comments

The statements below were collected to provide the reader with a broad view of what the industry has stated about the security of the root name server system and the overall DNS, especially in light of the October, 2002 DDoS attack:

> "The root servers, dispersed throughout the world, are key way stations in the routing of Internet messages and other traffic. The Internet was designed so that no single point of failure could cripple the whole system. While half of the root servers are located in the United States, buildings that once served as Internet hubs are no longer located in a few central places."
>
> Marc Maiffret, eEye Digital Security, Viejo, CA Washington Post, September 28, 2001 http://www.washingtonpost.com/ac2/wp-dyn?pagename=article&node=&contentId=A38036-2001Sep27&notFound=true

> "We ought to consider whether it is prudent to maintain this degree of homogeneity or whether we should require that every DNS zone be served by multiplicity of implementations on a diverse set of platforms. This is not unlike the long established requirement of geographic diversity between servers."
>
> Karl Auerbach, October 14, 2001 http://www.cavebear.com/rw/steps-to-protect-dns.htm

> "The stability of the Internet, its resilience against attack, and its ability to recover after a catastrophe, would be vastly improved if the DNS were to have the redundancy offered by multiple roots."
>
> Karl Auerbach, Cisco Engineer, ICANN Board, 2000, Wired News, November 13, 2001 http://www.names4ever.com/services/domain-news-11-13-01.html

> The CERT Coordination Center, which tracks internet vulnerabilities for the US government, warned June 28 that a flaw in DNS resolver libraries (the code that handles the transformation of domain names into IP addresses) in multiple Unix applications were susceptible to a buffer overflow attack. Computer Wire, May 9, 2002 http://www.theregister.co.uk/content/archive/26967.html

> "The only way to stop such attacks is to fix the vulnerabilities on the machines that ultimately get taken over and used to launch them. There's no defense once the machines are under the attacker's control."
>
> Alan Paller, Sans Institute, Washington Post, October 22, 2002
>
> http://www.washingtonpost.com/ac2/wp-dyn/A828-2002Oct22?language=printer

> "Government could improve security of the infrastructure by requiring that the service providers with whom it does business filter out spoofed IP addresses. Server operators mitigated the effect by disabling response to ICMP echo traffic."
>
> John Pescatore, Gartner Inc.,Stamford, Conn, Government Computer News, 11/4/02 http://www.gcn.com/21_32/web/20404-1.html

"Regardless of the success of the attack, bringing down the root servers would not result in a shutdown of the Net as we know it…the software that runs the root servers likely has flaws that could be exploited by attackers. But "the sky is not falling." The importance of the root servers has been overstated, Fred Cohn said, arguing that their core functions could be rebuilt within hours. This attack shows that it's possible to wreak havoc among a few hundred technical people who have to batten down the hatches...But there have been no serious negative consequences."

Fred Cohn, University of New Haven, CNET News.com, November 7, 2002

http://news.com.com/2100-1023-964978.html?tag=m

"One of the things that we have learned from the viruses and worms that have plagued our existence on the Internet is that diversity improves the resistance of the overall system. However, we do not have a great deal of software diversity at the upper layers of the Domain Name System- to a very large degree the same software is used: BIND running on Unix (including BSD and Linux derivatives). This means that many of these servers may be vulnerable to the same kind of attack."

Karl Auerbach, October 14, 2001,

http://www.cavebear.com/rw/steps-to-protect-dns.htm

The distributed and redundant nature of the root server system makes it less vulnerable to physical attack than, say, the public switched telephone communications system that has to protect numerous single points of failure.

ICANN Meeting, Presentation, November, 2001
http://www.icann.org/committees/security/dns-security-update-1.htm

A spokesman for UUNET, which is the service provider for two of the root servers, told internetnews.com it was the "largest, most targeted attack" ever seen. "This did not affect the end user but it was huge and concerted. It was rare because it was aimed at all 13 servers. It was an attack on the Internet itself and not a particular Web site or service provider," he explained.

http://boston.internet.com/news/article.php/1486981

In a set of presentations to the community at the November 2001 ICANN meeting, operators of the DNS root name servers stressed that the distributed architecture of the system was designed to be robust in the face of disaster or malicious attack. "ICANN cannot solve 'the' whole Internet security problem – and it shouldn't try to. It can – and should – promote protection of the name and number services upon which the Internet relies."

http://www.icann.org/committees/security/dns-security-update-1.htm

Summary: Evaluation

How secure is the Root Server Name System?

Prior to evaluating the security of the root server, the reader should consider the foundation of information assurance and apply it to the root name server system process. Security measures should consider these basic fundamentals:

Confidentiality

Confidentiality provides assurance that information is shared only among authorized persons or organizations. Breaches of confidentiality occur when data is not handled in a manner adequate enough to safeguard the confidentiality of the information concerned.

Integrity

The integrity of data is not only whether the data is "correct", but whether it can be trusted and relied upon. Assurance is needed that the information is authentic and complete. Security measures must be taken to ensure that the data cannot be corrupted or lost. The data should be in its original state and not altered.

Availability

Availability provides assurance that the systems responsible for delivering, storing and processing information are accessible when needed, by those who need them. Security measures must be taken to ensure that the data is available at all times.

Due Diligence

Due diligence provides the assurance that security is an ongoing process. There is a need for constant and continued vigilance.

Definitions

Term	Definition
Authoritative	Adjective describing a domain name server (DNS) or a response from a name server that is referencing its own domain data, the zone file. The authoritative server contains an entire copy of the zone that is derived from local configuration data, possibly with the help of another authoritative name server for the zone. Data on its domains is obtained without the need for caches or the help of any resolver.
Cache; Caching	A cache (pronounced CASH) is a place to store something temporarily. The files you automatically request by looking at a Web page are stored on your hard disk in a cache subdirectory under the directory for your browser (for example, Internet Explorer). When you return to a page you've recently looked at, the browser can get it from the cache rather than the original server, saving you time and the network the burden of some additional traffic. You can usually vary the size of your cache, depending on your particular browser. The act of recording authoritative response to resolver queries for future reference. Generally cached records will be purged after a predetermined time.
Denial of Service (DoS)	On the Internet, a denial of service (DoS) attack is an incident in which a user or organization is deprived of the services of a resource they would normally expect to have. Typically, the loss of service is the inability of a particular network service, such as e-mail, to be available or the temporary loss of all network connectivity and services
Distributed Denial of Service (DDoS)	On the Internet, a distributed denial-of-service (DDoS) attack is one in which a multitude of compromised systems attack a single target, thereby causing denial of service for users of the targeted system. The flood of incoming messages to the target system essentially forces it to shut down, thereby denying service to the system to legitimate users.
DNS	The Domain Name System (DNS) is the distributed database of the Internet which contains a mapping of domain names to IP addresses and vice versa. The database is distributed because each domain can be administered by a different organization.
DNS Name Servers	DNS name servers maintain mappings of domain names to IP addresses (and vice versa) and answer queries including, but not limited to "What is the IP address associated with this particular domain name?", and "What is the domain name associated with this particular IP address?". DNS name servers themselves also use resolvers to ask other DNS name servers questions to which they don't know the answers themselves.
DNSSEC	DNS Security (or DNSSEC) applies cryptography to the Domain Name System to authenticate the information served.
Domain Name	A unique designator on the Internet made up of symbols separated by dots, such as www.sans.org.
Elevation of Privilege	The ability of a user to gain unauthorized privileges on a machine or network. An example of privilege elevation would be an unprivileged user who could contrive a way to be added to the Administrator's group.
ICMP packets	ICMP packets carry network data used for reporting errors or checking network connectivity, as in the case of the common "ping" packet. A flood of such data can block access to servers by clogging bottlenecks in the network infrastructure, thus preventing legitimate data from reaching its destination. However, ICMP data is not essential to network administration, and many servers, and the routers that direct data to its destination, tend to block the protocol.

Term	Definition
Internet Protocol	The Internet Protocol (IP) is the method or protocol by which data is sent from one computer to another on the Internet. Each computer (known as a host) on the Internet has at least one IP address that uniquely identifies it from all other computers on the Internet.
ICANN	The Internet Corporation for Assigned Names and Numbers (ICANN) is the global non-profit organization responsible for coordinating the Internet's core systems of unique identifiers, most notably the Domain Name System (DNS).
IP Address	A unique identifier number that is provided for any host on any TCP/IP network, including the Internet.
Protocol	In information technology, a protocol is the special set of rules that end points in a telecommunication connection use when they communicate. Protocols exist at several levels in a telecommunication connection.
Resolver	The physical structure of the DNS consists of resolver programs. The task of the DNS Resolver client program is to create queries and send them to a DNS name server for resolution. A resolver is capable of performing a recursive search of the Domain Name System to locate records that would answer a query. It does this by querying domain name servers, including the root name servers.
Recursive	A recursive query is a request from a host to a resolver to find data on other name servers.
Root Zone	The ancestor of all zones and is the parent of the top level domains. It is written as ". ". Root (as it is often called) has no labels.
Root Zone File	A root zone file is a section of the domain name system with the data necessary for resolving specified Internet domain names to the appropriate number form of an Internet Protocol (IP) address. The root zone file usually resides on the DNS name servers that administer a site.
Spoof; Spoofing	The basic purpose of spoofing is to confuse a DNS name server into giving out bad information. For example, to fake an Internet address so that one looks like a certain kind of Internet user. IP spoofing, for example, involves trickery that makes a message appear as if it came from an authorized IP address. A remote user can send specially crafted DNS packets to a target DNS server to inject false domain name information into a DNS cache.
Top Level Domain	On the Internet, a top-level domain (TLD) identifies the most general part of the domain name in an Internet address. A TLD is either a generic top-level domain (gTLD), such as “com” for "commercial, “edu” for "educational," and so forth, or a country code top-level domain (ccTLD), such as "fr" for France or "is" for Iceland.
Unauthenticated Zone Transfers	A remote attacker can use malicious zone transfers to crash vulnerable BIND servers, resulting in a denial-of-service condition that disables name resolution service.
Zone Transfers	Zone transfers are the method of the root name server hierarchy to distribute the root zone file to primary and secondary domains. Secondary name servers update their own zone data from its primary server most often use zone transfers.

Sources:

http://whatis.techtarget.com/

http://www.techweb.com/encyclopedia/

http://www.menandmice.com/online_docs_and_faq/glossary/glossarytoc.htm?resolver.htm

Appendix A Root Name Server Operators and Locations

Server	Operator	Cities	IP Address	URL
A	VeriSign Global Registry Services	Herndon VA, US	198.41.0.4	www.verisign-grs.com
B	Information Sciences Institute	Marina Del Rey CA, US	128.9.0.107	http://www.isi.edu
C	Cogent Communications	Herndon VA, US	192.33.4.12	http://www.psi.net
D	University of Maryland	College Park MD, US	128.8.10.90	http://www.umd.edu
E	NASA Ames Research Center	Mountain View CA, US	192.203.230.10	http://www.nasa.gov
F	Internet Software Consortium	Palo Alto CA, US; San Francisco CA, US	IPv4: 192.5.5.241 IPv6: 2001:500::1035	http://www.isc.org
G	U.S. DOD Network Information Center	Vienna VA, US	192.112.36.4	http://nic.mil
H	U.S. Army Research Lab	Aberdeen MD, US	IPv4: 128.63.2.53 IPv6: 2001:500:1::803f:235	http://www.arl.mil
I	Autonomica	Stockholm, SE	192.36.148.17	http://www.nordu.net
J	VeriSign Global Registry Services	Herndon VA, US	192.58.128.30	N/A
K	Reseaux IP Europeens - Network Coordination Centre	London, UK	193.0.14.129	http://www.ripe.net
L	Internet Corporation for Assigned Names and Numbers	Los Angeles CA, US	198.32.64.12	N/A
M	WIDE Project	Tokyo, JP	202.12.27.33	http://www.wide.ad.jp

Sources:

http://root-servers.org/
http://www.icann.org/committees/dns-root/y2k-statement.htm

Appendix B Steps in the Root Name Server System Process

End Notes

1. Conrad, Kato, Manning.
2. McGuire and Krebs.
3. P. Mockapetris.
4. Conrad, Kato, and Manning.
5. Ibid.
6. P. Mockapetris.
7. Conrad, Kato, and Manning.
8. ICANN. Committee on ICANN Evolution and Reform.
9. ICANN. ICANN DNS Security Update #1.
10. Ibid.
11. Conrad, Kato, and Manning
12. ICANN, ICANN DNS Security Update #1.
13. Conrad, Kato, and Manning
14. ICANN, ICANN DNS Security Update #1.
15. Ibid.
16. Declan McCullagh.
17. ICANN, ICANN DNS Security Update #1.
18. Conrad, Kato, and Manning
19. ICANN, ICANN DNS Security Update #1
20. Ibid.
21. Ibid.
22. Evan Hansen.

References

1. Auerbach, Karl. “Protecting the Internet's Domain Name System.” October 14, 2001. URL http://www.cavebear.com/rw/steps-to-protect-dns.htm (January 25, 2003).

2. Brenton, Chris with Cameron Hung. Active Defense: A Comprehensive Guide to Network Security. San Francisco: Sybex Inc, 2001.88 - 92.

3. Bush, R., D. Karrenberg, M. Kosters, R. Plzak. “Root Name Server Operational Requirements.” Request for Comments: 2870. June, 2000. URL http://www.rfc-editor.org/rfc/rfc2870.txt (January 11, 2003).

4. The Business Technology Network. “TechEncyclopedia.” The Computer Language Company. 2003. URL http://www.techweb.com/encyclopedia/ (February 1, 2003).

5. Crothers, Tim. Internet Lockdown: Internet Security Administrator’s Handbook. New York: Hungry Minds, Inc., 2001. 17-21; 159-160.

6. Computer Wire. “DNS vulnerability critical’.” The Register. May 9, 2002. URL http://www.theregister.co.uk/content/archive/26967.html (February 1, 2003).

7. Conrad, David, Akira Kato, and Bill Manning. “Root Nameserver Year 2000 Status.” July 15, 1999. URL http://www.icann.org/committees/dns-root/y2k-statement.htm (January 11, 2003).

8. Dynamic DNS Network Services, LLC. “Anatomy of a DNS Query: How DNS Works”. 2003. URL http://www.dyndns.org/support/kb/ (February 1, 2003).

9. ElBoghdady, Dina. “Internet Vulnerable to Terrorists, Experts Warn.” Washingtonpost.com. Friday, September 28, 2001. URL http://www.washingtonpost.com/ac2/wp-dyn?pagename=article&node=&contentId=A38036-2001Sep27&notFound=true (January 11, 2003).

10. Feinler, E., K. Harrenstien, M. Stahl. “DOD Internet Host Table Specification.” October, 1985. FTP ftp://ftp.rfc-editor.org/in-notes/rfc952.txt (February 1, 2003).

11. Hansen, Evan. “Key Internet server moved for security.” Cnet News.com. November 7, 2002. URL http://news.com.com/2100-1023-964978.html?tag=m (January 4, 2003).

12. IANA. “Internet Assigned Numbers Authority.” December 30, 2002. URL http://www.iana.org/ (January 25, 2003).

13. ICANN, Committee on ICANN Evolution and Reform. “Working Paper on ICANN Mission and Core Value.” May 6, 2002. URL http://www.icann.org/committees/evol-reform/working-paper-mission-06may02.htm (January 11, 2003).

14. ICANN. “DNS Root Server System Advisory Committee.” November 15, 2002. URL http://www.icann.org/committees/dns-root/ (January 4, 2001).

15. ICANN. “ICANN DNS Security Update #1.” January 4, 2002. URL http://www.icann.org/committees/security/dns-security-update-1.htm (January 25, 2003).

16. ICANN. “The Internet Corporation for Assigned Names and Numbers.” URL
17. http://www.icann.org/ (January 4, 2003).

18. ICANN. “Security and Stability Advisory Committee”. URL http://www.icann.org/committees/security/ (January 25, 2003).

19. ICANN. “Top Level Domains.” URL http://www.icann.org/tlds/ (January 11, 2003).

20. Jackson, William. “DNS attacks could be a warning shot.” November 4, 2002. Government Computer News, Vol. 21 No. 32. URL http://www.gcn.com/21_32/web/20404-1.html (January 11, 2003).

21. Krebs, Brian and David McGuire. “Attack On Internet Called Largest Ever.” October 22, 2002. Washingtonpost.com URL http://www.washingtonpost.com/ac2/wp-dyn/A828-2002Oct22?language=printer (January 11, 2003).

22. McCullagh, Declan. “ICANN: To Serve and Protect.” Wired News. November 13, 2001. URL http://www.names4ever.com/services/domain-news-11-13-01.html (January 25, 2003).

23. McGuire, David and Brian Krebs. "Attack on Internet Called Largest Ever." Washingtonpost.com. October 22, 2002. URL http://www.washingtonpost.com/ac2/wp-dyn/A828-2002Oct22?language=printer (January 4, 2003).

24. Men&Mice. “Making DNS Easy.” 2002. URL http://www.menandmice.com/online_docs_and_faq/glossary/glossarytoc.htm?resolver.htm (February 8, 2003).

25. Mockapetris, P. “Domain Names – Concepts and Facilities.” Request for Comments: 1034. November 1987. FTP ftp://ftp.rfc-editor.org/in-notes/rfc1034.txt (February 1, 2003).

26. Naraine, Ryan. “Massive DdoS Attack Hit DNS Root Servers.” October 23, 2002. URL http://boston.internet.com/news/article.php/1486981 (January 11, 2003).

27. Root Servers Technical Operations Association. URL http://root-servers.org/ (January 4, 2003.)

28. Salamon, András. “DNS Resources Directory”. 2001. URL http://www.dns.net/dnsrd/ (February 1, 2003)

29. Templeton, Brad. “How DNS Works.” Electronic Frontier Foundation. URL http://www.templetons.com/brad/dns/howworks.html (January 25, 2003).

30. Whatis.com. “Definitions for thousands of the most current IT-related words.” URL http://whatis.techtarget.com/ (January 25, 2003).

Last Updated: December 13th, 2017

Upcoming SANS Training

Click Here for a full list of all Upcoming SANS Events by Location

SANS Security East 2018	New Orleans, LAUS	Jan 08, 2018 - Jan 13, 2018	Live Event
SANS Amsterdam January 2018	Amsterdam, NL	Jan 15, 2018 - Jan 20, 2018	Live Event
Northern VA Winter - Reston 2018	Reston, VAUS	Jan 15, 2018 - Jan 20, 2018	Live Event
SEC599: Defeat Advanced Adversaries	San Francisco, CAUS	Jan 15, 2018 - Jan 20, 2018	Live Event
SANS Dubai 2018	Dubai, AE	Jan 27, 2018 - Feb 01, 2018	Live Event
SANS Las Vegas 2018	Las Vegas, NVUS	Jan 28, 2018 - Feb 02, 2018	Live Event
Cyber Threat Intelligence Summit & Training 2018	Bethesda, MDUS	Jan 29, 2018 - Feb 05, 2018	Live Event
SANS Miami 2018	Miami, FLUS	Jan 29, 2018 - Feb 03, 2018	Live Event
SANS Scottsdale 2018	Scottsdale, AZUS	Feb 05, 2018 - Feb 10, 2018	Live Event
SANS London February 2018	London, GB	Feb 05, 2018 - Feb 10, 2018	Live Event
SANS Southern California- Anaheim 2018	Anaheim, CAUS	Feb 12, 2018 - Feb 17, 2018	Live Event
SANS Secure India 2018	Bangalore, IN	Feb 12, 2018 - Feb 17, 2018	Live Event
SANS Dallas 2018	Dallas, TXUS	Feb 19, 2018 - Feb 24, 2018	Live Event
SANS Brussels February 2018	Brussels, BE	Feb 19, 2018 - Feb 24, 2018	Live Event
SANS Secure Japan 2018	Tokyo, JP	Feb 19, 2018 - Mar 03, 2018	Live Event
Cloud Security Summit & Training 2018	San Diego, CAUS	Feb 19, 2018 - Feb 26, 2018	Live Event
SANS New York City Winter 2018	New York, NYUS	Feb 26, 2018 - Mar 03, 2018	Live Event
CyberThreat Summit 2018	London, GB	Feb 27, 2018 - Feb 28, 2018	Live Event
SANS London March 2018	London, GB	Mar 05, 2018 - Mar 10, 2018	Live Event
SANS San Francisco Spring 2018	San Francisco, CAUS	Mar 12, 2018 - Mar 17, 2018	Live Event
SANS Secure Osaka 2018	Osaka, JP	Mar 12, 2018 - Mar 17, 2018	Live Event
SANS Secure Singapore 2018	Singapore, SG	Mar 12, 2018 - Mar 24, 2018	Live Event
SANS Paris March 2018	Paris, FR	Mar 12, 2018 - Mar 17, 2018	Live Event
SANS SEC460: Enterprise Threat Beta	OnlineCAUS	Jan 08, 2018 - Jan 13, 2018	Live Event
SANS OnDemand	Books & MP3s OnlyUS	Anytime	Self Paced