June 2006

INFORMATION TECHNOLOGY LABORATORY

Bulletin

ADVISING USERS ON INFORMATION TECHNOLOGY

DOMAIN NAME SYSTEM (DNS) SERVICES: NIST RECOMMENDATIONS FOR SECURE DEPLOYMENT

Shirley Radack, Editor
Computer Security Division
Information Technology Laboratory
National Institute of Standards and Technology

Domain Name System (DNS) services have an important function in helping users readily access the many resources that are available through the Internet. DNS services make communications convenient for the user by translating the unique resource identifier that is known as the Internet Protocol (IP) address into a domain name that is easy for the user to remember. The IP address to which a user wishes to be connected is represented by four groups of numbers separated by dots, such as123.67.43.254. The computers in the network route communication packets across the Internet based on the IP addresses of the packets. However, when accessing websites and using e-mail services, the user can simply employ a domain name such as *nist.gov*, which is easier to remember than the full IP address. The DNS transforms human-readable domain names into machine-readable IP addresses and also does the reverse process, taking a query with an IP address and returning the domain name associated with it.

The DNS infrastructure, which carries out the domain name translation, is made up of computing and communication entities that are geographically distributed throughout the world. There are more than 250 top-level domains, such as *.gov* and *.com*, and several million second-level domains, such as *nist.gov* and *ietf.org*. As a result, there are many name servers in the DNS infrastructure that contain information about only a small portion of the domain name space. The different servers work together to provide DNS services. The domain name data provided by DNS is intended to be publicly available to any computer located anywhere in the Internet.

While DNS services are not the primary target of most attacks on information systems today, the DNS infrastructure is expected to become more vulnerable as more applications use DNS for network operations. NIST's Information Technology Laboratory (ITL) has developed guidance to help organizations protect their DNS components, prevent possible future attacks on domain name information, and maintain the availability of DNS services and data.

NIST Special Publication (SP) 800-81, *Secure Domain Name System (DNS) Deployment Guide*

NIST SP 800-81, *Secure Domain Name System (DNS) Deployment Guide*, presents NIST's recommendations to help organizations analyze their operating environments and the threats to their DNS services, and to apply appropriate risk-based security measures for all DNS components. Written by ITL's Ramaswamy Chandramouli and Scott Rose, the publication provides guidelines for the secure deployment of each DNS component through the use of configuration options and checklists that are based on policies or best practices. Development and publication of the guide were carried out in collaboration with the Department of Homeland Security (DHS).

NIST SP 800-81 explains the structure and operations of DNS data, software, and transactions and discusses the threats, the security objectives, and the security approaches that can be employed. Extensive guidance is provided on maintaining data integrity and performing source authentication, and on configuring DNS deployments to protect the

ITL Bulletins are published by the Information Technology Laboratory (ITL) of the National Institute of Standards and Technology (NIST). Each bulletin presents an in-depth discussion of a single topic of significant interest to the information systems community. Bulletins are issued on an as-needed basis and are available from ITL Publications, National Institute of Standards and Technology, 100 Bureau Drive, Stop 8900, Gaithersburg, MD 20899-8900, telephone (301) 975-2832. To be placed on a mailing list to receive future bulletins, send your name, organization, and business address to this office. You will be placed on this mailing list only.

Bulletins issued since August 2005:

- *Implementation of FIPS 201, Personal Identify Verification (PIV) of Federal Employees and Contractors, August 2005*
- *Biometric Technologies: Helping to Protect Information and Automated Transactions in Information Technology Systems, September 2005*
- *National Vulnerability Database: Helping Information Technology System Users and Developers Find current Information About Cyber Security Vulnerabilities, October 2005*
- *Securing Microsoft Windows XP Systems: NIST Recommendations for Using a Security Configuration Checklist, November 2005*
- *Preventing and Handling Malware Incidents: How to Protect Information Technology Systems from Malicious Code and Software, December 2005*
- *Testing and Validation of Personal Identity Verification (PIV) Components and Subsystems for Conformance to Federal Information Processing Standard 201, January 2006*
- *Creating a Program to Manage Security Patches and Vulnerabilities: NIST Recommendations for Improving System Security, February 2006*
- *Minimum Security Requirements for Federal Information and Information Systems: Federal Information Processing Standard (FIPS) 200 Approved by the Secretary of Commerce, March 2006*
- *Protecting Sensitive Information Transmitted in Public Networks, April 2006*
- *An Update on Cryptographic Standards, Guidelines, and Testing Requirements, May 2006*

availability of DNS services and prevent denial of service attacks. Other topics covered include how to secure DNS query and response activities, how to minimize information exposure through DNS data content control, and how to maintain secure operations. The appendices explain the technical terms and the acronyms used in the publication and contain extensive references to publications and websites with additional information.

The publication is available on NIST's web pages at: http://csrc.nist.gov/publications/nistpubs/index.html.

The Domain Name System Infrastructure

The Domain Name System is composed of several components. Users enter domain names to access Internet resources, through a program such as a web browser. The browser calls the DNS to provide the IP address for the appropriate web server and web page. This function of mapping domain names to IP addresses is *name resolution*, and the client system uses the DNS protocol to perform the name resolution function. The DNS has a data repository where the domain names and their associated IP addresses are stored. Software manages this data repository, which may be distributed, and provides name resolution service. This function is the *name server*. The function, which accesses the services provided by a DNS name server on behalf of user programs, is called the *resolver*. The DNS infrastructure is composed of the communication protocol, the various DNS components, the policies governing the configuration of these components, and procedures for creation, storage, and usage of domain names.

Securing the Domain Name System

The primary security goals for DNS are data integrity and source authentication, which are needed to ensure the authenticity of domain name information and to maintain the integrity of domain name information in transit. The availability of DNS services and data is also very important; DNS components are often subjected to denial of service attacks intended to disrupt access to the resources whose domain names are handled by the attacked DNS components. Misdirection of DNS data to a malicious site is another major security concern.

Who We Are

The Information Technology Laboratory (ITL) is a major research component of the National Institute of Standards and Technology (NIST) of the Technology Administration, U.S. Department of Commerce. We develop tests and measurement methods, reference data, proof-of-concept implementations, and technical analyses that help to advance the development and use of new information technology. We seek to overcome barriers to the efficient use of information technology, and to make systems more interoperable, easily usable, scalable, and secure than they are today. Our website is http://www.itl.nist.gov.

DNS Vulnerabilities

The DNS is susceptible to many of the same vulnerabilities as other distributed computing systems. These include vulnerabilities at the platform, software, and network levels. For most distributed systems, the security objectives of confidentiality, integrity, and availability of information apply. A loss of confidentiality is the unauthorized disclosure of information. A loss of integrity is the unauthorized modification or destruction of information. A loss of availability is the disruption of access to or use of information or an information system.

However, because the DNS serves as an infrastructure system for the global Internet, it has the following special characteristics not found in many distributed computing systems.

* There are no well-defined system boundaries. Participating entities are not subject to geographic or topologic confinement rules.

* There is no need for data confidentiality, one of the three security objectives for information. Public DNS data should be accessible to any entity regardless of the entity's location or affiliation.

Because of these special characteristics, conventional network-level attacks, such as masquerading and message tampering, and attacks that tamper with the integrity of the hosted and disseminated data, can have significant functional impacts on the entire Internet and on its users.

For example, a masquerader who spoofs the identity of a DNS node can deny access to services to the entire collection of Internet resources for which the node provides information. All of the domains served by the node would be affected, and the denial of service would impact all clients needing access to the resources.

False DNS information provided by a masquerader or intruder can corrupt the information cache of the DNS node providing that subset of DNS information. The name server providing Internet access service to the organization's users would be affected, and all users would be denied services and access to the resources provided by the server.

When the integrity of DNS information is attacked, the entire information retrieval process would be broken. The information maintained by the authoritative system or the information cache of an intermediary that has accumulated information from several historical queries would be affected. This situation can cause a denial of service for the DNS name resolution function or a misdirection of users to the wrong resources.

If the name resolution data hosted by the DNS system is inaccurate, there could be an increased workload on the DNS system or the provision of obsolete data that could result in denial of service to Internet resources. For most software, such as conventional database management systems (DBMS), the independence of the program data acts as a buffer to protect against the adverse impacts due to erroneous data. In the case of DNS, the data content determines the integrity of the entire system.

NIST Recommendations

NIST recommendations to protect DNS information are based on specifications developed by the Internet Engineering Task Force (IETF), an open international community of network designers, operators, vendors, and researchers concerned with the evolution of the Internet architecture and the smooth

operation of the Internet. See the *More Information* section below for information about the IETF's Domain Name System Security Extensions (DNSSEC) specifications, Transaction Signature (TSIG) specification, and for a link to IETF web pages.

Because of the functional impacts of attacks on the DNS, NIST recommends that organizations take the following actions to protect their DNS services:

* Implement appropriate system and network security controls for securing the DNS hosting environment, such as operating system and application patching, process isolation, and network fault tolerance.

* Protect DNS transactions such as the update of DNS name resolution data and data replication that involve DNS nodes within the organization's control. The transactions should be protected using hash-based message authentication codes based on shared secrets, as outlined in the IETF TSIG specification. Message authentication codes (MACs) are cryptographic functions that provide assurance to the receiver of data that the sender of the data is truly the sender and that the data has not been modified since it was authenticated. A hash function is a one-way function that produces a short representation of a longer message and is used to determine whether or not data has been changed after it was transmitted.

* Protect the ubiquitous DNS query/response transaction that could involve any DNS node in the global Internet using digital signatures based on asymmetric cryptography, as outlined in IETF's DNSSEC specification.

* Enforce content control of DNS name resolution data using a set of integrity constraints that are able to provide the right balance between performance and integrity of the DNS system.

NIST recommends that organizations secure their DNS name server through the deployment of the DNSSEC for zone information. A zone may be either an entire domain or a domain with one or more sub-domains. A zone is a configurable entity within a name server under which information on all Internet resources pertaining to a domain and a selected set of sub-domains is described. Zones are administrative building blocks of the DNS name space, just as domains are the structural building blocks.

Protection approaches for DNS software include choice of version, installation of patches, running the version with restricted privileges, restricting other applications in the execution environment, dedicating instances for each function, controlling the set of hosts where software is installed, placing the software properly within the network, and limiting information exposure by logical/physical partitioning of zone file data or running two name server software instances for different client classes. The latest version of name server software should be used.

Organizations should:

* Install a DNSSEC-capable name server implementation.

* Check zone file(s) for any possible integrity errors. NIST SP 800-81 details the technical steps that a DNS administrator can take in generating a zone file to keep network exposure to a minimum. This process should be done prior to signing a zone to authenticate security. Network information that should be kept absolutely private should not be published in DNS at all.

* Generate an asymmetric key pair for each zone and include them in the zone file. The DNSSEC specifies generation and verification of digital signatures using asymmetric keys. This requires generation of a public key-private key pair. Although the DNSSEC specification requires the use of just one key pair, experience from pilot implementations suggests that at least two different types of keys are needed for easier routine security administration operations such as key rollover (changing of keys) and zone re-signing. NIST SP 800-81 provides guidance on the use of NIST-approved algorithms for digital signatures and for hash algorithms to be used as part of the algorithms suite for generating digital signatures.

* Sign the zone. The process for signing a zone file consists of generating a hash, generating a signature, and capturing the signature information in a file.

* Load the signed zone onto the server.

* Configure name servers that deploy DNSSEC-signed zones or query-signed zones to perform DNSSEC processing. NIST SP 800-81 discusses the mechanisms involved in the DNSSEC approach, the operations that those mechanisms entail, and a secure way of performing those operations by using checklists.

Other NIST recommendations deal with the basic steps of DNSSEC deployment for caching name servers.

* Install a DNSSEC-capable resolver implementation.

* Obtain one or more trust anchors for zones that the administrator wants to be validated. Until all zones become signed zones, there could be a situation in which a zone is signed but its parent zone is not signed. A chain of trust should be established through all of the zones in the DNS tree to assure the authenticity of the public key of a zone signer.

* Configure the resolver to turn on DNSSEC processing.

Other recommendations in the guide deal with the secure configuration and the operations of name servers.

More Information

NIST recommendations for securing the DNS are based on the following primary security specifications that were developed by the IETF, an open international technical group:

* Internet Engineering Task Force (IETF) Domain Name System Security Extensions (DNSSEC) specifications, covered by Request for Comments (RFCs) 4033, 4034, 4035, and 3833; and

* IETF Transaction Signature (TSIG) specifications, covered by RFCs 2845 and 3007.

Documents produced by the Internet Engineering Task Force are referenced in Appendix C of NIST SP 800-81. General information about IETF is available at http://www.ietf.org/.

The IETF community's ultimate goal is for DNSSEC to be fully deployed across the entire domain tree on the infrastructure side, and implementation in applications that can demand the services provided by DNSSEC. At present, there are no operational nodes in the DNS domain tree that provide DNSSEC capabilities. The first step towards full deployment is to provide DNSSEC capability for domain sub-trees that have high security needs.

Once DNSSEC capabilities become widely available in the infrastructure, application developers will be able to develop DNSSEC applications and use DNSSEC as a means for network security. In the future, all DNS name servers and clients should be able to perform at least some of the operations detailed in the DNSSEC specifications and in NIST SP 800-81.

NIST publications assist organizations in planning and implementing a comprehensive approach to IT security. For information about NIST standards and guidelines that are referenced in the DNS guide, as well as other security-related publications, see http://csrc.nist.gov/publications/index.html.

Recent standards and guidelines of particular interest to the federal community address the process that federal agencies should apply in determining appropriate and effective security controls for their systems. Federal Information Processing Standard (FIPS) 199, *Standards for Security Categorization of Federal Information and Information Systems*, requires agencies to categorize their information systems as low-impact, moderate-impact, or high-impact for the security objectives of confidentiality, integrity, and availability. FIPS 200, *Minimum Security Requirements for Federal Information and Information Systems*, specifies the minimum security requirements for information and information systems in seventeen security-related areas. Federal agencies must meet the minimum security requirements through the use of the security controls in accordance with NIST SP 800-53, *Recommended Security Controls for Federal Information Systems*. NIST SP 800-53 has been revised to include safeguards and countermeasures for information systems that reflect the state of the practice, including DNSSEC. Information about the proposed revision and the public review period is available from the NIST publications website.

Disclaimer

Any mention of commercial products or reference to commercial organizations is for information only; it does not imply recommendation or endorsement by NIST nor does it imply that the products mentioned are necessarily the best available for the purpose.