SAC 049
SSAC Report on DNS Zone Risk Assessment and Management

A Report from the ICANN
Security and Stability
Advisory Committee
(SSAC)
03 June 2011

Preface

This is a Report of the Security and Stability Advisory Committee (SSAC). The SSAC advises the ICANN community and Board on matters relating to the security and integrity of the Internet's naming and address allocation systems. This includes operational matters (e.g., matters pertaining to the correct and reliable operation of the root name system), administrative matters (e.g., matters pertaining to address allocation and Internet number assignment), and registration matters (e.g., matters pertaining to registry and registrar services). The SSAC engages in ongoing threat assessment and risk analysis of the Internet naming and address allocation services to assess where the principal threats to stability and security lie, and advises the ICANN community accordingly. The SSAC has no official authority to regulate, enforce or adjudicate. Those functions belong to others, and the advice offered here should be evaluated on its merits.

The contributors to this Report, reference to the committee members' biographies and statements of interest, and committee members' objections to the findings or recommendations in this Report, are at end of this Report.

Table of Contents

1. Introduction

This Report discusses circumstances that result in the loss or disruption of domain name resolution that can temporarily eliminate a domain name from the Internet. Without understanding the mechanisms underlying Domain Name System (DNS) operations and understanding the information necessary to construct DNS information, domain name registrants are at risk for long-term service interruptions.

The Report provides an overview and background of the domain name registration process and how registration relates to domain name resolution. It considers technical or business circumstances that might result in loss or disruption of domain name resolution. The SSAC represents such circumstances as risks and recommends measures domain name registrants should take to reduce the impact to their businesses or organizations should any such circumstance affect their domain name(s).

2. Overview and Background

Internet users rely on a unique distributed name system to identify computers and services accessible via the Internet. Names registered in this distributed database are called domain names. The DNS is used to access this database. While the DNS has many uses, the most familiar and common use of the DNS is to obtain the Internet Protocol (IP) address associated with a user-friendly domain name (e.g., `www.example.com`). The process of providing this translation from domain names to Internet Protocol (IP) addresses starts with domain name registration (where an individual or organization registers a domain and thus the right to use it), moving to configuring the DNS (where the registered user, the registrant, identifies the names and addresses of name servers that will provide authoritative name resolution), and then hosting the DNS for a particular domain name (i.e., the parties that operate the registered user's authoritative name servers).

2.1 Domain Name Registration

Internet users obtain domain names through a registration process. An Internet user (or organization) first chooses a Top Level Domain (TLD) *registry* in which he will register a domain name (e.g., `com`). The user then chooses an available label to register (e.g., `example`). (In practice, label availability may influence the choice of TLD registry.) Through the registration process, the registry delegates authority to the user over his domain name. This process is often performed through a party called a domain name *registrar*. The user – now formally a domain name *registrant* – becomes responsible for the delegated part of the domain space named `example.com`. The registrant can now compose selected names within the domain name, e.g., `www.example.com` and `mail.example.com`.

The SSAC reminds those registrants who use ICANN accredited registrars that they are obliged to provide complete and accurate registration information for each domain name they register. Clause 3.7.7.2 of the Registrar Accreditation Agreement specifically warns that inaccurate information may be a cause for the cancellation of the domain name registration, which would, as a consequence, cause the domain to stop resolving.[1] Other registries may have similar requirements.

2.2 Configuring DNS

The registrant must make certain information available so that other Internet users can use the DNS to obtain the IP addresses associated with domain names under his authority; for example, a public-facing web or email server. The registrant does so by composing a *zone file* of configuration information. A DNS zone file nominally includes the domain names of all the computers and services the registrant wishes to make accessible via the Internet and the IP addresses (Internet Protocol Version 4 (IPv4) or Internet Protocol Version 6 (IPv6)) associated with these domain names; it also includes certain mandatory and other resource records. The registrant then arranges for the zone file to be hosted at what is formally called an *authoritative* name server. The term *authoritative* is significant. While other servers called *recursive* name servers may provide name resolution for generally any domain name accessible via the public Internet (by querying other authoritative name servers), only the information hosted by an authoritative name server is treated as the accurate and complete set of information associated with a given domain name.

2.3 Hosting DNS

To "host DNS", the domain name registrant chooses a party or parties who will support an authoritative name service on his behalf, i.e. to host or publish the DNS zone file for the registrant's domain name. Such parties configure and operate a DNS name server to meet functional and operational standards. The registrant can choose to self-host an authoritative name service or he can contract with a third party to host the authoritative name service on his behalf. The third party may be any external party that provides name service to customers. Many domain registrars and resellers, ISPs, and businesses that offer web, email, or other managed services (e.g., network access, security) offer DNS hosting as a service.

Once the registrant chooses a DNS hosting provider, he must provide his registry, usually through a domain name registrar, with the domain name and the associated IP address information of the DNS hosting provider's name server(s) that will host his zone file. The TLD registry will include this information in the TLD zone file. Note that in many third-party DNS hosting scenarios, this step may be performed (with the registrant's *consent*) by his chosen DNS hosting provider.

[1] ICANN Registrar Accreditation Agreement, 21 May 2009 <http://www.icann.org/en/registrars/ra-agreement-21may09-en.htm>.

2.4 DNS Zone File Composition and Publication Considerations

How a domain name registrant composes and publishes a DNS zone file is influenced by his choice of DNS hosting provider:

1. In self-hosted scenarios, the registrant's technical or administrative staff gathers the resource information, composes the DNS zone file, and publishes this on the registrant's name server(s).
2. In certain third-party hosting scenarios, the DNS hosting provider allows or expects the registrant to compose a DNS zone file in its entirety. The registrant delivers this to the hosting provider using whatever media, web portal, or transfer method the DNS hosting provider requires.
3. In other third-party hosting scenarios, the registrant submits some but not all zone data to the DNS hosting provider via a web submission form, email, or other electronic or out-of-band manner. The DNS hosting provider uses this information to compose a zone file (or to configure its name service platforms with the equivalent of the zone data submitted by the registrant).

In scenarios (2) and (3), the registrant may not be party to the actual preparation of the published zone data. Specifically, the registrant may not be made aware of, or keep all of, the potentially critical information that is used to create DNS resource records. For example, the registrant may not know the IP addresses of web, email, or other hosted services he has outsourced, whether to the same or separate business entities. The SSAC thinks registrants may not know or appreciate the risk associated with such circumstances. Specifically,

> *A registrant who does not have complete knowledge of the information used to create the zone file for a domain is at risk of having name resolution interrupted without the ability to restore name service.*

Why is this important? Domain name resolution is an essential and critical service. You or your organization's Internet presence relies on the ability of users to determine the IP addresses that you have associated with the names of your web, email, or other public-facing Internet services. If this resolution is not available, very few Internet users will connect to your web, email or other services. Any circumstance where name resolution is interrupted is a threat to you or your organization's online presence. The remainder of this report explains the technical and business circumstances that place name service disruption at risk. We explain how to assess the risk and recommend measures that registrants can take to mitigate them.

3. Assessing Risk

Registrants should be aware that certain attacks, incidents, or circumstances could harm a registrant's online presence. Examples of attacks, circumstances or incidents that may leave the registrant without a complete and accurate copy of the configuration information or the ability to update erroneous information used to create a zone file include:

1. A business or technical failure of a third-party DNS hosting provider. Examples of business failures include bankruptcy, or abrupt cessation of business by the operator, or as a result of a legal proceeding. Examples of technical failures include loss of Internet access, or damage to the provider's equipment or facilities that are significant enough to disrupt or permanently prevent the provider from restoring name service or resuming normal business operations.
2. A temporary (technical) failure of the registrant's self-hosted DNS hosting service. The technical failures here are similar to those mentioned in (1).
3. An attack resulting in compromise of the domain name registrant's domain registration account, usually at the domain name registrar, where the attacker alters the DNS configuration information associated with a domain, either replacing the intended IP address of the authoritative name server(s) with IP addresses under the attacker's control, or creating additional IP address entries.
4. A lock-out situation, i.e. a transfer of the domain or a change in the delegation of a domain, during which changes to DNS configuration information may be prohibited.
5. An attack against the registrant's administrative account for DNS hosting (including the self-hosted scenario) where the attacker alters DNS zone data for misuse of the registrant's DNS; for example, to deface or phish the registrant's domain.
6. A configuration error or insider attack, where an authorized administrator of a domain name registration account or administrative account for DNS hosting alters the correct DNS configuration or zone data.

The types of harm resulting from such attacks, incidents, or circumstances include:

- Abrupt loss of, or loss of access to, the configuration information that is used to compose the registrant's authoritative zone file (or equivalent, for those DNS hosting providers that manage zone data in platform specific manners).
- Loss or disruption of name resolution service for a registered domain.
- Inconsistent name resolution. This can be a consequence when the registrant has provisioned for resilient name service (two or more DNS hosting providers that support authoritative name service for a domain name) but the DNS hosting providers are operating with conflicting zone data and are not providing the same answers to queries.

- Delay in the publication of changes to zone data may cause continued use of stale or inaccurate zone data (i.e., the binding of a web server name to a wrong IP address) or suppression of changes that were necessary to rectify erroneous zone data.

The duration of such harms varies, but registrants should be aware that loss of, disruption of, or inconsistent availability of name resolution service could persist for an indeterminate and possibly long period of time in circumstances where the registrant is unable to recover complete and accurate zone information.

4. Recommendations for Managing Risk

The SSAC recommends that registrants consider implementing the following safeguards and proactive measures to manage the risk associated with loss, disruption, or inconsistent availability of name service.

Recommendation 1: Thoroughly document all aspects of your DNS architecture and operations.

Documentation should include but not be limited to:

1. Complete and accurate contact information, including emergency or abuse contacts, for all parties that provide DNS service.
2. Complete and accurate contact information, including emergency or abuse contacts, for all hosting parties on whom you depend upon for configuration information. Examples include web, email, voice, or other hosting providers on whose systems your services are hosted and from whom you will obtain naming and IP address information for DNS resource records (e.g., MX, CNAME, NAPTR, or other resource record types).
3. Names and IP addresses of all name servers on which your zones are hosted.
4. Topology information, i.e. information that illustrates location and connectivity of your DNS hosting providers.
5. Copies of the published zone file.
6. Copies of all the information that is needed to compose your zone file.
7. Notes and instructions on the steps used to compose the zone file and the rationale for the contents.
8. Historical copies of all information listed above.
9. Operational statistics and trends related to load serviced by the DNS architecture. (These are useful when troubleshooting.)

Recommendation 2: Design for resiliency.

Design your name service so that it is as close to "always available" as possible. This means that your DNS service should be resilient to failure of any individual application, host or communications service. Typical availability standards for DNS are much higher than other Internet services; few DNS hosting providers who commit to an availability standard advertise anything less than 99.999 percent availability.

When considering a resilient design, it is important to identify human technical, topological, and hosting provider single points of failure in your name service infrastructure. Once you identify weak links in your existing design, eliminate these by introducing diversity where your name service is less resilient than desirable.

Recommendation 3: Actively manage DNS information.

Change control is a critical component of DNS information management. Implement an approval process that documents the origin and reason for the change, the intended effect of the change, any dependencies (i.e., configuration changes to other resources affected by the change), and the party that authorized the change. Track changes by maintaining an audit trail or log as part of this process. Implement an archival process to ensure that your DNS information is regularly backed up, as well as a process to restore DNS (zone) information should the need occur. Schedule regular tests of zone restoration. Such tests can be as simple as copying the most recent DNS information from archive media to a name server and restarting the name server.

Recommendation 4: Protect domain registration and hosting accounts against unauthorized access or misuse.

Consider implementing measures to protect your domain registration account that SSAC identifies in "SAC044: A Registrant's Guide to Protecting Domain Name Registration Accounts."[2] While SAC044 applies specifically to domain registration accounts, many measures are generally prescriptive: you can apply similar measures to protect accounts with DNS or other (web, email) hosting providers.

Recommendation 5: Monitor the health and well being of your name service.

Implement the practices for monitoring name resolution recommended in SAC044 or engage a trusted third party to monitor on your behalf.

[2] "SAC044: A Registrant's Guide to Protecting Domain Name Registration Accounts," ICANN Security and Stability Advisory Committee, 05 November 2010 <http://www.icann.org/en/committees/security/sac044.pdf>.

Recommendation 6: Track operational statistics and trends.

Collecting and reviewing information related to load serviced by the DNS architecture is useful when troubleshooting operational problems and making decisions about infrastructure investments.

Recommendation 7: Develop a continuity plan for recovering from DNS outages.

Have a plan to respond to all possible outage types. Identify who is responsible, what actions responsible parties must take, and make certain responsible parties have access to all the documentation they need to perform their role in the recovery process. Document all incidents and perform a post-incident (mortem) analysis to assess the effectiveness of the plan.

Recommendation 8: Before making changes in provisioning, plan carefully.

Consider the order in which you must make changes so that you avoid unnecessary delays should any status locks be applied to the domain registration or third party provider accounts as a consequence of your change activities. As general guidance, follow these steps:

1. If you intend to change registrars (in those cases where a registrar is how you interact with the registry), do this before other changes.
2. If you intend to transfer the domain to a new registrant, do this before any change to the DNS configuration information associated with the domain.
3. If you intend to change DNS hosting providers, do this before making changes to zone file information.
4. If you intend to change the delegation of the zone, provide the gaining DNS hosting provider with the complete and accurate zone file before changing the delegation.

Recommendation 9: Make informed choices when selecting DNS providers.

When considering an operator to provide authoritative name service for your domains, ask questions that will help you make an informed choice and that will also help you formulate a strategy for managing risk. Sample questions to ask operators include:

1. How do you construct zone data (what information do you require from my organization)?
2. At how many sites will you host my zones?
3. Where (geographically) will the zones be hosted?

4. What is the bandwidth and server sizing for each site?
5. What measures do you take to secure name servers against attack?
6. What measures do you deploy to detect and mitigate Distributed Denial of Service (DDOS) attacks?
7. How do you monitor zones you host?
8. What information or reports do you provide based on your monitoring?
9. What forms of notifications or alerts do you provide customers for security events? Maintenance events?
10. What service levels do you commit to maintain?
11. Can your zone hosting monitoring mechanisms be integrated into my operational monitoring?

This list is not exhaustive but representative of the types of questions to ask during interviews or in a request for proposal.

5. Acknowledgments, Statements of Interests, and Objections, and Withdrawals

These sections provide the reader information on three aspects of our process. The Acknowledgments section lists the members who contributed to this particular document. The Statements of Interest section points to the biographies of the Committee members and any conflicts of interest, real, apparent or potential, that may bear on the material in this document. The Objections and Withdrawals section provides a place for individual members to disagree with the content of this document or the process for preparing it.

5.1 Acknowledgments

The committee wishes to thank the following SSAC members for their time, contributions, and review in producing this Report.

Patrik Fältström
Jim Galvin
Merike Kaeo
Xiaodong Lee
Danny McPherson
Richard Wilhelm
Suzanne Woolf

5.2 Statements of Interest

SSAC member biographical information and Statements of Interest are available at: http://www.icann.org/en/committees/security/biographies-25mar11-en.htm.

5.3 Objections and Withdrawals

There were no objections or withdrawals.

Addendum: DNSSEC

DNS Security Extensions (DNSSEC) uses encryption methods to provide operational-level protection against the unauthorized alteration of DNS information.[3] DNSSEC provides (1) origin authentication of DNS information and thus provides protection against impersonation attacks; (2) data integrity check and thus protection against cache-poisoning and related (e.g., Kaminsky[4]) attacks; and (3) *authenticated denial of existence* for a particular name: an assurance that the domain name does not exist in the zone file.

While DNSSEC increases the operational security of the DNS, it also adds complexity to day-to-day DNS operations. In particular, DNSSEC involves the use of public key cryptography, which itself requires the generation of public-private key pairs and distribution (publication) of public keys associated with signed zone data. Registrants must consider management of these keys, whether by an individual, organization, or a third-party agent such as a registrar or DNS hosting provider when they assess and seek to mitigate risk associated with domain zone data.

The SSAC notes that as of the date of this report, registrar support for, and hosting of, DNSSEC-signed zone data is evolving rapidly (when compared to the hosting of traditional DNS). All members of the community are still acquiring operational experience after the signing of the root zone of the DNS, and best practices are slowly emerging. Consequently, the SSAC makes no specific recommendations at this time regarding DNSSEC except to encourage registrants that choose to adopt DNSSEC to discuss DNSSEC support with DNS hosting providers and to choose agents that can assist you with key management, DNSSEC signing of resource record sets, and public key distribution. The SSAC expects to examine DNSSEC-specific zone risk considerations again in a future report.

[3] See DNSSEC Protocol Requests for Comment (RFCs) at <http://www.dnssec.net/rfc>.

[4] See: <http://www.networkworld.com/news/2008/080608-kaminsky-many-ways-to-attack.html>.