SSAC Advisory SSAC0011
Problems caused by the non-renewal of a domain name associated with a DNS Name Server

A Report from the ICANN
Security and Stability
Advisory Committee
(SSAC)
June 2006

About the Security and Stability Advisory Committee

The Security and Stability Advisory Committee (SSAC) is an advisory committee to the Internet Corporation for Assigned Names and Numbers (ICANN).

The Committee's purpose is to offer independent advice to the ICANN board, the ICANN staff and the various ICANN supporting organizations, councils and committees as well as to the technical community at large on matters relating to the security and integrity of the Internet's naming and address allocation systems. The Committee has no official authority to regulate, enforce or adjudicate. Those functions belong to others. The advice offered by the Committee should be evaluated on its merits, not on the status of the Committee or its members.

The Committee draws its membership from the commercial and not-for-profit sectors. It has broad geographic representation and has representation across industry and academe, including all segments of the domain name system (DNS) community. The committee includes members who operate root servers, generic and country code top-level domain servers, registrars and address registries. Some members are network security experts or researchers. The Committee members serve without pay, each a technical contributor in his or her own organization and in the community at large. An ICANN Fellow also serves on the Committee and is compensated by ICANN.

Because the Committee is composed of people actively working in the field, conflicts of interest arise from time to time. Committee members are expected to declare conflicts of interest, whether actual, potential or apparent, but Committee members are not required or expected to recuse themselves. Whenever Committee members or other contributors work for organizations that may have a vested interest in the matter at hand, the Committee's practice is for each participant to disclose such relationships and expect the participants to provide technical information without attempting to influence others.

The Committee operates primarily by issuing Reports, Advisories and Comments. These are usually written and edited by the SSAC Fellow, Dave Piscitello under the direction of Committee members. The Reports, Advisories and Comments represent output from the Committee as a whole. Further information about the Committee is posted to the Committee's Web site at http://www.icann.org/committees/security/. The Appendix contains the current list of members and contributors to this report.

Problems caused by the non-renewal of a domain name associated with a DNS Name Server

Introduction

This report by the Security and Stability Advisory Committee (SSAC) considers the problems that may arise when the registrant of a domain name *A* uses a DNS name server in domain *B* for domain name resolution, and the registrant of domain name *B* accidentally or intentionally allows its domain name registration to expire. The report explains that several unanticipated consequences are possible. In circumstances where coordination across well-intentioned parties is lost, name service for domain *A* may be interrupted or may become unpredictable; in other circumstances, a new registrant of domain *B* may alter domain *A*'s DNS information for malicious purposes, including phishing attacks, email interception, and redirection of Internet users to different websites with different and possibly harmful content.

Note that these incidents involve (a) registration of expired (deleted) domain names and subsequent operation of a DNS name server by a different party than the previous registrant, and (b) take place beyond redemption grace periods provided by registrars and registries (see, for example, [1]).

Audience and Objectives

This Advisory is written for Domain Name registrants, registrars and registries, but is relevant to anyone who is involved or wishes to become familiar with issues relating to domain name registration and domain name service operations. The actions recommended herein consider the policies and practices in place at the time the Advisory was published. Changes to policies and practices may require different or additional considerations.

Relationship between Domain Name Registration and DNS Name Service

At the time of domain name registration, a registrar collects contact information for the registrant and for parties who can respond to operational and administrative matters relating to the registered domain name (the technical and administrative contacts, respectively)[1]. This *registration record* also includes the domain names of systems that will provide DNS name service for the registered domain name.

TLD operators add registered domain names to a Registry database of all active labels under the TLD label. The TLD operator also adds the registrant's DNS name server information to the DNS records it hosts on TLD name servers. The DNS name servers the registrant identifies are considered *authoritative* for the registrant's domain name, i.e.,

[1] SSAC 0010, Renewal Considerations for Domain Name Registrants [2], describes the registration, renewal, and deletion processes in more detail. Sections relevant to this Advisory are reproduced as Appendix A.

they are expected to maintain and return accurate DNS information when DNS queries are referred to them.

Registrants are responsible for creating DNS information for their domain names and for arranging authoritative name service for hosts within their domains. Examples of DNS information (resource records) include `MX` records to identify the location of a computer for receiving email associated with the domain name, and `A` or `AAAA` resource records which can be used to identify the Internet (IPv4 and IPv6) addresses of a computer that hosts a web or other service for that domain name.

To make all or part of the DNS information available to any user on the Internet, a registrant can choose to support DNS name service from a system that is assigned a domain name from

1. The registered domain; for example, `dns1.example.biz` can serve as an authoritative DNS name server for `example.biz,`

2. Another domain the registrant has registered; for example, if the registrant registers the domain names `example.biz` and `example.net`, the registrant can arrange for `dns1.example.net` to support DNS name service for `example.biz`. and

3. A domain registered by a different party than the registrant, e.g., the registrant's registrar or reseller, an ISP, domain name hosting company or other party the registrant contracts to provide DNS service.

Configuration (1) is called an *in-bailiwick* DNS service. Configurations (2) and (3) are called *out-of-bailiwick* DNS services.

Domain name service is necessary for the correct operation of most Internet applications, thus availability and accuracy are critical service metrics for DNS. Accordingly, most organizations will arrange for name service support from multiple DNS name servers. The standard advice is to have at least two name servers, and it is not uncommon to have three or more.

In cases like these, it is common for organizations to provide DNS using combinations of in- and out-of-bailiwick name servers. In such configurations, a registrant assumes that

- The registrant of the domain from which the out-of-bailiwick name server is assigned a name does not allow the name registration to expire,

- The domain name remains registered to the same party with whom registrant has arranged out-of-bailiwick name service, and

- If either of these conditions change, someone will notify registrant.

In the next section, we consider scenarios where these conditions are not satisfied and may cause problems for registrants who depend upon them.

How Deleted Names Can Adversely Affect DNS Service

Registrants create operational dependencies between domain name service and domain name registrations when they arrange to host DNS records on systems under different and multiple domain names. Specifically, when name service for any domain `example.tld` is provided by a host that is assigned a name from a domain other than `example.tld`, the registrant's name service relies on the continued operation of that domain (and name server), by the party with whom the registrant of `example.tld` established an operational arrangement.

In the simple case, consider a scenario where the registrant of domain `example.tld1` arranges for name service to be provided from a host named `ns1.example.tld2`. If the registration of the domain `example.tld2` expires,

- The label `example` is deleted from the `tld2` Registry database,
- The `tld2` name servers will not resolve any name in `example.tld2`, and
- Name service for `example.tld1` is interrupted.

Suppose the registrant of `example.tld1` chooses to provide a primary name service from a host in its own domain, e.g., `dns1.example.tld1` and also arranges for secondary name service to be provided from `ns1.example.tld2.` Again, if the registration of the domain `example.tld2` expires,

- The label `example` is deleted from the `tld2` Registry database,
- The `tld2` name servers will not resolve `ns1.example.tld2`, but in this scenario,
- Name service for `example.tld1` is interrupted for any resolver that queries `ns1.example.tld2` to resolve names in `example.tld1` names that are configured to.

Note that in these cases, the registrant of `example.tld2` could be the same as the registrant of `example.tld1`, or a different party entirely. In these scenarios, the name servers could in fact be configured and operating properly but are no longer reachable: oversight or lax management of domain name *registrations* caused the name to expire.

Next, we consider a scenario where an attacker exploits an expired domain name registration to harm the registrant of `example.tld1.`

Suppose the registrant of domain `example.tld1` arranges for name service to be provided from a host named `ns1.example.tld2`. An attack against `example.tld1` might be executed as follows:

- The registration of the domain `example.tld2` expires,

- The label `example` is deleted from the `tld2` Registry database,
- An attacker registers the domain name `example.tld2`,
- The attacker runs a name server at `ns1.example.tld2`,
- The attacker creates DNS records for `example.tld1` that resolve names from `example.tld1` to the attacker's systems, and
- Traffic intended for hosts in `example.tld1` that is resolved by the attacker's name server is redirected to the attacker's exploit systems.

The effect of this attack is similar to DNS cache poisoning and pharming attacks that are commonly used to abet phishing, identity theft, web defacement and user impersonation attacks. We have illustrated the attack using the simple case of a single name server. However, this attack is remains effective against some number of users even when `example.tld1` has multiple name servers.

Remedies

Domain name registrants are ultimately responsible for managing domain name registrations and name services for their domain names. When arrangements are made to host name service out-of-bailiwick for a registered domain name, a registrant should:

- Identify a party in its own organization who is responsible for coordinating DNS name service matters with the operator of the out-of-bailiwick name server,
- Identify a technical contact in the out-of-bailiwick name server operator's organization who will be responsible for name administration matters,
- Establish a formal process for DNS record and other name service administration matters with the out-of-bailiwick name server operator, and
- Actively monitor name service to verify that name resolution is accurate for DNS records at all authoritative name servers (whether in- or out-of-bailiwick).

These actions can reduce the risk that deletion of a domain name registration will interrupt name service or expose the registrant's domain to traffic redirection attacks and operational instabilities.

Registries and registrars should advise registrants to maintain accurate contact and DNS name server information in domain name registration records. SSAC encourages registrars to use this Advisory and complementary educational information as the basis for building public awareness of the importance of maintaining correct DNS name server information in domain name registration records.

Accurate contact and name server information helps registries, registrars and technical staff in other registered domains identify inconsistencies in name service operation and possibly intervene before domain name service is interrupted and traffic hijacking attacks are attempted. For example, in the scenarios described above, if the name server `ns1.example.tld2` is identified in the registration record for the domain `example.tld1`, then the registry, registrars and resellers for `tld1`, alone or in concert with registry,

registrars and resellers of `tld2` may have sufficient information to take one or more of the following actions:

- Provide periodic reminders to encourage technical contacts to verify DNS configuration and name server information in the registration record,
- Monitor name service for domains in the Registry and intervene when they detect an incorrect DNS configuration,
- Delete a lame delegation or delay the completion of a suspicious change of delegation until it can be corroborated.

Some Registries implement services like these today (see [3, 4]). SSAC recommends that registries and registrars study methods for monitoring name service and provide notice to registrants, particularly where coordination across registries is needed.

Findings

The Committee offers the following findings for consideration:

(1) Registrants create operational dependencies between domain name service and domain name registrations when they arrange to host DNS records on systems that are assigned names from out-of-bailiwick domains.

(2) Domain name registrations are not permanent, and may might not be renewed. If a registration is not renewed and a different party may might register it.

(3) Registrants should not assume that registries and registrars will notify parties other than the domain name registrant when a domain name registration is not renewed. While some may offer such services, registries and registrars are not obliged to identify interdependencies registrants may have created across domain name registrations.

(4) Registrants put name service operation at risk of interruption if they do not provide accurate contact information to registries and registrars for situations where a domain's DNS records are hosted on systems under different domain names registered by the same registrant,

(5) In situations where a domain's DNS records are hosted on systems that are assigned names from out-of-bailiwick domains, **registrants put name service at risk of interruption and toor redirection attacks by parties with malicious intentions when domain names on which the registrant depends are not renewed and subsequently registered.**

Recommendations

Domain name registrants are ultimately responsible for providing reliable name service for their domain names. All registrants, whether holders of one or numerous domain

names, are encouraged to consider the following measures to minimize the risks associated with re-use of domain names.

(1) Maintain accurate contact information in domain name registration records. When records are accurate, registries and registrars can contact registrants with notices of renewal. Such renewal notices help registrants avoid interruptions in name service and reduce exposure to redirection attacks.

(2) Establish a chain of accountability for domain name registration. Each domain name registration record identifies three contact parties: the registrant, an administrative contact, and a technical contact. Make certain that these parties understand who is responsible and accountable for renewing domain name registrations. In circumstances where registrants outsource domain registration to a reseller, make arrangements with the reseller to monitor and renew domain names.

(3) Maintain accurate contact information for all registrants of domain names with whom your organization has arranged DNS name service hosting. Make certain that administrative and technical contacts in your organization have access to this contact information to assist in resolving operational matters.

(4) Monitor your domain name service. Registrants should actively monitor domain name servers that host their DNS records to verify that their authoritative DNS name servers are providing accurate domain name information.

(5) Use DNSSEC to protect against undetected modification of DNS records. DNS Security (DNSSEC, RFCs 4033, 4034, 4035) provides a means to verify that the name server claiming authority over the DNS records is authentic and data integrity measures to assure that DNS information acquired from the name server claiming authority are accurate and have not been tampered with.

References

[1] Redemption Grace Periods for Deleted Names
http://www.icann.org/bucharest/redemption-topic.htm

[2] SSAC 0010, Renewal Considerations for Domain Name Registrants
http://www.icann.org/committees/security/renewal-considerations-15may06.pdf

[3] JPRS Takes Measures to Mitigate Risks Caused by Improper Management of DNS Servers Associated with JP Domain Names
http://jprs.co.jp/en/topics/051213.html

[4] JPRS Commences an Effort to Eliminate the Risk Caused by Improper Management of DNS Servers Associated with JP Domain Names
http://jprs.co.jp/en/topics/050805.html

Appendix A

Name Registration, Renewal and Deletion

(reproduced from SAC0010, *Renewal Considerations for Domain Name Registrants*)

For a registrant, the domain name registration process begins at a registrar. Registrars are parties that operate under agreements with ICANN to register domain names on behalf of the registrant (an individual, organization, or company)[2],[3]. Technically, each TLD Registry assures uniqueness of a second level label assigned within a TLD; for example, there will only be one label "example" within the com registry, assuring the uniqueness of example.com. When a registrant registers a name, a TLD Registry adds the second level label to a database of domain names assigned and registered within the TLD.

Registrars collect certain information from the registrant of each domain name at the time of registration. This registration record contains contact information for the domain name registrant and for parties who can respond to operational and administrative matters relating to the registered domain name (the technical and administrative contacts of the registration record, respectively). The registrant must also identify the name servers that will host the zone file for the domain. Registration assures that a domain name is unique within a registry of domain names, and grants the registrant the use of the domain name for a specified period of time. Registration also provides contact information that can be used to resolve disputes as well as technical and administrative matters related to the domain name.

A fee for domain name use is collected by a registrar or reseller, and registrants may register names for a term of one or multiple years. When the term of a domain name registration is about to expire, many registrars and resellers will notify registrants in advance, as part of a customer care and retention program. Some registrars and resellers provide auto-renewal services. Registrars and resellers commonly use electronic mail to deliver domain name expiration notices. The notices are sent to one or more of the contact email addresses (administrative, technical, name holder) provided by the registrant when the name is registered. However, registrars and resellers of gTLD registrations are not bound by their agreements with ICANN to make such notifications. *The registrant is responsible for providing complete and accurate registration information. One obvious incentive for keeping this information accurate is to prevent a situation where a registrar is unable to notify a registrant that a domain name registration is about to expire.*

Most ICANN accredited registrars of gTLD domain names provide some form of grace period after expiry before the domain name is cancelled. Grace periods range from zero

[2] Registrars must be accredited by ICANN to register names from gTLDs, but some of the same registrars also provide registration services for certain ccTLDs without any connection to ICANN. However, ccTLD managers (and not ICANN) determine how domain names are registered and make their own arrangements with any third parties who offer registration services for their ccTLD.
[3] ICANN maintains a list of accredited registrars for gTLDs at http://www.icann.org/registrars/accredited-list.html.

to 45 days, with most registrars offering at least 30 days. During this period, registrars may adopt a range of approaches to notify the registrant that a name registration is about to expire, including phoning the registrant, faxing the registrant, postal mail, removing the domain name from the zone, or putting up a parked web page informing users that the domain name has expired.

Registries operating under agreements with ICANN may voluntarily provide additional measures to prevent cases where a domain name is cancelled as a result of mistake, inadvertence, or fraud (for example, [4]). A gTLD registry may hold a cancelled domain name registration for an additional 30-day *Redemption Grace Period* before deleting it from the database and thus making the name available to any would-be registrant.

The Redemption Grace Period [2] [4] gives the registrant an extended opportunity to learn or detect that the domain name registration has expired. During this time, the domain name cannot be registered by any other party; however, the domain name is removed from the TLD's master zone file, the database that TLD domain name servers use to resolve domain names to Internet (IP) addresses. This action has a practical effect of preventing Internet users at large from accessing a web site operated in that domain or sending email to users in that domain. Often, if the domain name non-renewal is unintentional, a registrant can restore and renew the registration through the associated with this domain name. The registrar notifies the registry, the "hold" status of the domain name is removed, and (if the domain name is in active use) the domain name is restored to the TLD's master zone file.

After this 30-day period, a gTLD domain name is held in a 5-day delete pending period. During this period, the domain name is published in a pending delete list that identifies the date when the domain name will be made available for re-registration. Many parties in the community monitor the list of names that will become available for re-registration, and compete to get what they consider to be the most valuable domain names. Taking into account the various grace periods, most gTLD names become available for re-registration between 60 and 80 days of the original domain name expiry date.

Some important observations can be made from this overview of the domain name registration process:

1. Domain name registrations are temporary. While arrangements can be made to register a domain name over a span of many years, or to renew registrations automatically upon expiration, there is no way to establish "perpetual ownership".

2. Each domain name registration or renewal is an independent agreement between a registrar and registrant. Registrars are only obliged to notify the registration of a change in registration status of a domain name. Registrants are not obliged to notify any party who may refer to the domain name or rely on services (e.g., DNS name service) provided by systems assigned names from their domain names.

[4] Registrars may also register domain names in country-specific Top Level Domains, ccTLDs. Country code TLD managers set their own policy and decide whether to offer services such as the redemption grace period.

3. Contact information in the domain name registration record is used to resolve disputes as well as technical and administrative matters related to the domain name. If this information is not kept accurate, registries and registrars will not be able to contact registrants with notices of renewal.

4. Domain name server information in the domain name registration record is useful in identifying the authoritative information for a domain (the master/zone file). If this information is not kept accurate, technical and administrative matters related to name service operation for the domain may not be attended to in a timely manner.

Acknowledgements

SSAC wishes to acknowledge Jaap Akkerhuis, Patrik Fältström, Daniel Karrenberg, Dave Piscitello and Bruce Tonkin for their contributions to this Advisory.

Members of the Committee

Dr. Stephen Crocker has been appointed to chair the Security and Stability Advisory Committee. Dave Piscitello has been appointed Fellow to the Committee.

Alain Aina, Consultant

Jaap Akkerhuis, NLnet Labs

KC Claffy, CAIDA

Patrik Fältström, Cisco Systems

Johan Ihrén, Autonomica

Rodney Joffe, UltraDNS

Olaf Kolkman, NL NetLabs

Mark Kosters, Verisign

Allison Mankin, Consultant

Ram Mohan, Afilias

Russ Mundy, SPARTA, Inc

Frederico Neves, registro.br

Jon Peterson, NeuStar

Ray Plzak, ARIN

Mike St. Johns, Nominum

Doron Shikmoni, ForeScout, ISOC-IL

Bruce Tonkin, Melbourne IT; Chairman, Generic Names Supporting Organization

Paul Vixie, ISC

Suzanne Woolf, ISC

Support for the committee is provided by Jim Galvin (eList eXpress).