SSAC
ICANN Security and Stability Advisory Committee

Security and Stability Advisory Committee

Public Meeting

Marrakech

June 25, 2006

Unintended Consequences of Reuse of Lapsed Domain Names & Description of the Standing Panel of Experts

Agenda

- **Introduction**
  Steve Crocker, SSAC Chair
- **Renewal Considerations for Domain Name Registrants**
  Dave Piscitello, ICANN SSAC Fellow
- **Problems caused by the non-renewal of a domain name associated with a DNS Nameserver**
  Dave Piscitello, ICANN SSAC Fellow
- **Introducing the Standing Panel of Experts**
  Lyman Chapin, SPE Chair
- **SSAC Web Site Makeover**
  Steve Crocker, SSAC Chair
- **Public Questions and Answers**

SSAC

- Volunteer Committee of Experts
- Wide range of security and stability issues
  - Engineering stability
  - Traditional security analysis
  - Interactions between technology and market forces
- Provides Advice, not decisions
  - To the board
  - To the other parts of ICANN
  - To the broad Internet community

SSAC
ICANN Security and Stability Advisory Committee

Renewal Considerations for Domain Name Registrants

David Piscitello
dave.piscitello@icann.org

What are we talking about?

- Incidents where the expiry of a domain name registration had unanticipated consequences
  - In some cases, registrants inadvertently relinquished name
  - In some cases, registrants willingly relinquished name but did not anticipate the possible consequences
  - In all cases, the incidents occurred outside applicable redemption grace periods

Representative Incidents

- pack216.org (Cub Scout Pack in Virginia, US)
  - Registrant did not maintain accurate contact information
  - Registration for a cub scout pack web site expired
  - New registrant used as a referral link to pornographic web sites
- crisiscentersyr.org (counseling center in New York, US)
  - Organization merged with another counseling center
  - Domain name was not renewed
  - New registrant copied the center's home page and added referral links to pornographic web sites
- sigcat.org (Special Interest Group on CD/DVD Applications & Technology)
  - Domain name inadvertently allowed to expire
  - New registrant used as a referral link to pornographic web sites

Reputational Harm

- Embarrassment, tarnish of brand, and loss of reputation
  - for the previous domain holder
  - for any web site that had referral links to the domain name
- Avoiding these consequences is the primary consideration for many registrants

Commercial Considerations

- Many registrants do not realize that
  - A secondary market for domain names exists
  - Recurring revenue opportunities exist (e.g., domain name monetization)
  - Hyperlinks and other references to name may not work
  - Competitor can register the name (loss of business)
  - Unconnected company can register the name (consumer confusion)
- These considerations are often secondary to reputational harm for many registrants but may influence how registrants treat domain names
  - Risk and asset management

What the incidents reveal

- Many registrants do not realize that
  - Domain name registrations are temporary
  - Each domain name registration or renewal is an independent agreement between a registrar and registrant
  - Neither registrants nor registrars are obliged to notify third parties of the change in registration of a domain name
- Bad things happen when domain name registration records are not kept accurate
  - Registries and registrars cannot contact registrants regarding registration status
  - Operational (e.g., name service) issues may not be attended to in a timely manner

Findings

(1) The domain name registration process, and in particular, the renewal processes, are not always fully understood by parties who register domain names.

(2) Policies and processes currently in place may protect registrants for a grace period following the expiration of a domain name registration.

- If registrant does not renew the domain name it may be registered by another party
- A new registrant may use a domain name in a manner inconsistent with or in competition against a former registrant

Findings (continued)

(3) Incidents where registrants do not renew domain names, whether voluntarily or involuntarily (e.g., through oversight) can result in reputational harm.

(4) A secondary market for domain names exists today; in this market, nearly all domain names have (some) commercial value.

(5) Registrants should not allow a domain name to expire without investigating the commercial value of the name.

Recommendations

(1) Keep domain name registration information accurate.

- By keeping contact information accurate, registrants are less likely to fail to renew a domain name as a result of oversight.

(2) Establish a chain of accountability for domain name registration.

– Make certain that someone is responsible and accountable for renewing domain name registrations.

Recommendations (continued)

(3) Choose registrars and resellers carefully.

- Compare registration services offered by registrars
- Register domains with registrars who offer multi-year registrations and auto-renewal processes.
- Choose registrars who
  - send multiple renewal notices by email,
  - send renewal notices by postal mail,
  - offer extended grace periods, and who
  - offer a service to redeem domain names for the registrant from the registry during applicable grace periods.

Recommendations (Continued)

(4) Look for additional services.

– Some registrars offer safeguards to prevent domain names from being released without signed consent or other non-repudiable forms of authorization.

(5) Determine the reputational and commercial values of your domain.

(3) Consider options other than relinquishing a registered name.

- Most (if not all) canceled names are viable targets for re-registration.

Recommendations (continued)

(7) Begin any research on domain name valuation and complete domain name transactions well before your name is due for renewal.

- Registrants have a limited amount of time before the name is made available for registration to any other party.
- Allow sufficient time (at least 60 days) prior to expiration to conduct any research and complete any transactions prior to the expiry date of the domain registration.

SSAC
ICANN Security and Stability Advisory Committee

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

David Piscitello
dave.piscitello@icann.org

What are we talking about?

- Situations where one domain’s DNS name service is affected by changes in another domain name’s registration status

- Possible consequences
  - Name service for a domain is interrupted or unpredictable
  - DNS information is altered for malicious purposes
    - phishing attacks, email interception, and redirection of Internet users to different websites with different and possibly harmful content.

Relationship between Domain Name Registration and DNS Name Service

- When a domain name is registered, a registrar collects information about registrant, esp.
  - Contact information
  - **Domain names** of Name Servers that will be authoritative hosts for the registrant’s DNS records

Example Whois Registration Record

.

.

.

Domain Name: example.biz

Registrar: <…>

Administrative Contact: <…>

Technical Contact: <…>

.

.

.

Name Server: DNS1.example.biz

Name Server: DNS1.example.NET

Name Server: DNS1.exampleISP.NET

Bailiwick

- A registrant can support DNS name service from a system that is assigned a domain name from
  1. the **registered domain** (e.g., example.biz)
     - dns1.example.biz can support name service for example.biz
  2. **another of the registrant's domains** (e.g., example.net)
     - dns1.example.net can support name service for example.biz.
  3. a **domain registered by a different party**
     - e.g., the registrant's registrar/reseller, ISP, domain name hosting company or other trusted party
     - dns1.exampleisp.net can support name service for example.biz
- Configuration (1) is called an **in-bailiwick** DNS service
- Configurations (2) and (3) are called **out-of-bailiwick** DNS services

Assumptions made when out-of-bailiwick NS is used

- The domain from which the out-of-bailiwick name server is assigned a name will not expire
- The domain name remains registered to the same party with whom the registrant has arranged out-of-bailiwick name service, and
- If either of these conditions change, someone will notify the registrant
- In practice, these conditions may change

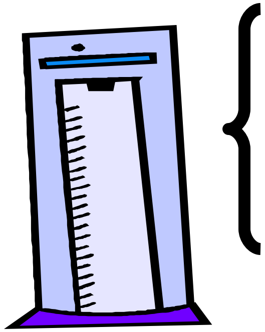
SCENARIO #1

One DNS Name Server, Out-of-Bailiwick

Registration Record
Registrant: JANE DOE
Domain Name: FOO.TLD
Registrar: <…>
Administrative Contact: <…>
Technical Contact: <…>
.
.
.
Name Server: DNS1.BAR.TLD

Registration Record
Registrant: FRED ISP
Domain Name: BAR.TLD
Registrar: <…>
Administrative Contact: <…>
Technical Contact: <…>
.
.
.
Name Server: DNS1.BAR.TLD

JANE DOE ARRANGES FOR FRED ISP TO HOST DNS RECORDS ON DNS1.BAR.TLD



WWW.FOO.TLD A 10.0.0.5
FTP.FOOT.TLD A 10.0.0.9

DNS1.BAR.TLD

SCENARIO #1

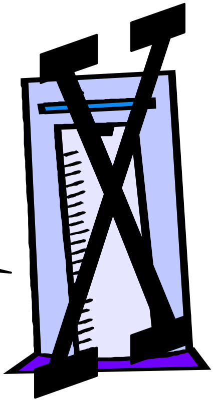
Impact of Non-renewal of BAR.TLD

Registration Record
Registrant: JANE DOE
Domain Name: FOO.TLD
Registrar: <…>
Administrative Contact: <…>
Technical Contact: <…>
.
.
.
Name Server: DNS1.BAR.TLD

Registration Record
Registrant: FRED ISP
Domain Name: BAR.TLD
Registrar: <…>
Administrative Contact: <…>
Technical Contact: <…>
.
.
.
Name Server: DNS1.BAR.TLD

DELETED

DELEGATION IS LAME
DNS1.BAR.TLD
DOES NOT EXIST



DNS1.BAR.TLD

CONSEQUENCE:

NAME SERVICE FOR FOO.TLD IS INTERRUPTED

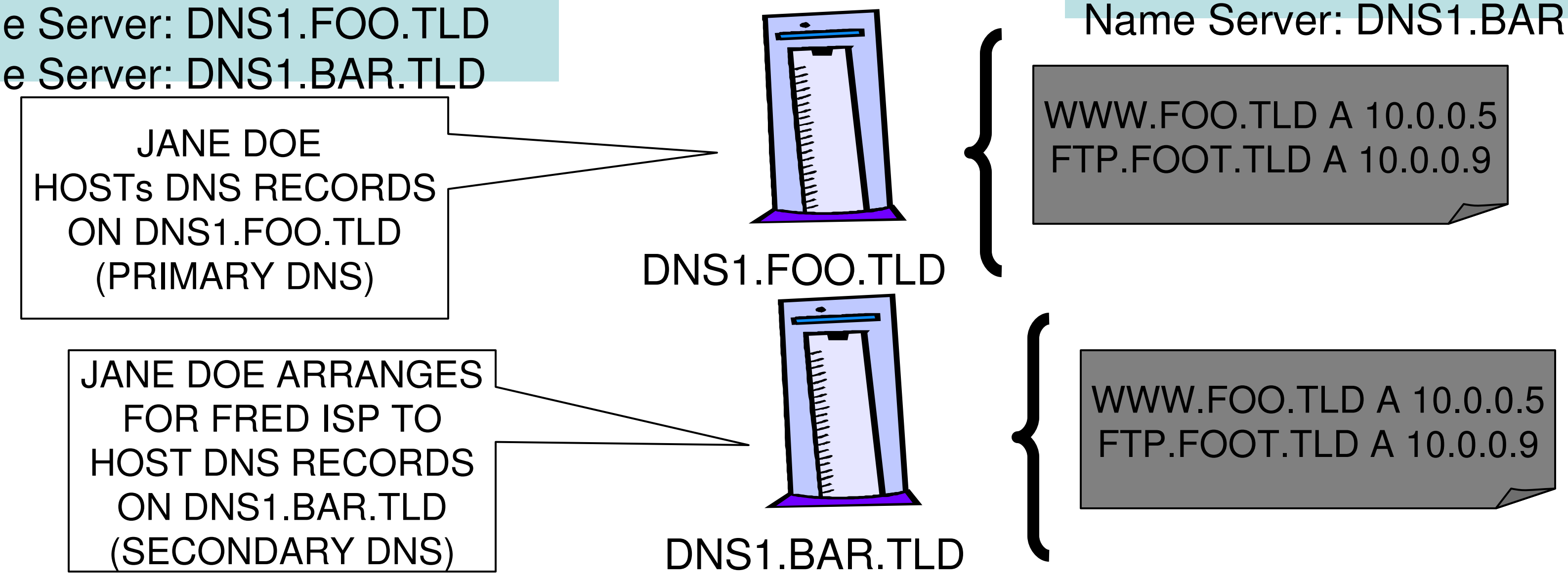
SSAC
ICANN Security and Stability Advisory Committee

SCENARIO #2

Out-of-Bailiwick DS Name Server for Redundancy

Registration Record
Registrant: JANE DOE
Domain Name: FOO.TLD
Registrar: <…>
Administrative Contact: <…>
Technical Contact: <…>
.
.
.
Name Server: DNS1.FOO.TLD
Name Server: DNS1.BAR.TLD

Registration Record
Registrant: FRED ISP
Domain Name: BAR.TLD
Registrar: <…>
Administrative Contact: <…>
Technical Contact: <…>
.
.
.
Name Server: DNS1.BAR.TLD



JANE DOE
HOSTs DNS RECORDS
ON DNS1.FOO.TLD
(PRIMARY DNS)

JANE DOE ARRANGES
FOR FRED ISP TO
HOST DNS RECORDS
ON DNS1.BAR.TLD
(SECONDARY DNS)

SCENARIO #2

Impact of Non-renewal of BAR.TLD

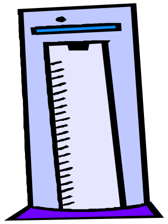
Registration Record
Registrant: JANE DOE
Domain Name: FOO.TLD
Registrar: <…>
Administrative Contact: <…>
Technical Contact: <…>
.
.
.
Name Server: DNS1.BAR.TLD

Registration Record
Registrant: FRED ISP
Domain Name: BAR.TLD
Registrar: <…>
Administrative Contact: <…>
Technical Contact: <…>
.
.
.
Name Server: DNS1.BAR.TLD

DELETED

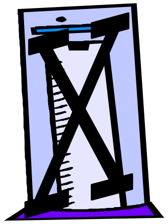
IN-BAILIWICK NS
REMAINS OPERATIONAL

DELEGATION IS LAME
DNS1.BAR.TLD
DOES NOT EXIST



DNS1.FOO.TLD

WWW.FOO.TLD A 10.0.0.5
FTP.FOOT.TLD A 10.0.0.9



DNS1.BAR.TLD

CONSEQUENCE:

NAME SERVICE FOR FOO.TLD IS UNPREDICTABLE

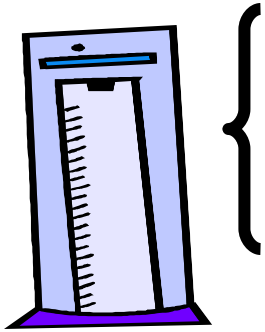
SSAC
ICANN Security and Stability Advisory Committee

SCENARIO #3
(As depicted, same as #1, but could be #2)

Registration Record
Registrant: JANE DOE
Domain Name: FOO.TLD
Registrar: <…>
Administrative Contact: <…>
Technical Contact: <…>
.
.
.
Name Server: DNS1.BAR.TLD

Registration Record
Registrant: FRED ISP
Domain Name: BAR.TLD
Registrar: <…>
Administrative Contact: <…>
Technical Contact: <…>
.
.
.
Name Server: DNS1.BAR.TLD

JANE DOE ARRANGES FOR FRED ISP TO HOST DNS RECORDS ON DNS1.BAR.TLD



WWW.FOO.TLD A 10.0.0.5
FTP.FOOT.TLD A 10.0.0.9

DNS1.BAR.TLD

SCENARIO #3

BAR.TLD not renewed, registered by bad actor

Registration Record
Registrant: JANE DOE
Domain Name: FOO.TLD
Registrar: <…>
Administrative Contact: <…>
Technical Contact: <…>
.
.
.
Name Server: DNS1.BAR.TLD

Registration Record
Registrant: FRED ISP
Domain Name: BAR.TLD
Registrar: <…>
Administrative Contact: <…>
Technical Contact: <…>
.
.
.
Name Server: DNS1.BAR.TLD

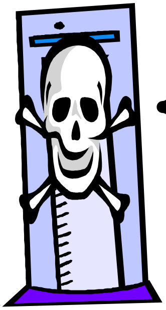
DELETED

Registration Record
Registrant: BADACTOR
Domain Name: BAR.TLD
Registrar: <…>
Administrative Contact: <…>
Technical Contact: <…>
.
.
.
Name Server: DNS1.BAR.TLD

FRED ISP DOES NOT RENEW BAR.TLD

ATTACKER REGISTERS BAR.TLD

ATTACKER ALTERS DNS RECORDS OF FOO.TLD



DNS1.BAR.TLD

```
WWW.FOO.TLD A 192.168.0.5
FTP.FOO.TLD A 192.168.0.9
```

CONSEQUENCE:

FOO.TLD IS PHISHING PHODDER

Remedies

- Registrant actions:
  - identify a party in your own organization who is responsible for coordinating 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
  - actively monitor name service to verify that name resolution is accurate for all DNS records at all authoritative name servers (whether in- or out-of-bailiwick)

Accurate Registration Information can help

- If accurate contact and name server information is available, registrars and resellers could:
  - Remind to technical contacts to verify DNS configuration and name server information in the registration record
  - Warn registrants that the domain name registration record contains incorrect name server information
  - Monitor name service for domains in the Registry and intervene when it detects an incorrect DNS configuration
    - Delete a lame delegation
    - Block what appears to be maliciously altered delegation

Findings

(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 name from out-of-bailiwick domains.

(2) Domain name registrations are not permanent, and may not be renewed.

Findings (continued)

(3) Registrants put name service operation at risk of interruption if they do not provide accurate contact information for registries and registrars.

(4) Registrants put name service at risk of interruption when domain names on which the name service depends are not renewed and subsequently deleted by a Registry.

(5) Registrants expose their domains to redirection attacks when domain names on which name service depends are not renewed and subsequently registered by a party with malicious intentions.

Recommendations

(1) Maintain accurate contact information in domain name registration records.

(2) Establish a chain of accountability for domain name registration.

(3) Maintain accurate contact information for all registrants of domain names with whom you have arranged to host your domain zone files.

(4) Monitor your domain name service. Registrants should actively monitor domain name servers that host their domain name zone files to verify that all name servers are providing accurate domain name information.

(5) Use DNSSEC to protect against undetected modification of DNS records.