The Wild Card Incident of 9/15/2003

Steve Crocker Chair
Security and Stability Advisory Committee
Primary Security and Stability
ICANN Components

- Constituent Participatory Organizations
  - Generic Names Supporting Organization
  - Country Code Names Supporting Organization
  - Government Advisory Council
    - 80 countries and 5 treaty organizations
  - Root Server Advisory Committee

- Specialist Groups
  - IANA
    - Administers root database and address allocation
  - Security and Stability Advisory Committee
    - Volunteer experts on security and stability issues
SECSAC Committee

- Steve Crocker, Chair
- Alain Patrick Aina
- Jaap Akkerhuis
- Doug Barton
- Steven M. Bellovin
- Rob Blokzijl
- David R. Conrad
- Johan Ihren
- Mark Kosters
- Allison Mankin
- Ram Mohan
- Russ Mundy
- Jun Murai
- Frederico A.C. Neves
- Ray Plzak
- Doron Shikmoni
- Ken Silva
- Bruce Tonkin
- Paul Vixie
- Rick Wesson

Staff support: Jim Galvin
SECSAC Committee Strengths

- Root Server Operators
- gTLD Operators
- ccTLD Operators
- Name Space Registries
- Regional Internet Registries (RIRs)
- Registrars
- Internet Security

No policy or political members(!)
On Sept 15, VeriSign introduced change to .com and .net domain

Redirected unassigned names to their own server (SiteFinder)

Immediate complaints and problem reports

Several actions, including SECSAC
SECSAC Involvement

- Advisory issued 9/22
- Public inputs
  - secsac-comment@icann.org
- Public meetings 10/7 & 10/15
- More public inputs
- Report will come toward end of November
SECSAC in the larger process

- SECSAC is an advisory committee
  - We only speak. We don’t decide or enforce. Others may choose to listen.
  - ICANN management will deliberate and choose path following our report.
- Focus on Security and Stability
  - Not competition, etc.
  - But may include large issues
What Happened

- VeriSign used the wild card feature to redirect all uninstantiated names to their own servers
  - Previously, returned standard error code
  - This was a change to an existing service
- Some things broke
- Some took defensive action
Registries, Registrars, and Registrants

- End user requests add/modify/delete
- Registrar submits add/modify/delete to registry
- Registry updates zone
- Master updated
- Slaves updated

Diagram:

- Registry
- Zone DB
- Registrar
- Registrants
Name Resolution

Name resolution is the process by which resolvers and name servers cooperate to find data in the name space.

To find information anywhere in the name space, a name server only needs the names and IP addresses of the name servers for the root zone (the “root name servers”).
Name Resolution

- A name server receiving a query from a resolver looks for the answer in its authoritative data first and then in its cache.
  - If it doesn’t have the requested data and is not authoritative for the domain in the query, other servers must be consulted.
Name Resolution Example

- Let’s look at the resolution process step-by-step:

Name Resolution Example

The workstation *annie* asks its configured name server, *dakota*, for *www.nominum.com*’s address.

Name Resolution Example

The name server *dakota* asks a root name server, *m*, for *www.nominum.com*’s address.

What’s the IP address of *www.nominum.com*?

*ping www.nominum.com.*
Name Resolution Example

The root server \textit{m} refers \textit{dakota} to the \textit{com} name servers.

- This type of response is called a “referral”.

Here’s a list of the com name servers. Ask one of them.

- \texttt{dakota.west.sprockets.com}
- \texttt{m.root-servers.net}
- \texttt{annie.west.sprockets.com}

\texttt{ping www.nominum.com.}
Name Resolution Example

The name server *dakota* asks a *com* name server, *f*, for *www.nominum.com*’s address.

What’s the IP address of *www.nominum.com*?

ping *www.nominum.com*. 

---

*annie.west.sprockets.com* 

*dakota.west.sprockets.com* 

*f.gtld-servers.net* 

*m.root-servers.net*
Name Resolution Example

The *com* name server *f* refers *dakota* to the *nominum.com* name servers

If the Name doesn’t exist


Here’s the address of www.nnominum.com
Name Resolution Example

The name server *dakota* asks a *nominum.com* name server, *ns1.sanjose*, for *www.nominum.com*’s address.

What’s the IP address of *www.nominum.com*?

*ping www.nominum.com.*
Name Resolution Example

The nominum.com name server ns1.sanjose responds with www.nominum.com’s address.

Name Resolution Example

Here’s the IP address for www.nominum.com.

Broad Areas of Concern

- Abruptness
  - No notice or community involvement
  - But internal and private testing
  - Is it the right thing?
    - Changes in the core vs innovation
    - Lots more to say
- Competition
  - Not our concern; belongs elsewhere
Initial Advisory

- VeriSign: Please roll back
- Tech Community: Please clarify specs
  - IETF, IAB, network and DNS operators
- ICANN: Please clarify procedures
<table>
<thead>
<tr>
<th>Time</th>
<th>Session</th>
<th>Presenter</th>
</tr>
</thead>
<tbody>
<tr>
<td>10:00</td>
<td>Welcome</td>
<td>Arnaud de Borchgrave, Steve Crocker</td>
</tr>
<tr>
<td>10:20</td>
<td>VeriSign Site Finder</td>
<td>Scott Hollenbeck</td>
</tr>
<tr>
<td>11:00</td>
<td>What was affected</td>
<td>David Shairer</td>
</tr>
<tr>
<td>11:30</td>
<td>Community Tech Responses</td>
<td>Paul Vixie</td>
</tr>
<tr>
<td>12:00</td>
<td>Information Flow</td>
<td>Richard M. Smith</td>
</tr>
<tr>
<td>12:30</td>
<td>LUNCH</td>
<td></td>
</tr>
<tr>
<td>2:00</td>
<td>Protocol Problems and</td>
<td>Steven M. Bellovin</td>
</tr>
<tr>
<td></td>
<td>Architectural Issues</td>
<td></td>
</tr>
<tr>
<td>2:30</td>
<td>Internet Protocols and</td>
<td>John C. Klensin</td>
</tr>
<tr>
<td></td>
<td>Innovation</td>
<td></td>
</tr>
<tr>
<td>3:00</td>
<td>Other Issues; Open Session</td>
<td></td>
</tr>
<tr>
<td>3:30</td>
<td>Next Steps</td>
<td>Steve Crocker</td>
</tr>
<tr>
<td>4:00</td>
<td>Adjourn</td>
<td></td>
</tr>
<tr>
<td>Time</td>
<td>Agenda Item</td>
<td>Presenter</td>
</tr>
<tr>
<td>-------</td>
<td>-------------------------------------------------</td>
<td>----------------------------------------</td>
</tr>
<tr>
<td>1:00</td>
<td>Welcome</td>
<td>Steve Crocker</td>
</tr>
<tr>
<td>1:15</td>
<td>VeriSign Business Overview of Site Finder</td>
<td>Anthony Renzette</td>
</tr>
<tr>
<td>1:45</td>
<td>Technical Review Panel Summary</td>
<td>Scott Hollenbeck</td>
</tr>
<tr>
<td>2:15</td>
<td>Technical Issues and VRSN Responses</td>
<td>Matt Larson</td>
</tr>
<tr>
<td>2:45</td>
<td>Usability Market Research</td>
<td>Ben Turner</td>
</tr>
<tr>
<td>3:15</td>
<td>Next Steps</td>
<td>Chuck Gomes</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Rusty Lewis</td>
</tr>
<tr>
<td>3:30</td>
<td>BREAK</td>
<td></td>
</tr>
<tr>
<td>3:45</td>
<td>Measuring ISP Responses to SiteFinder</td>
<td>Benjamin Edelman</td>
</tr>
<tr>
<td>4:15</td>
<td>Global Name Registry Statement</td>
<td>Hakon Haugnes</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Geir Rasmussen</td>
</tr>
<tr>
<td>4:30</td>
<td>Other Issues; Open Session</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Steve Crocker</td>
</tr>
</tbody>
</table>
Tentative Issues

- Abruptness
- Rightness
- Systemic Stability
- Confidence
- Technical Clarity
- Process Clarity

- Displaced Costs
- Innovation at core vs edge
- Future architecture
- Role of standards
- Existing wild card use
  - .museum, .name, etc
Next Steps

- More Public Input
  - Secsac-comment@icann.org
- Report
- ICANN and others will follow through