Redirection in the COM and NET Domains

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

9 July 2004

Table of Contents

Preface and Acknowledgements

This is a report by the Security and Stability Advisory Committee (SSAC)[1] describing a sequence of actions undertaken by VeriSign, Inc. in September and October 2003, the reactions of the Internet technical community and the implications of the chain of events for the security and stability of the Internet. Formed in the wake of the events of September 11, 2001, SSAC is an advisory committee to ICANN (the Internet Corporation for Assigned Names and Numbers) that reports directly to the ICANN Board and advises "the ICANN community and Board on matters relating to the security and integrity of the Internet's naming and address allocation systems" (Appendix 1). As an advisory committee, the Committee offers 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. The Committee 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 Committee's membership draws from the commercial and not-for-profit sectors, has broad geographic representation and has broad representation across industry and academe (Appendix 1), including all segments of the domain name system (DNS) community. We have members who operate root servers, top-level domain servers (both generic and country code), registrars and address registries. Some of our members are network security experts or conduct network security research. The Committee is composed of volunteers, who serve without pay, each a technical contributor in his or her own organization and in the community at large.

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. In the current activity, several members work for VeriSign or for companies doing business with VeriSign or work for companies competing with VeriSign. In all cases, the members have made their situations clear and have been careful to provide technical information without attempting to influence others on the Committee. SSAC's policy concerning conflict of interest is posted to the committee's Web site.[2] Biographies and declarations of potential sources of conflict of interest are included in Appendix 2.

Like any such effort, preparing this report owes much to many:

- Two public meetings were held and chaired by Stephen Crocker in Washington, D.C. on 7 October 2003 and 15 October 2003. We are grateful for the venues and logistical support provided by the Center for Strategic and International Studies (CSIS) and the Academy for Educational Development and their staffs. Arnaud

[1] http://ssac.icann.org/. The Committee's acronym was originally SECSAC. It has been changed to SSAC.
[2] http://ssac.icann.org/conflict-of-interest.htm

de Borchgrave, Senior Adviser and Director at CSIS, hosted the CSIS meeting on 7 October and gave the welcoming talk.

- Both meetings benefited from considerable organizational help provided by Marilyn Cade of AT&T, Elana Broitman of Register.com and Carla LaFever of MCI. Laura Brewer, Theresa Darrenougue, Kathy Robson and Deanna Baker of Realtime Reporting & Captioning provided transcription services, and Steve Conte and John Crain supplied network support.
- Paul Ott and Ari Elias-Bachrach ordered and analyzed the comments received on "secsac-comment" (now called “ssac-comment").
- Fourteen speakers offered analysis and made presentations at these meetings: Steven Bellovin, AT&T; Benjamin Edelman, Harvard University; Charles Gomes, VeriSign; Hakon Haugnes, Global Name Registry; Scott Hollenbeck, VeriSign (7 and 15 October 2003); John Klensin, John C. Klensin and Associates; Matt Larson, VeriSign; Russell Lewis, VeriSign; Geir Rasmussen, Global Name Registry; Anthony Renzette, VeriSign; David Schairer, XO Communications; Richard Smith, privacy consultant; Ben Turner, VeriSign; Paul Vixie, ISC. kc claffy also made substantial contributions as did Mike St. Johns and Suzanne Woolf. James Galvin, Principal at eList eXpress, provided continuous staff support to the Committee during the process.
- ICANN's At-Large Advisory Committee (ALAC) organized a public briefing and discussion on wildcard services on 27 October 2003 in Carthage, Tunis, in conjunction with ICANN's quarterly meeting, supported an online forum, and provided analysis of user responses.
- Many people attended or listened in on the meetings where they offered thoughtful comments and observations. Many more participated in the online discussions. To list them all would overwhelm this document, so however inadequately, the Committee offers its blanket thanks to the community.

Douglas Maughan, Cyber Security Program Manager at HSARPA, U.S. Department of Homeland Security, and SRI, International provided partial financial support for preparation of this report under Contract No. 61-00273. We are grateful to Victoria Stavridou, Steven Cheung and Lori Truitt of SRI for their assistance. Additional support for report production and distribution has been provided by ICANN; we are particularly indebted to Tanzanica King for her help in design and layout.

This report was written and edited by Stephen Crocker and Amy Friedlander under the direction of the Committee, which has complete responsibility for the work, its content and its recommendations.

Executive Summary

On 15 September 2003, VeriSign, Inc. changed the way that NET and COM registries responded to lookups on nonexistent -- or uninstantiated -- domain names. In so doing, the company changed the way that the domain name system (DNS), a fundamental component of the Internet architecture, provides services for two large top-level domains. VeriSign's action was aimed at the World Wide Web but had unexpected effects on the other parts of the Internet. VeriSign refers to this set of changes as the introduction of its Site Finder service, focusing attention on the functionality provided to Web users who mistyped domain names and were routed to VeriSign's servers. The specific technical change substituted a "synthesized response" for an error message, and applications that relied on the original error code unexpectedly failed. At ICANN's insistence and after widespread protest from the technical community, VeriSign suspended the Site Finder service on 4 October 2003.

This report by the Security and Stability Advisory Committee (SSAC), an advisory committee to ICANN, describes VeriSign's actions of September-October 2003 and the technical community's responses to those actions and then analyzes the sequence of actions and reactions from the perspective of security and stability of the Internet. The Committee then presents its findings and recommendations. The Committee's primary focus is not Site Finder, per se. Rather, our focus is two-fold: that core registry operations were modified, thereby changing existing services, and that the change was introduced abruptly without broad notice, testing, refinement or community agreement.

The Committee finds that VeriSign's actions did not have network-shattering effects but did violate fundamental architectural principles and well-established codes of conduct and good practice intended to ensure stability. Users' decisions and control were preempted and users were potentially subjected to violations of their privacy. Local responses, patches and work-arounds reduced overall coherence. Services that had been functioning satisfactorily were disturbed and the direct and indirect costs of these disruptions were imposed on third parties. Specifically:

Finding (1): VeriSign introduced changes to the NET and COM registries that disturbed a set of existing services that had been functioning satisfactorily. Names that were mistyped, had lapsed, had been registered but not delegated, or had never been registered in DNS were resolved as if they existed. As a consequence, certain e-mail systems, spam filters and other services failed resulting in direct and indirect costs to third parties, either in the form of increased network charges for some classes of users, a reduction in performance, or the creation of work required to compensate for the consequent failure.

Finding (2): The changes violated fundamental Internet engineering principles by blurring the well-defined boundary between architectural layers. VeriSign targeted the Site Finder service at Web browsers, using the HTTP protocol, whereas the DNS protocol, in fact, makes no assumptions – and is neutral – regarding the protocols of the queries to it. As a consequence, VeriSign directed traffic operating under many protocols

to the Site Finder service for further action, and thus, more control was moved toward the center and away from the periphery, violating the long-held end-to-end design principle.

Finding (3): The mechanisms proposed by VeriSign to ameliorate the undesirable effects of their diversion on protocols other than HTTP put VeriSign in the implementation path of every existing and future protocol that uses DNS. For every such protocol, it would be necessary to consult with VeriSign to figure out how to simulate the response of the protocol to "no such domain." This is an unacceptable invasion of clear layering.

Finding (4): Despite a long period of internal research and development, the system was brought out abruptly. The abruptness of the change violated accepted codes of conduct that called for public review, comment and testing of changes to core systems; this process exists to ensure that changes are introduced with minimal disruption to existing services and hence with minimal disruption to the security and stability of the Internet. It also precluded the possibility that administrators, IT departments, ISPs and other intermediaries on whom end users rely might be adequately prepared to deal with the consequences.

Finding (5): In response, workarounds and patches were introduced quickly, cumulatively reducing the overall coherence of the system and again violating the established practices of public evaluation, testing, discussion and review before core services are implemented and deployed. These workarounds further blurred the functional layers intrinsic to the Internet's robust architecture and in some instances created additional -- and unintended -- harmful effects.

Finding (6): Information about intended e-mail senders and receivers was necessarily accepted by VeriSign's servers without the knowledge or consent of either sender or receiver. VeriSign strenuously denied retaining this information.

Finding (7): The behavior of end users redirected to the Web site was observed by a program embedded in the Site Finder service, and users could neither accept it, reject it nor substitute another, similar service for it.

Finding (8): The cycles of changes and responses collectively undermined expectations about reliable behavior and in so doing reduced trust in the security and stability of the system.

On the basis of these findings, the Committee makes the following recommendations:

Recommendation (1): Synthesized responses should not be introduced into top-level domains (TLDs) or zones that serve the public, whose contents are primarily delegations and glue, and where delegations cross organizational boundaries over which the operator may have little control or influence. Although the wildcard mechanism for providing a default answer in response to DNS queries for uninstantiated names is documented in the defining RFCs (Requests for Comment), it was generally intended to be used only in narrow contexts (for example, MX records for e-mail applications), generally within a single enterprise, and is currently used in top-level domains that are generally small and well-organized.

Recommendation (2): Existing use of synthesized responses should be phased out in TLDs or zones that serve the public, whose contents are primarily delegations and glue, and where delegations cross organizational boundaries.

Recommendation (3): There exist shortcomings in the specification of DNS wildcards and their usage. The defining RFCs should be examined and modified as necessary with a focus on producing two results: first, clarification of the use of synthesized responses in DNS protocols; second, provision of additional guidance on the use of synthesized responses in the DNS hierarchy.

Recommendation (4): Changes in registry services should take place only after a substantial period of notice, comment and consensus involving both the technical community and the larger user community. This process must (i) consider issues of security and stability, (ii) afford ample time for testing and refinement and (iii) allow for adequate notice and coordination with affected and potentially affected system managers and end users. Thirty years of experience show that this strategy ensures robust engineering and engenders trust in the systems and the processes surrounding their maintenance and development.

1.0 Introduction

On 15 September 2003, VeriSign, Inc. changed the way that NET and COM registries responded to lookups on nonexistent -- or uninstantiated -- domain names. In so doing, the company changed the way that the domain name system (DNS), a fundamental component of the Internet architecture, provides service for two large top-level domains. VeriSign's actions consisted of a period of private research followed by a launch of service on 15 September 2003. The changes in service were aimed at the World Wide Web but had unexpected effects on the other parts of the Internet. VeriSign refers to this set of changes as the introduction of its Site Finder service, focusing attention on the functionality provided to Web users who mistyped domain names and were routed to VeriSign's servers. However, the effects rippled through multiple communities who depend upon predictable operation of the Internet including registrars, registrants, system administrators, Internet service providers (ISPs) and, most specifically, end users. Outcry from the technical community, which is described in more detail in Section 2.1, as well as formal communications prepared by the Internet Architecture Board (IAB) and the ICANN Security and Stability Advisory Committee (SSAC), identified a series of issues arising from VeriSign's action and the reaction to it that affected security and stability.

The scope of this report is to review the findings of the public meetings held on 7 October and 15 October 2003 as well as other information that surfaced from the Internet technical community, and on the basis of that review to make recommendations to ICANN. Since the Committee's mandate is focused on issues of security and stability, our principal focus has been to understand the implications of VeriSign's action from the perspective of security and stability of the Internet. Inevitably, examination of VeriSign's use of redirection in the COM and NET domains also calls attention to pre-existing use of the same mechanism in the several other, vastly smaller domains, and our findings and recommendations address these domains as well. Our primary focus is not Site Finder, per se. Rather, our focus is two-fold: that core registry operations were modified, thereby changing existing services, and that the change was introduced abruptly without broad notice, testing, refinement or community agreement. Since our concern here is on both the change itself and the method of introducing the change, we refer to both with the terse shorthand "VeriSign's action."

VeriSign took the position that its action was compliant with protocol specifications and therefore did not affect security and stability of the Internet; VeriSign's presentation and input are summarized in Section 2.2 of this report. However, as SSAC's 22 September 2003 message to ICANN observes, "Security and stability [are] not limited to a narrow interpretation of the technical specifications of the protocol documents; it also includes engineering, operational, business, and policy issues" (Appendix 3). During the development of the Internet over the last 30 years, the technical community has grappled with the tension between regulating infrastructure services on behalf of the public and promoting competition among the private sector interests who provide these services. These relationships derive from three sets of policy considerations: technological innovation, economic competition and reliable infrastructure service. Within the framework of this report, Sections 2.3 and 2.4 present discussions of how technology and organization have intertwined in the development of protocols, codes of conduct and good practice to build a robust Internet. Section 2.5 summarizes the technical issues. Section 3 presents findings and recommendations.

Ultimately, the matter is one of fostering and sustaining trust. Most Web and e-mail end users have seen error messages when a name fails to resolve. These error messages usually come either as a Web page displayed on their browsers, perhaps supported by a well-known search service, or as a bounced message in their e-mail in-boxes. And many, if not most, end users know the rough contours of the explanation: That the name is supposed to correspond to a sequence of numbers that represent an address and that the registry databases maintain the relationship between the name and the address. The sophistication of the addressing system and the complexities of how this communication actually works across a range of heterogeneous platforms, devices and networks are typically and intentionally hidden (that is, the typical user does not see all of the steps in the transmission). Most users outside the technical communities rely on intermediary services, such as Internet Service Providers and technical support units in their organizations, to keep their systems up and running.[3] For the public, information technology systems require trust: “They [the systems] must do what they are required to do -- and nothing else.”[4]

[3] Systems administrators can run traces on the system to assess performance and identify errors so the system is both seamless and transparent.

[4] Computer Science and Telecommunications Board, National Research Council, *Making IT Better: Expanding Information Technology Research to Meet Society’s Needs* (Washington, DC: National Academy Press, 2000), p. 114.

2.0 Summary of Events and Issues Raised by the Internet Technical Community

This section describes the events of September-October 2003; presents a brief summary of VeriSign's Site Finder; provides an overview of Internet design principles, naming, IP (Internet Protocol) addresses and wildcards; and offers an analysis of the issues that the Internet technical community raised.

2.1 Events of September – October 2003

VeriSign, Inc.'s corporate Web pages describe the company's products and services. According to the company's Web page, VeriSign's COM NET Registry "is the authoritative registry for .com and .net domain names and supports registrars who offer these registrations to their customers." VeriSign's COM NET Registry "manages relationships with more than 100 ICANN-accredited Registrars who submit over 100 million domain name transactions daily" (Key terms and concepts will be described hereafter in section 2.3.).[5] On 15 September 2003, VeriSign changed the way the COM and NET registries responded when presented with uninstantiated names.

Names might be uninstantiated for one of several reasons: A name might not exist because it had been misspelled, had lapsed or had never been registered. A name might also be registered or reserved but not included in the lookup database used for domain name queries. In these instances, instead of returning the standard error code, the name server responded with the address of one of VeriSign's servers. Web browsers were directed to a site called SiteFinder.com; everything else either failed or, as in the case of mail, behaved in ways unexpected by the sender.

News of VeriSign's action was reported in the Wall Street Journal (5 September 2003) and Computer Business Review (9 September 2003) before the actual release, and on the day itself by the New York Times (15 September 2003). The action was characterized in the press as a potentially highly lucrative business venture that affected Web users. "VeriSign Mulls Way to Make Money from Typos" read the headline in Computer Business Review. And the story began, "VeriSign Inc. is testing changes to its domain name system services, which could generate tens of millions in revenue a year for itself and partners, and which would impact the way almost every internet user surfs the web."[6]

Although the press carried these very brief descriptions of VeriSign's action a few days prior to its introduction, there was no discernible reaction until the launch of Site Finder on 15 September. Moreover, such reportage in the largely mainstream press hardly conforms to the process of review and comment to which the Internet technical community is accustomed within the framework of the Internet Engineering Task Force

[5] Naming and Directory Services, VeriSign COM NET Registry; http://www.VeriSign.com/nds/naming/registrar/index.html?sl=070406; verified 21 April 2004.

[6] Kevin Murphy, VeriSign Mulls Ways to Make Money from Typos, Computer Business Review Online, 9 September 2003, http://www.cbronline.com/cbr_archive/d04afc52ae9da2ee80256d9c0018be8b; verified 6 July 2004.

(IETF). Indeed, after the launch, the technical community to VeriSign's change responded swiftly in both informal expressions within the community on various mailing lists and in formal communications to ICANN.[7] By 7 October, 13 formal letters and messages objecting to Site Finder from individuals and organizations around the world, ranging from AT&T to the Museum Domain Management Association, had been sent to ICANN.[8] A petition to ICANN garnered approximately 18,000 signatures, and 220 messages were sent to ICANN's wildcard-comments address between 27 September and 9 October 2003, three days after VeriSign disconnected the Site Finder service. By 19 October, comments to ICANN totaled 330. An analysis of the comments received by 9 October cited specific problems with the network, patches, user interfaces, e-mail, link checkers, configurations that rely on detecting that a domain name that is not registered and non HTTP/SMTP protocols. The problems clustered into four broad topics: trust, registration, "Things Break" and user services and choice. In the analyses that followed, the topics raised by the broad technical community have consistently recurred.[9]

On 19 September 2003, four days after the release of SiteFinder.com, ICANN issued its first advisory requesting VeriSign suspend the service voluntarily given concerns that had been expressed about the threat that VeriSign's actions posed to security and stability. VeriSign declined to do so in a communication dated 21 September 2003, arguing that such action was "premature," absent collection and review of available data. On 3 October and following preliminary communications by SSAC and the Internet Architecture Board (IAB), ICANN more forcefully demanded that VeriSign suspend "the changes to the .com and .net top-level domains introduced on 15 September 2003 by 6:00 PM PDT on 4 October 2003."[10] On the same day that the letter was sent to VeriSign, ICANN also issued a public advisory, noting widespread concern expressed about the implications of the changes for the security and stability of the Internet, stating:

> For all these reasons, ICANN has today insisted that VeriSign suspend the Site Finder service, and restore the .com and .net top-level domains to the way they were operated prior to 15 September 2003. If VeriSign does not comply with this demand by 6:00 PM PDT on 4 October 2003, ICANN will be forced to take the steps necessary to enforce VeriSign's contractual obligations.[11]

Despite its objections, VeriSign complied. The service has been suspended, ostensibly temporarily, and the matter remains unresolved. Relevant correspondence is included as Appendix 4.

[7] VeriSign's Wildcard Service Deployment, Internet Community Comments; http://www.icann.org/topics/wildcard-history.html; verified 21 April 2004.

[8] Internet Community Comments, Ibid.; verified 21 June 2004.

[9] Thomas Roessler, SiteFinder: Community Comments, At-Large Advisory Committee, Carthage, October 2003; http://www.icann.org/presentations/roessler-wildcard-carthage-27oct03.pdf; verified 22 May 2004.

[10] Letter from Paul Twomey to Russell Lewis, 3 October 2003; http://www.icann.org/correspondence/twomey-to-lewis-03oct03.htm; verified 22 May 2004; included in Appendix 3.

[11] Advisory, 03 October 2003; http://www.icann.org/announcements/advisory-03oct03.htm; verified 22 May 2004; included in Appendix 3.

As of 4 October, the suspension was characterized as "temporary, pending full review of the technical issues by IAB and SSAC."[12] On 22 September, SSAC had issued a preliminary statement as a first step in its examination of this situation (Appendix 3). In this document, the Committee outlined a series of considerations:

- Conformance with the protocol specifications as defined by the engineering community.
- Conformance with accepted best practices and operational procedures as defined by the engineering and operational communities.
- Consideration of the technical stability and security of the domain name system and the Internet as a whole in light of the both the change introduced by VeriSign and the corresponding changes being introduced by others.
- Current procedural and governance controls to assure review and analysis of changes to the critical components of the Internet.
- Public confidence in the stability and reliable operation of the Internet.

The Committee continued, "VeriSign's change appears to have considerably weakened the stability of the Internet, introduced ambiguous and inaccurate responses in the DNS, and has caused an escalating chain reaction of measures and countermeasures that contribute to further instability."[13]

The Committee then called for inputs and held an open meeting on Tuesday, 7 October 2003, in Washington, D.C. at which there were presentations from industry representatives as well as opportunities for questions. A second meeting was scheduled on Wednesday, 15 October 2003, also in Washington, D.C., to provide VeriSign with an extended period of time to present information and research it had developed in reference to its service. Representatives from VeriSign offered a vigorous explanation of its actions. Both meetings were Web cast and questions taken from remote participants by telephone and e-mail. Transcripts and presentations for both meetings are available at http://ssac.icann.org/.

2.2 VeriSign's Presentation and Input

VeriSign consistently described Site Finder as an aid to end users that provided Web search assistance for those who were potentially stymied by an apparent dead end. In this section and Appendix 5, we summarize the main technical points of VeriSign's position. Critiques that surfaced in the public meetings and in other communications are discussed in Section 2.5.2.

[12] Letter from Paul Twomey to VeriSign, 6 October 2003; http://www.icann.org/correspondence/twomey-to-verisign-06oct03.htm. Included in Appendix 3.

[13] Message from Security and Stability Advisory Committee to ICANN Board, 22 September 2003; http://www.icann.org/correspondence/secsac-to-board-22sep03.htm; verified 4 June 2004.

In its white paper describing the implementation[14] as well as in the presentations on both 7 October and 15 October, representatives of the company emphasized customer satisfaction, while acknowledging in the October discussions that the company had instituted refinements to their service in response to problems that had arisen. The authors of the white paper also described policies concerning network traffic monitoring and communications, indicating that these policies were compliant with relevant guidelines.[15] The authors state that the server monitoring data would not be made public at the launch of Site Finder but that the company was "considering making this information available in the future."[16] At the 7 October public meeting, Scott Hollenbeck, Director of Technology for the VeriSign COM NET Registry, said that the company had conducted "extensive testing prior to the launch of the service for several months with a series of partners."[17] When asked for an explanation of the methodology and experiment design,[18] Ben Turner, VeriSign Vice President, Naming Services, responded, "As we've offered to the committee before, our plan is to make available all the data that we have so that everybody can see the same results that we've evaluated and have an open evaluation of that data."[19] As of this writing, the Committee is not aware that this information has been released.

VeriSign argued that the service was useful to end users and that its changes to DNS were compliant with the relevant protocols, pointing to other top-level domains, such as MUSEUM, in which the wildcard mechanism was used.[20] At the 7 October public meeting, Hollenbeck described Site Finder as follows: Users who entered a URL ending in NET or COM that could not be resolved to a Web site were offered a page, hosted by a VeriSign server, offering URLs to alternative sites that seemed similar to the unresolvable URL. The Web page also offered users "the ability to surf the web or

[14] VeriSign Naming and Directory Services, VeriSign, Inc., VeriSign's Site Finder Implementation, 27 August 2003; http://www.verisign.com/resources/gd/sitefinder/implementation.pdf, verified 1 July 2004. We note the second paragraph of the Introduction: "VeriSign's Site Finder service improves the user web browsing experience when the user has submitted a query for a nonexistent second-level domain name in the *.com* and *.net* top-level domains. Before this service was implemented, when a user entered a URL containing a nonexistent (e.g., unregistered) domain name ending in *.com* or *.net*, his or her web browser returned an error message that contained no useful information. With the rollout of Site Finder, in the same situation users now receive a helpful web page offering links to possible intended destinations and allowing an Internet search." (The 27 August 2003 document was marked as a limited distribution document. The document was released publicly after the launch but the date was not changed.)

[15] See Section 2.4, Ibid., p. 4, notes 11-15.

[16] Ibid., p. 4. This sentence cites Guideline G1.16, which addresses publishing the results of the DNS query and response server port monitoring, and quotes the justification, to "allow the user community to see the benefits, including added user efficiencies provided by the new service." As quoted Ibid., p. 4, note 13.

[17] Scott Hollenbeck's presentation at the 7 October 2003 meeting; see SSAC Meeting Real Time Captioning, 7 October 2003, http://ssac.icann.org/captioning-07oct03.htm; verified 1 July 2004.

[18] kc claffy, question at the 7 October 2003 meeting; see SSAC Meeting Real Time Captioning, 7 October 2003, http://ssac.icann.org/captioning-07oct03.htm; verified 1 July 2004.

[19] Ben Turner, response at the 7 October 2003 meeting; see SSAC Meeting Real Time Captioning, 7 October 2003, http://ssac.icann.org/captioning-07oct03.htm; verified 1 July 2004. Mr. Turner took questions at the 7 October meeting but made his formal presentation at the 15 October meeting.

[20] As of mid-June 2004, the following top-level domains use the wildcard mechanism: AC, CX, IO, MP, NU, PH, PW, SH, TD, TK, TM, TV, WS, CC, MUSEUM. The following had no functioning name server: KM. Ólafur Guðmundsson to S. Crocker and J. Galvin, e-mail communication, 16 June 2004.

something else or to search a list of fairly well-known categories. "From the DNS perspective," he began his presentation, "it [Site Finder] involved putting a wildcard A record in the com and net zones as described in RFC 1034."[21] He continued, "For protocols other than HTTP, we provide a protocol-defined response."[22] Representatives of the company expanded on these points in four separate presentations at the 15 October meeting in which they described a lengthy process of research and development, examination of relevant protocols and user studies. Presentations addressed concerns that had been raised by the technical community since the launch and the steps that they with their Technical Review Panel of outside experts had taken to address these concerns. VeriSign's technical staff also engaged in discussions on various mailing lists.

VeriSign had assembled its Technical Review Panel (TRP) composed of industry experts drawn from outside the company together with VeriSign's engineers, who described their role as to "listen and answer questions."[23] The TRP reviewed the consequences of VeriSign's action by examining the effect on different protocols. The "Summary of TRC Findings" as presented by Hollenbeck (see Appendix 5, slide [9]) listed the effects on the top 10 protocols: HTTP, SMTP, DNS, IRC, epmap, pop3, microsoft-ds, netbios-ns, netbios-ssn, ftp. The summary characterizes the user experience before Site Finder and the user experience with Site Finder, provides a judgment of the change, and suggests a remedy, if applicable.

The second column of the summary table describes the user experience prior to the introduction of Site Finder. In all cases except HTTP and SMTP, the user experience before the change is that "'Name error' from DNS is presented to the user through their application". In the case of HTTP, the user received either an error message or a search page from a local application. In the case of SMTP, mail with an invalid address was "rejected with a 'Name error' from DNS presented to user through their application."[24] After the change, VeriSign's Technical Review Panel noted that for HTTP, there was an improvement for some users. In all of the other protocols except netbios-ssn, VeriSign's Technical Review Panel commented, "users may notice a delay compared to previous behaviour." VeriSign's TRP did not comment on netbios-ssn. VeriSign's Technical Review Panel identified, where possible, solutions to reduce the impact on existing applications. It was not possible to eliminate all impact on users, and thus some users would either have to change their software or change their behavior.[25]

[21] Hollenbeck's presentation at the 7 October 2003 meeting; see SSAC Meeting Real Time Captioning, 7 October 2003, http://ssac.icann.org/captioning-07oct03.htm; verified 1 July 2004.

[22] Ibid..

[23] VeriSign Site Finder: Technical Review Panel Summary, Scott Hollenbeck, Director of Technology, VeriSign, in Site Finder Review, SECSAC Meeting, 15 October 2003, Washington, DC, slide [4]; http://www.icann.org/presentations/turner-secsac-dc-15oct03.pdf; verified 26 May 2004; included in Appendix 5. For a description of the VeriSign Site Finder Technical Review Panel, see http://www.verisign.com/nds/naming/sitefinder/trp.html; verified, 20 June 2004.

[24] See "TRP Work Product – VeriSign Takeaways," in Hollenbeck, Site Finder Review, Slide [9]; http://www.icann.org/presentations/turner-secsac-dc-15oct03.pdf; verified 20 June 2004; included in Appendix 5

[25] The summary page of this presentation (slide [8]) claims "no catastrophic problems" and "no identified security or stability problems." Additionally, "most issues deemed minor or inconvenient." The summary

But at both meetings, the focus of VeriSign's position rested on the usefulness of the service to end users and the levels of satisfaction that end users had expressed. Ben Turner, Vice President of VeriSign, cited survey research in which 76 percent of the respondents rated the Site Finder site excellent or very good and only 4 percent rated it poor.[26] Finally, Rusty Lewis, Executive Vice President, closed the series of presentations that senior members of the company gave on 15 October, by acknowledging that advanced notice was appropriate and that if the service were to be re-launched, there would be at least 30 to 60 days of notice. He emphasized the importance of adhering to accepted best practice and concluded, "We believe that encouraging innovation at the core is just as important as encouraging innovation at the edge."[27]

2.3 Design Principles and Good Practice in the Internet Technical Community

To much of the user public, the Internet is variously conceived as a cloud, a network of networks or a telephone system with text, sound and images, delivered via a home computer or some other device. To the technical community, it is a set of protocols that enable signals to be transmitted over heterogeneous devices and multiple systems. Historically, the achievement has been both organizational, embodied in the IAB and the Internet Engineering Task Force (IETF), and technological, embodied in the logical architecture as well as in the lines, routers, servers and multitude of end-user devices. The assumptions, values, expected codes of conduct and practice have proved as important as the hardware and software engineering.

Much has been made of the "open" character of the Internet, and with time and success, the notion of "open" has taken on a broad range of meanings in diverse contexts. Within context of the engineering, the Internet is based on the notion of an open architecture, meaning that new protocols and services can be created, and is an "open data network," meaning that it can operate over and support highly heterogeneous technologies and applications, including those yet to be imagined.[28] This commitment to openness does not mean "anything goes." Rather, the diversity and complexities that can arise from the commitment to an open architecture are enabled by an equally deep commitment to a discipline of a minimal set of core protocols that are kept very stable. This core includes the Internet Protocol (IP), the routing system and the domain name system, as shall be explained further in the next section.

page acknowledged some software changes might be required. This summary does not reflect our reading of the Technical Review Committee's specific findings.

[26] Ben Turner's presentation at the 15 October 2003 meeting; see SSAC Meeting Real Time Captioning, 7 October 2003, http://ssac.icann.org/captioning-15oct03.htm; verified 29 June 2004; see also Ben Turner, Usability Market Research, in Site Finder Review, Slide [44]; http://www.icann.org/presentations/turner-secsac-dc-15oct03.pdf; verified 29 June 2004. .

[27] Rusty Lewis' presentation at the 15 October 2003 meeting; see SSAC Meeting Real Time Captioning, 7 October 2003, http://ssac.icann.org/captioning-15oct03.htm; verified 29 June 2004.

[28] This history is well known. We rely in part on the summary provided by the Computer Science and Telecommunications Board; see Computer Sciences and Telecommunications Board, National Research Council, *The Internet's Coming of Age* (Washington, D.C.: National Academies Press, 2001), pp. 36-40.

The stability at the core supports innovation both above and below this set of core protocols. Below it is where new transmission technologies and new signaling protocols have been introduced, including the Ethernet, the increase of speeds from 50k bits per second to multi-gigabit technologies and the use of both wired and wireless transmission media. Above it are the new protocols, new applications and new services, such as the World Wide Web and many other innovations large and small, such as search engines, e-commerce, voice over IP (VoIP) and so on. We emphasize these innovations above and below the core require the core to be kept under very tight discipline and to be both small and stable.

Often this arrangement of a robust active set of innovations above the core and equally robust set of innovations below is pictured as an hourglass figure in which the least number of required elements appears at the narrowest point with more and more choices – and complexity – above and below. In this hourglass image, applications and services above the core are at the edge of the network and are not at the control of the network operators. As a result, innovation, intelligence and complexity occur at the periphery or the edge, and the network, or the core, provides only simple, basic levels of service. Known as the "end to end argument," this design posed a radical challenge by the original Internet architects to existing principles behind the public switched telephone network (PSTN), where intelligence was concentrated in the center where network operations were controlled and "dumb" devices were located at the periphery where end users had access to them.

The original architects of the Internet made a second fundamental decision: to divide the complexities of the network by employing the principle of layering. Layers provide services to the layers above them without needing to know details of the upper layer operations and use the services of the layers below also without needing to know the details of how those services are provided. Application developers may build on the lower layers. As a result, there has been a profusion of innovation on a stable base. Conversely, innovative applications have respected the boundary between applications and core services, which remain stable and unaffected by the ferment of creativity the network can support. Thus, making changes to the center is necessarily done slowly, carefully and relatively infrequently.

At the heart of this logic is the robustness principle, summed up in the maxim, "Be conservative in what you send and liberal in what you receive."[29] Related to the robustness principle is the principle of least surprise, "Do what you think the other party is expecting." As a practical matter, given the challenges of networking across heterogeneous systems and technologies and the requirements of robustness and simplicity, there has arisen a careful process of review, discussion, testing and refinement. This is part of the popular notion of the Internet's "open" character: That these discussions take place publicly and with broad input from concerned communities within the framework of the IETF and the resulting protocol reflects consensus among those concerned. The process serves the highly practical purpose of enabling change to occur in a heterogeneous technological environment in a way that preserves both

[29] CSTB traces the articulation of this maxim to Jon Postel in 1979; see Ibid, p. 39, n. 15.

heterogeneity and stability. The results of these consensus deliberations are protocols that set forth the agreed upon conditions that an implementation must meet to work.

2.4 ICANN, IP Addresses, Domain Names, Wildcards and Error Messages

As the preceding section suggests, the "Internet" is an organizational phenomenon as well as a set of logical relationships and configurations of equipment. The issues raised by VeriSign's action lie precisely in the intersection of these three elements, in particular in the relationship between domain names and the associated IP addresses and the way that this relationship is managed.

Outside the technical communities of network engineers and software developers, the IP address is typically thought of as the sequence of numbers that identifies the physical server connected to the Internet; the subtleties of hosts, networks and routers are usually glossed over. More precisely, the IP address refers to the numbers that identify each sender or receiver of information that is sent in packets. It has two parts: the identifier (or string of numbers) associated with a particular network on the Internet and the identifier (or string of numbers) associated of the specified device or machine or within that network.

The domain name is the term associated with an institution, organization, entity or even individual and is also the term that is more widely recognized. The domain names form a hierarchy that branches like a tree, with each sub-level branching out from the domain name of its upper level. Again, many of the distinctions and implications of root, top-level, second-level and sub-domains are generally not well understood outside the technical communities. Indeed, many end users probably confuse the familiar second level domain (for instance, "example" for a hypothetical company called "Example Corporation") with the domain name itself, not realizing that the fully qualified domain name would be "example.com." The hierarchy is reflected in the sequence from right to left with the top-level domain name to the right of the ".", the familiar second-level domain immediately to the left of the ".", and the sub-domain (if any) to the left of the second-level domain. A "zone" is one or more levels in the hierarchy (root, top-level, second-level and so on) handled by a name server.[30] When a DNS query is referred to another name server, that process is called "delegation." In addition to the domain name of the delegated server, the response includes the IP address of the name server to which the query is referred; this IP address is known as "glue." In some zones, like COM, the expectation is that responses will be primarily delegations.

ICANN manages the distribution of IP addresses and domain names through an organizational system of registries, registrars and registrants.[31] ICANN accredits

[30] SSAC has recently set forth a set of recommendations concerning delegation of zones and sub-zones; see DNS Infrastructure Recommendation of the Security and Stability Advisory Committee SAC 005 Document 005 Version 1, 1 November 2003; http://www.icann.org/committees/security/dns-recommendation-01nov03.htm; verified 26 May 2004.

[31] The glossary provided by ICANN (http://www.icann.org/general/glossary.htm; verified 25 May 2004) provides the following definitions for potential registrants, that is, those who wish to register a domain name For *Registrar*: "Domain names ending with .biz, .com, .info, .name, .net or .org can be registered

domain name registrars[32] and has the ultimate responsibility for ensuring that domain names are uniquely assigned. The operation of the registry databases and the actual work of registering domain names and maintaining the relationships fall to the registry operators themselves. VeriSign operates the registry for the very large NET and COM top-level domains (TLDs).

The domain name system (DNS) is a set of databases and programs that allow the fully qualified domain name to be translated into or linked to an IP address through a series of queries. The fundamental concepts behind DNS are well-established and were set forth in Requests for Comment (RFCs) 1033, 1034 and 1035, all three dated November 1987.[33] As described in RFC 1034, DNS has three major components: the domain name space and resource records, which are stored in what computer scientists call a "tree structure ;" name servers, which have information about the domain's tree structure; and resolvers, which obtain information from name servers in responses to a query from a client. There are several types of resource records. "A" records are the primary type and provide an IP address for a specific name. The tightly defined operation wherein an unambiguous name is presented to the system and the system returns a unique IP address is called "lookup." VeriSign's action, as previously described, added a new "wildcard" A record that matched all uninstantiated names.

RFC 1034 allows for flexibility in the way that DNS can respond to queries for uninstantiated names. It describes wildcards as "instructions for synthesizing" information associated with a name. The original specifications are not clear when it is appropriate to use wildcards, but at the time, wildcards were anticipated for use in mail

through many different companies (known as "registrars") that compete with one another. A listing of these companies appears in the Accredited Registrar Directory. The registrar you choose will ask you to provide various contact and technical information that makes up the registration. The registrar will then keep records of the contact information and submit the technical information to a central directory known as the "registry." This registry provides other computers on the Internet the information necessary to send you e-mail or to find your web site. You will also be required to enter a registration contract with the registrar, which sets forth the terms under which your registration is accepted and will be maintained."
For *Registry*: "The 'Registry' is the authoritative, master database of all domain names registered in each Top Level Domain. The registry operator keeps the master database and also generates the "zone file" which allows computers to route Internet traffic to and from top-level domains anywhere in the world. Internet users don't interact directly with the registry operator; users can register names in TLDs including .biz, .com, .info, .net, .name, .org by using an ICANN-Accredited Registrar."

[32] "'Accredit' means to identify and set minimum standards for the performance of registration functions, to recognize persons or entities meeting those standards, and to enter into an accreditation agreement that sets forth the rules and procedures applicable to the provision of Registrar Services." (See http://www.icann.org/faq/#WhatisICANN; verified 23 May 2004.)

[33] Requests for Comment (RFCs) are both a system of communication and a way of documenting developments and proposed developments within the Internet technical community. They may be found at http://www.ietf.org/rfc.html. RFC 1033 is the "Domain Administrators Operations Guide" (M. Lottor, SRI International, November 1987). RFC 1034 is "Domain Names – Concepts and Facilities (P. Mockapetris, ISI, November 1987). RFC 1035 is "Domain Names – Implementation and Specification (P. Mockapetris, ISI, November 1987). These have been updated over the years. A useful introduction to DNS for non-experts is the Internet Society's briefing by Daniel Karrenberg, The Internet Domain Name System Explained for Non-Experts, ISOC Member Briefing #16. It is available at http://www.isoc.org/briefings/016/; verified 23 May 2004.

applications: “This facility is most often used to create a zone which will be used to forward mail from the Internet to some other mail system. The general idea is that any name in that zone which is presented to [a] server in a query will be assumed to exist, with certain properties, unless explicit evidence exists to the contrary.”[34]

Good practice regarding wildcards has evolved. But the IAB’s 19 September 2003 commentary observes, “Even after twenty years of experience with the DNS, the effects of unexpected uses of wildcards can still be quite surprising, because the small but fundamental way in which they change the record lookup rules has a nasty way of violating implicit (or, sometimes, explicit) assumptions in deployed DNS-using software.” The report has been included as Appendix 6 and its principal points are summarized in the following paragraphs.

The IAB acknowledged that the wildcard mechanism had been a part of the DNS protocol since the specifications were originally written. However, the mechanism was also understood to be tricky, especially when more than one protocol is invoked. An authoritative name server returns one of three responses to a query: “success,” “no data” (which means that the name exists but the does not have information about it) and “no such name”. When wildcards are present, the “no such name” response cannot occur and server provides the same response to queries that otherwise might have been either “success” or “no data.” Hence, in the instance of Site Finder and other similar services, mistakes in typing are processed, rather than rejected, and the user redirected to a page that provides information. But this may be, in a sense, a false positive since the system appears to be providing a valid response when in fact it is masking an error, and an error is a legitimate form of information. Applications that rely on the “no such name” response fail since the “no such name” response no longer occurs.

The IAB analysis identified two main problems:

- the authoritative servers for these two zones no longer give out "no such name" responses for any possible name in these zones, and
- every possible name rooted in one of these zones which, until this change, did not exist at all, now has a synthesized address record pointing at a "redirection server" run by the operator of this zone.

The commentary then listed and briefly discussed a series of problems encountered in recent experiences with wildcards: Web browsers, e-mail, spam filters, automated tools, error messages, interaction with other protocols, charging, single point of failure, privacy, use of reserved names and undesirable workarounds. From an architectural point of view, the commentary concluded, the wildcard mechanism violated two fundamental principles: Robustness and the Principle of Least Astonishment (see discussion in Section 2.3). It is possible to use wildcards in certain situations, the commentary continued, and the Museum Domain Management Association claims to have done so (Appendix 7). However, theirs may be a relatively rare case where the domain is

[34] RFC 1034, Section 4.3.3.

restricted to a “clearly bounded community.” “Warning flags,” the IAB cautions, were that the action:

- affected more than one protocol, and
- was done high enough up in the DNS hierarchy that its effects were not limited to the organization that chose to deploy these wildcard records.

As of mid-June 2004, there are 258 top-level domains listed in the root zone of which 15 use the wildcard mechanism. These are generally very small or, as in the instance of MUSEUM, represent well-defined communities. Indeed, the Museum Domain Management Association estimates its “maximum anticipated population” to be “about 1,000th the size of .com”. In its 6 October 2003 Statement Concerning Wildcard A Records in Top-Level Domains, included as Appendix 7, the Association describes the lengthy and open process in which the mechanism was developed within the museum community. Moreover, given the small size of the community, the Statement observes, “The potential for disruption to applications written in reliance on the lack of wildcards is clearly smaller than in any case where wildcards are introduced into a significantly larger TLD, especially where that introduction occurs after a protracted period of operation without wildcards.”[35]

2.5 Summary of Technical Issues

VeriSign’s action consisted of a change to the registry operations and a change to the operation of those servers. It had two adverse effects. First, it changed the way the registry functioned by returning seemingly legitimate addresses for domain names which really did not exist. Second, it introduced this change abruptly, without public notice, without coordination, without independent testing and refinement, and without agreement from the community of users affected by the change. Both of these dimensions, the fact of the change and its abruptness, violated community standards and caused harm to individual users and enterprises. In this section, we describe those changes and those effects in greater detail.

Prior to VeriSign’s action, when the name server[36] received a query for an uninstantiated name (which might be a name that had not been registered in DNS, one that had previously existed but did so no longer, or a misspelling of an existing name), RCODE 3, the standard error code for “name error,” was returned, thus alerting the requester that the name was not instantiated. After VeriSign’s action, the VeriSign registries responded to queries for an uninstantiated name by returning the IP address of one of its servers as if the requested name were instantiated and fully in operation. Instantiated names were not affected.

[35] Museum Domain Management Association, Statement Concerning Wildcard A Records in Top-Level Domains, 6 September 2003, http://musedoma.museum/policy/wildcard/; verified 20 June 2004.

[36] We note that only NET and COM were affected by VeriSign’s action; other domains were unaffected. However, for purposes of simplicity, we have described the events in this section without introducing this qualification.

However, the change in the way that errors were reported – or not reported – to the end user had substantial and destabilizing effects. As described in the previous section, the response, "no such name," possesses important meanings. We emphasize the point that error responses contain information upon which other systems then act. Consequently, effectively eliminating the "no such name" response has ramifications through the system, preempts the expected behavior, and, in this instance, provoked localized efforts to work around or restore the system. In addition, the burden of work was, in many cases, shifted to system administrators and help desk staff, who suddenly had to cope with unanticipated changes and reactions from bewildered end users.[37]

2.5.1 Protocol Independence and the Effects on Mail Systems

As required by the principle of layering, described in Section 2.3, when a DNS query is made to a name server, the purpose of the query is not included. That is, there is no way for the name server to tell whether that query is for the purpose of looking up a Web page, sending mail, initiating a file transfer, logging in remotely to a machine, or initiating a network management action. Each of these services, and many others not mentioned here, are embodied in their own protocols. All of them require the translation of domain names into IP addresses. But the DNS lookup message does not include the name of the protocol that has triggered this lookup. Specifically, the operation of the name server is independent of the functionalities of the query submitted to it.

VeriSign's action implicitly violated that separation. It assumed that all – or at least the vast preponderance – of queries involving uninstantiated names were intended to be HTTP (Web) queries or SMTP (e-mail) transactions. Consequently, it made assumptions about the protocol initiating the query.

When the requester made the connection to a VeriSign server, if it was indeed, a Web request, then it reached the Site Finder service. If it was an e-mail transaction, it reached VeriSign's so-called "bounce" server, initially named "Snubby." If it was neither a Web query nor an e-mail transaction, then the VeriSign server refused the connection.[38]

[37] One comment reported to ICANN's mailing list server: "I mistyped a URL and VeriSign's wildcard service suggested I visit a porn site with a similar name! I find this highly offensive." As quoted in Roessler, October 2003, Slide 4.

[38] The following summary discussion of problems in e-mail systems is based on several sources: see David Schairer's presentation at the 7 October 2003 meeting; see SSAC Meeting Real Time Captioning, 7 October 2003, http://ssac.icann.org/captioning-07oct03.htm; verified 20 June 2004; see also David Schairer, Consequences I: What Was Affected, Washington, DC, 7 October 2003; http://www.icann.org/presentations/shairer-secsac-dc-07oct03.pdf; verified 23 May 2004. Richard Smith also addresses problems with e-mail systems resulting from Site Finder; see Richard Smith, Why Site Finder is Breaking MS Outlook & Windows Networking Utilities, CircleID, 21 September 2003, http://www.circleid.com/article/273_0_1_0_C/#outlook; verified 21 June 2004. Paul Vixie documents additional problems in his message, Re: VeriSign SMTP Reject Server Updated, 20 September 2003, NANOG (North American Network Operators Group), http://www.merit.edu/mail.archives/nanog/2003-09/msg00994.html; verified, 21 June 2004. The previously described IAB commentary contains an extensive discussion of effects on e-mail systems; see Appendix 6. There was also discussion on the e-mail

VeriSign's handling of e-mail was particularly problematic. The early implementation, which was quickly replaced, appears to have been flawed and did not handle the SMTP protocol properly, resulting in inconsistent behaviors on the part of sending servers. Some treated the problem as a transient delivery failure, causing the message to be re-queued. Others treated the transaction as a permanent failure, causing the message to be returned to the sender. And still others treated the transaction as a temporary server failure, causing unpredictable behavior on the part of the sender. (For example, in the last instance, some systems just kept trying to send because they were not receiving answers that they understood.)

In addition to inconsistent responses, prior to VeriSign's action, a bounced message would have been returned immediately because the domain name would not have resolved, thus giving the end user an immediate response and providing an error message which stated that the domain name does not exist.

There are further subtleties. In some environments, particularly corporate environments, there is sometimes a list of mail addresses to try to reach someone. If the first address fails, then the system that is trying to deliver the mail tries the next one. Subsequent to VeriSign's action, such a mail system's attempt to go down the list was interrupted because the first attempt looked good – even if it were not. End users experienced a range of problems.[39] But overall, from the perspective of mail systems, David Schairer, Vice President, Software Engineering for XO Communications, concluded at the October 7 meeting, there were network impacts and operational costs. Specifically:

- Bounced messages increased traffic and costs;
- Undeliverable mail increased costs for mail server farms; and
- Mail queuing reduced performance.[40]

On September 20, 2003, VeriSign replaced its Snubby mail rejection (or "bounce") server with an alternate implementation that used Postfix.[41] The only purpose, VeriSign stated on its Site Finder FAQ, was to reject mail "immediately."[42] In its subsequent operations, the server accepted e-mail operations and then in the course of processing attempts to deliver mail to specific users, sent back "no such user" response for each one of those. This is better from the sense that it gave a more immediate response. However, it confuses a "no such user" response with the more accurate "no such domain" response.

archive maintained by the IETF; see for example, ftp://ftp.ietf.org/ietf-mail-arhcive/ietf/2003-09.mail ("What *are* they smoking").

[39] David Schairer, Consequences I: What Was Affected, Washington, DC, 7 October 2003; see especially Slide 8; http://www.icann.org/presentations/shairer-secsac-dc-07oct03.pdf; verified 23 May 2004.

[40] Ibid., see especially Slide 9.

[41] On VeriSign's response to feedback concerning e-mail, see Hollenbeck's comments in the 7 October 2003 transcript, SSAC Meeting Real Time Captioning, 7 October 2003, http://ssac.icann.org/captioning-07oct03.htm; verified 20 June 2004. See also Site Finder FAQ, SMTP Server Issues (Updated 21 Sep 03), http://www.verisign.com/nds/naming/sitefinder/info.html.

[42] Site Finder FAQ, SMTP Server Issues (Updated 21 Sep 03), http://www.verisign.com/nds/naming/sitefinder/info.html

But VeriSign's fix also created additional concerns. Larger messages (in excess of 10 MB) bounced with a "message too large" error rather than the more appropriate "domain not found" error and a very low timeout value on client response might cause slow senders to time out and frequently retry.[43] Moreover, as a result of this new strategy, information about e-mail senders and recepients entered VeriSign's computers, thus allowing a possible analysis of who is sending mail to whom, unbeknownst to either sender or recepient. VeriSign strongly asserted that the company was not keeping that information or making use of it. Nor is there any evidence that they did so or would do so. However, if another registry operator chose to implement a similar service, it is possible that this information, as well as the content of the message itself, could be accepted and stored.

In any case, there is no opportunity under this strategy to observe independently what the facts might be. That is, in the first implementation (Snubby), one could at least observe that this information was not collected. In the latter case, although VeriSign was able to give the much prompter, albeit incorrect response, of "no such user," the fix raises the concern that VeriSign *might* be collecting information that users would not expect them to collect nor architecturally was there any way for the user to have given permission for this information to be collected. Thus, an ambiguity was created for the end user knowledgeable enough to recognize the implications.

VeriSign's action also affected certain spam filters.[44] One of the strategies used by some spam filters is to check whether the domain name of the sender exists. For example, prior to VeriSign's action, if a message putatively from user@madeupdomainname.com had been sent, the spam filter would have tested the existence of madeupdomainname.com and would have gotten the response, "no such domain name". Subsequent to VeriSign's actions, it would have received the address of a server for madeupdomainname and thus presumptively – and potentially erroneously -- classified the message as legitimate. Thus, in one action, VeriSign disabled all of those spam filters.

It may be argued that only a small number of spam filters employ this strategy. Further, it may be asserted that this strategy is not the most effective one for eliminating spam. It is beyond the scope of this report to make judgments on the relative merits of different spam filters. We simply note here that VeriSign's action did have the effect of disabling this class of spam filters.

2.5.2 Site Finder

As reported earlier, VeriSign offered copious evidence showing that a majority of users were pleased with Site Finder.[45] However, some critics pointed out problems in usability

[43] Schairer, Consequences I, Slide 7.

[44] The previously referenced IAB commentary addresses the effect on filters; see Appendix 6.

[45] In response to specific questions about the overall methodology and the release of the survey instrument, which are customary among academic researchers, VeriSign refused to disclose either. Moreover,

(for example, that the site was only in English[46] and was not broadly accessible to certain populations, such as the visually impaired[47]). Moreover and of greater concern from the perspective of this Committee are two effects on end users: substitution for existing services[48] and removal of choice.[49] The Site Finder service substituted itself for equivalent services already existent at the desktop; MSN and AOL offer similar services in the form of plug-ins for browsers so that when the error message "no such domain name" is returned, a comparable search takes place. VeriSign's action had the effect of disabling existing services and depriving users of a choice as to which service, if any, is to be provided at the desktop and how to configure it. All those choices were removed.

Some critics have viewed this imposition of a service as denying users an opportunity to participate, specifically, removing the opportunity to refuse or to "opt out."[50] We note here that the actual effect is broader: not only were users not able to opt out but if they had already had an existing service, it was replaced by VeriSign's Site Finder service. Thus, in addition to the often heard complaint that VeriSign did not provide a way to opt out of this service, they also pre-empted decisions users had already made.[51]

There was a further problem beyond the unilateral imposition of this service. It also subjected end users to potential scrutiny of which they were unaware and about which they had no control. Analysis of Site Finder revealed that a "web bug" had been embedded in the page so that information about behavior of users of the page was sent to a company named Omniture, which monitors Web traffic.[52] Information about users of Site Finder was thus passed off to a third party, again without the consent of the users and perhaps without their knowledge.

Benjamin Edelman offered evidence of push-back, based on analysis of data provided by Alexa. See Benjamin Edelman, Measuring ISP Response to VeriSign SiteFinder, Washington, DC, 15 October 2003; http://www.icann.org/presentations/edelman-secsac-dc-15oct03.pdf; verified 23 May 2004.

[46] At the 15 October 2003 meeting, VeriSign stated that "future" releases of Site Finder would support "at least" German, Japanese, Spanish, French, Chinese and "other" languages; see Matt Larson's presentation in SSAC Meeting Real Time Captioning, 15 October 2003, http://ssac.icann.org/captioning-15oct03.htm; verified 20 June 2004.

[47] Limitations based on language and accessibility are cited by Schairer in his presentation at the 7 October 2003 meeting, see SSAC Meeting Real Time Captioning, 7 October 2003, http://ssac.icann.org/captioning-07oct03.htm; verified 21 June 2004.

[48] On substitution of Site Finder for existing services, see Roessler, SiteFinder: Community Comments, At-Large Advisory Committee, Carthage, October 2003, Slide 5.

[49] Ibid., Slide 7.

[50] Ibid., Slide 7. Roessler notes, "Most users didn't even intend to use the service – no conscious decision to mistype domain name." Lack of opt-out was also mentioned during the question and answers in the afternoon session of the 15 October 2003 meeting; see SSAC Meeting Real Time Captioning, 15 October 2003, http://ssac.icann.org/captioning-15oct03.htm; verified 20 June 2004.

[51] Consider, for example, a comment to the ALAC forum: "I am just an ordinary internet user going about my business, but what VeriSign did really makes me upset and it is an inconvenience. So I started to read more about this issue and the more I read, the more I get upset -- so I'm writing ICANN to help stop VeriSign from doing this. This is for the following reasons. 1) When I misspelled something, I don't want to be redirected to it's website, I just want to fix my mistake." Submissions to the ALAC Forum, http://forum.icann.org/alac-forum/redirect/msg00021.html.

[52] See Richard Smith's comments in the 7 October 2003 transcript, SSAC Meeting Real Time Captioning, 7 October 2003, http://ssac.icann.org/captioning-07oct03.htm; verified 20 June 2004.

Further, many sites, most notably public school systems, have strong filters in place to protect its end users from accessing inappropriate sites. The Site Finder service as initially launched included partial but not stringent controls on what sites could be looked up. It was quickly discovered that users connected to Site Finder could then reach sites that they could not otherwise have reached. Managers in charge of public schools and libraries in the U.S. were then faced with adding additional controls to their existing systems to protect against Site Finder. That is, Site Finder itself had to be added to the list of prohibited sites.

2.5.3 Workarounds and Inconsistencies: Implications for End Users

The implementation of Site Finder came as a surprise to users, network operators and Web site administrators.[53] Ameliorating VeriSign's action and dealing with end users' responses to it created work for system operators and increased costs, particularly for people without "high-speed, always-on Internet connections."[54] Between launch and suspension of the service, patches were released by ISPs and by vendors of DNS resolver software, most notably by Internet Systems Consortium (ISC), which provides BIND, the most commonly used DNS resolver software.[55] This solved certain problems on a relatively limited basis.[56] In quite a few cases, system operators, some at the ISP level, some at the enterprise level, sought to intercept VeriSign's synthesized response and then to retransform that response back to the original "no such domain" error code. This approach required identifying the specific address, for example, 1.2.3.4, and then blocking it.

For example, in Tennessee, 132 of the 139 public school districts are provided Internet service through a common provider. In aggregate, there are 1884 end sites, 900,000 students, 60,000 teachers/administrators and 250,000-plus computers. VeriSign's action triggered both a noticeable increase in help desk calls and an alternative pathway to reach

[53] This observation is made by Jonathan Zittrain and Benjamin Edelman of Harvard Law School's Berkman Center for Internet & Society who conducted an analysis of problems with Site Finder as reported on mailing lists, blogs, bulletin boards, online magazines and other venues, which they combined with a quantitative analysis of traffic. See Index of Concerns as to Site Finder, http://cyber.law.harvard.edu/tlds/sitefinder/concerns.html; verified 21 June 2004. Negative impacts on users are also reported in Message from Tucow's Elliot Noss to Paul Twomey, 3 October 2003, http://www.icann.org/correspondence/noss-to-twomey-03oct03.htm; verified 21 June 2004.

[54] Schairer, 7 October 2003, SSAC Meeting Real Time Captioning, 7 October 2003, http://ssac.icann.org/captioning-07oct03.htm; verified 21 June 2004. Later in this presentation, he concluded, "All of us who do sell Internet services will have increased support costs, increased network costs, more things to worry about. We have had to go and patch things that we need to maintain. It has become sort of a chronic background hum that we will need to worry about."

[55] Paul Vixie, President of Internet Systems Consortium, Inc. (ISC), summarized the workarounds and their implications at the 7 October meeting; see Observed Workarounds to Synthetic Data Returned for Uninstantiated names in .COM/.NET, http://www.icann.org/presentations/vixie-secsac-dc-07oct03.ppt; verified 21 June 204.

[56] We note that the ISC patch did not work effectively within NAME; see presentation by Hakon Haugnes at the 15 October meeting, http://ssac.icann.org/captioning-07oct03.htm; verified 22 June 2004. These concerns were reiterated in a formal letter from the Global Name Registry to SSAC, G. Rassmussen to S. Crocker, 13 October 2003.

objectionable sites. The system administrators installed the ISC patch to counteract the VeriSign change.[57]

This action on the part of ISPs and name resolvers provided an immediate salve but is considered poor engineering. First, the list of server addresses that VeriSign might return can change over time. More awkwardly, addresses that are filtered out might be configured at some later time for legitimate sites and there would be no obvious reason to the user why those sites are unreachable. In this hypothetical example, the ISP or the name resolver would return the message "no such domain" when, in fact, the domain exists. Second, this strategy adds to the workload and complexity to systems maintained by ISPs and name resolvers. It now introduces the network or resolver operator into the decision process, further removing users from exercising choice. Thus, if users were happy with Site Finder, there would be no way to choose it and "opt-in" is precluded in this case just as "opt out" was precluded before.

From a broader perspective, this strategy has opened the door to network operators making decisions about content, that is, interfering or modifying the traffic going through their systems and doing so under the rubric of protecting users. The general principle that the Internet has operated under from its inception is that the lower layers of the network should be exclusively focused on accurate, reliable, efficient transmission of the messages sent from end user to end user. This experience raises the possibility that some network operators will see other opportunities for so-called "participation" in end users' experience.[58]

Good practice has always required extensive testing, engineering refinement and public comment from the community. In marked contrast, these fixes were hustled into operation quickly. Instability results from abruptness, whether from VeriSign's action or from the urgent responses to it. Whereas VeriSign had the benefit of months of preparation, albeit out of public view, the responses were instituted very quickly, and, of necessity, these responses, workarounds and fixes did not have the benefit of extensive testing and engineering refinement. Additionally, they were introduced locally and therefore not uniformly. Consequently, the end users' experience varied depending on which resolver or which ISP had instituted these changes and when.[59] Moreover, end users experienced one kind set of responses for errors in NET and COM but other kinds of responses in, for example, ORG or one of the other top-level domains.

[57] Personal communications, Collie to Woolf, 20 October 2003 (e-mail); Collie to Crocker, 24 May 2004. This action was taken by the provider before the SiteFinder matter came to the attention of state officials or the media.

[58] We note that this argument also cuts the other way. Once the door to content is opened, there exists potential for liability. This is a legal issue, outside the scope of this Committee. We simply note that in introducing engineering changes of this sort, the clean bright line that had previously been in place has become muddied.

[59] This point is made with some emphasis in the IAB commentary (Appendix 7), which summarizes "undesirable workarounds." The commentary notes that ISPs have responded to the deployment in a number of ways, "all of which are both understandable and worrisome." The passage concludes, "Even more worrisome is that different ISPs are taking different approaches to dealing with this, which may lead to a balkanization problem and create an ongoing headache for anyone having to deal with cross-network DNS or application debugging."

One of the fundamental objectives in the design of the domain name system is to give the same response no matter where the queries are initiated. This attribute is called *coherence*. Local introduction of countervailing changes necessarily resulted in varying responses at different locations and a loss of coherence.[60] We note further that VeriSign's single change triggered multiple countervailing reactions. That is, a significant number of hours were spent across multiple organizations to undo a change introduced by one organization. We offer up no quantitative measures of the magnitude of this change and its potential differential impacts among different populations of users around the world with different levels of connectivity and access to infrastructure services, but as a qualitative matter, this effect is inescapable.

Finally, some have suggested that the introduction of countervailing changes is comparable to the introduction of VeriSign's action. In particular and as previously mentioned, Internet Systems Consortium (ISC) released a modified version of its widely used BIND resolver with the capability to be configured to reverse or undo VeriSign's synthesized response. We note here however that two actions were required to install such a change: First, vendors such as ISC provided software to make it possible to undo the change. Second, network or site operators explicitly chose to install and put into operation those changes.

There was no opportunity for a single organization, ISC or any other entity, to unilaterally counteract VeriSign's action. Rather, a natural check-and-balance or propose-dispose cycle existed, even with in the very short time of these actions. The decision to intercept and reverse VeriSign's action required a decision on behalf of the users and not solely a response from a direct competitor to VeriSign.

2.6 Discussion and Conclusion

In Sections 2.1 and 2.2, we reviewed the actions of September and October 2003 and have offered a summary of VeriSign's input. As is consistent with its charter and its mandate, the Committee has considered the issues raised by the cycle of actions and responses from a broad perspective that has included consideration of fundamental architectural principles and good practice as they have evolved over the last 30 years, as briefly described in Section 2.3. From this vantage point, it becomes evident that VeriSign's action has exposed some tensions that had been known – or at least suspected. As summarized in Section 2.4, RFC 1034 does allow for use of the wildcard mechanism. But it is also clear that system designers expected this mechanism to be used in limited settings, for example, for mail or in enterprise settings. The IAB commentary, also discussed in Section 2.4, acknowledges the existence of the wildcard mechanism but goes

[60] Vixie's comment at the 7 October meeting is telling. He concluded: "From my perspective as a protocol and software person, the total result of this [sequence of patches] is incoherence and growing incoherence. The people who are responding to this are responding by making DNS response less coherent than they were. And that's not a direction I'd like to see us go in. So I think that the total result in terms of DNS incoherence is that we've seen some instability. And there will be more if the service is turned back on." SSAC Meeting Real-Time Captioning, 7 October 2003, [p. 34].

on to say that practice has evolved over the last three decades and that there were warning signs, namely, it affected more than one protocol, and was done high enough up in the DNS hierarchy that its effects were not limited to the organization that chose to deploy these wildcard records. Simply because the COM and NET domains are so very large, interaction effects become evident that might not be visible in another TLD, such as the small and well-managed MUSEUM. This is, in retrospect, not surprising. Rather, it is a concomitant to growth and expansion in a complex system where all potential interactions cannot be anticipated.

The Committee has wrestled with issues related to size, diversity, innovation and growth. It recognizes that the issue is not the wildcard per se but rather the larger question of how and under what circumstances synthesizing responses for uninstantiated names may or may not be appropriate. Indeed, synthesizing responses may make sense when the entity responsible for a zone can exercise responsibility for or control over the zones branching or delegated off from it. Such a private zone might be a corporate enterprise such as "madeupenterprise.com" where a manager can exercise authority over research.madeupenterprise.com, sales.madeupenterprise.com, HR.madeupenterprise.com and so on. On the other hand, there exist zones whose contents are primarily delegations and glue, and where delegations cross organizational boundaries; these are essentially public zones. In this case, the zone operator may not have authority over the behavior of zones delegated from it. This distinction differentiates between private and public zones, which embrace ccTLDs. But it recognizes that very large and diverse zones are qualitatively different from such specialized zones as MUSEUM and AERO, which do exercise at least influence, if not outright control, over the behavior of entities delegated off of it.

Accordingly and as a general rule, we recommend that wildcards not be used in A records in TLDs or zones that serve the public over which the operator may have little control or influence. For specific purposes, such as re-directing e-mail connection attempts, alternative mechanisms exist that are specific to each protocol, for example, the MX record for mail.

With respect to the sequence of actions in September-October 2003, which surfaced some of these tensions, the Committee concludes that VeriSign's action violates fundamental and well-tested principles of the Internet architecture and good practice. It interferes with long-standing design principles of robustness, supporting intelligence and innovation at the edges by maintaining stability at the core, and introducing changes and improvements at the core only after careful, public scrutiny, consensus, testing and refinement. In addition, VeriSign's action violates well-established principles of layering as was made very obvious in the initial presumption that HTTP was the requesting application layer. It muddies the distinction between the DNS service and higher level applications.

Second, the method of introduction of the change also raised its own set of issues. VeriSign's action initiated a set of countervailing changes that were in their totality incoherent and created a different set of costs for system administrators and others who were compelled to make changes to reverse or compensate for unanticipated and unannounced behaviors.

Third, economic as well as the technical and operational costs were borne by third parties. Although shifting costs to third parties is not necessarily a security or stability issue in and of itself, unilaterally imposing such costs on third parties without notice, consent or a viable alternative creates unforeseen and unavoidable costs for them and is therefore a source of instability.

Fourth, in addition to disrupting stability, end users were potentially exposed to invasions of their privacy of which they were unaware. Information embedded in e-mail headers ended up in VeriSign's servers and Web users re-directed to Site Finder were watched and information sent to a commercial third party.

In aggregate, perhaps the greatest casualty involves trust. Previously, threats to security and stability were perceived to be primarily external, arising from acts of nature, possible business failures or the behavior of malicious outsiders. This sequence of events has shown that the stability of the Internet can also be affected by the actions of trusted operators of core services acting in their own self interest. In Section 2.4 of this document, we identified three classes of people directly associated with operating the domain name system: registry operators, registrars and registrants. All of them were affected by VeriSign's action, but there is also a fourth set of people who count on the reliable operation of the domain name system – the users. As the Tennessee example shows, they can be system administrators or end users. They are the largest constituency. Yet they are the ones with the least say. Users who have no direct relationship with registry operators can fairly ask what are the rules governing stability of the core services? That question has more salience and urgency today than it did prior to VeriSign's action.

3.0 Findings and Recommendations

In this section, we set forth specific findings relative to questions of security and stability and make recommendations concerning future actions. In the previous sections, we described the events that transpired in September-October 2003 and the technological consequences of those events in the context of fundamental concepts, principles and accepted good practice. As acknowledged in Section 2.6, we recognize that these issues have surfaced suspected and in some instances well known tensions precisely because of the size and heterogeneity of the combined COM and NET domains. With growth, what might otherwise have been an irritant escalates and the potential for more widespread and chronic failures troubles the Committee and motivates its recommendations for future practice.

The Committee offers these findings and recommendations in the spirit of open review, comment and evaluation in the expectation that they will be considered and tested before they result in action. Overall, the Committee acknowledges that VeriSign's action did not cause network shattering and readily understandable failures or potential failures on the scale of the electricity grid's black-out in the Northeast United States last summer. Nor did it conjure up the specter of widespread catastrophe that might be easily grasped in the way that Y2K caught the public imagination. However, the sequence of reactions, localized failures, displaced and potentially chronic costs, fixes, patches and workarounds adds up to a troubling picture that violates basic engineering principles. Specifically,

Finding (1): VeriSign introduced changes to the NET and COM registries that disturbed a set of existing services that had been functioning satisfactorily. Names that were mistyped, had lapsed, had been registered but not delegated, or had never been registered in DNS were resolved as if they existed. As a consequence, certain e-mail systems, spam filters and other services failed resulting in direct and indirect costs to third parties, either in the form of increased network charges for some classes of users, a reduction in performance, or the creation of work required to compensate for the consequent failure.

Finding (2): The changes violated fundamental Internet engineering principles by blurring the well-defined boundary between architectural layers. VeriSign targeted the Site Finder service at Web browsers, using the HTTP protocol, whereas the DNS protocol, in fact, makes no assumptions – and is neutral – regarding the protocols of the queries to it. As a consequence, VeriSign directed traffic operating under many protocols to the Site Finder service for further action, and thus, more control was moved toward the center and away from the periphery, violating the long-held end-to-end design principle.

Finding (3): The mechanisms proposed by VeriSign to ameliorate the undesirable effects of their diversion on protocols other than HTTP put VeriSign in the implementation path of every existing and future protocol that uses DNS. For every such protocol, it would be necessary to consult with VeriSign to figure out how to simulate the response of the protocol to "no such domain." This is an unacceptable invasion of clear layering.

Finding (4): Despite a long period of internal research and development, the system was brought out abruptly. The abruptness of the change violated accepted codes of conduct that called for public review, comment and testing of changes to core systems; this process exists to ensure that changes are introduced with minimal disruption to existing services and hence with minimal disruption to the security and stability of the Internet. It also precluded the possibility that administrators, IT departments, ISPs and other intermediaries on whom end users rely might be adequately prepared to deal with the consequences.

Finding (5): In response, workarounds and patches were introduced quickly, cumulatively reducing the overall coherence of the system and again violating the established practices of public evaluation, testing, discussion and review before core services are implemented and deployed. These workarounds further blurred the functional layers intrinsic to the Internet's robust architecture and in some instances created additional -- and unintended -- harmful effects.

Finding (6): Information about intended e-mail senders and receivers was necessarily accepted by VeriSign's servers without the knowledge or consent of either sender or receiver. VeriSign strenuously denied retaining this information.

Finding (7): The behavior of end users redirected to the Web site was observed by a program embedded in the Site Finder service, and users could neither accept it, reject it nor substitute another, similar service for it.

Finding (8): The cycles of changes and responses collectively undermined expectations about reliable behavior and in so doing reduced trust in the security and stability of the system.

On the basis of these findings, the Committee makes the following recommendations:

Recommendation (1): Synthesized responses should not be introduced into top-level domains (TLDs) or zones that serve the public, whose contents are primarily delegations and glue, and where delegations cross organizational boundaries over which the operator may have little control or influence. Although the wildcard mechanism for providing a default answer in response to DNS queries for uninstantiated names is documented in the defining RFCs (Requests for Comment), it was generally intended to be used only in narrow contexts (for example, MX records for e-mail applications), generally within a single enterprise, and is currently used in top-level domains that are generally small and well-organized.

Recommendation (2): Existing use of synthesized responses should be phased out in TLDs or zones that serve the public, whose contents are primarily delegations and glue, and where delegations cross organizational boundaries.

Recommendation (3): There exist shortcomings in the specification of DNS wildcards and their usage. The defining RFCs should be examined and modified as necessary with a focus on producing two results: first, clarification of the use of synthesized responses in DNS protocols; second, provision of additional guidance on the use of synthesized responses in the DNS hierarchy.

Recommendation (4): Changes in registry services should take place only after a substantial period of notice, comment and consensus involving both the technical community and the larger user community. This process must (i) consider issues of security and stability, (ii) afford ample time for testing and refinement and (iii) allow for adequate notice and coordination with affected and potentially affected system managers and end users. Thirty years of experience show that this strategy ensures robust engineering and engenders trust in the systems and the processes surrounding their maintenance and development.

Appendices

1: Security Committee Charter; approved 14 March 2002. http://www.icann.org/committees/security/charter-14mar02.htm; verified May 26, 2004

2: Members of the Committee and Statements of Conflict of Interest

3: Message from Security and Stability Advisory Committee to ICANN Board, 22 September 2003; http://www.icann.org/correspondence/secsac-to-board-22sep03.htm; verified May 26, 2004

4: Correspondence between ICANN and VeriSign, Inc.

5: VeriSign Site Finder: Technical Review Panel Summary, Scott Hollenbeck, Director of Technology, VeriSign, in Site Finder Review, SECSAC Meeting, October 15, 2003, Washington, DC; http://www.icann.org/presentations/turner-secsac-dc-15oct03.pdf; verified May 26, 2004

6: IAB Commentary: Architectural Concerns on the use of DNS Wildcards, 19 September 2003; http://www.iab.org/documents/docs/2003-09-20-dns-wildcards.html; verified May 26, 2004

7: Museum Domain Management Association, Statement Concerning Wildcard "A" Records in Top-Level Domains, 6 October 2003; http://musedoma.museum/policy/wildcard/; verified May 26, 2004

Appendix 1: Security Committee Charter

Source: http://www.icann.org/committees/security/charter-14mar02.htm; downloaded, 7 June 2004

At its meeting on 14 March 2002, the ICANN Board approved the following charter for the ICANN Committee on Security and Stability:

Committee on Security and Stability
Charter

The Committee on Security and Stability will advise the ICANN community and Board on matters relating to the security and integrity of the Internet's naming and address allocation systems. Reporting directly to the Board, the Committee is chartered is to undertake the following tasks:

- To develop a security framework for Internet naming and address allocation services that defines the key focus areas, and identifies where the responsibilities for each area lie. The committee will focus on the operational considerations of critical naming infrastructure.

- To communicate on security matters with the Internet technical community and the operators and managers of critical DNS infrastructure services, to include the root name server operator community, the top-level domain registries and registrars, the operators of the reverse delegation trees such as in-addr.arpa and ip6.arpa, and others as events and developments dictate. The Committee will gather and articulate requirements to offer to those engaged in technical revision of the protocols related to DNS and address allocation and those engaged in operations planning.

- To engage 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 to advise the ICANN community accordingly. The Committee will recommend any necessary audit activity to assess the current status of DNS and address allocation security in relation to identified risks and threats.

- To communicate with those who have direct responsibility for Internet naming and address allocation security matters (IETF, RSSAC, RIRs, name registries, etc.), to ensure that its advice on security risks, issues, and priorities is properly synchronized with existing standardization, deployment, operational, and coordination activities. The Committee will monitor these activities and inform the ICANN community and Board on their progress, as appropriate.

- To report periodically to the Board on its activities.

To make policy recommendations to the ICANN community and Board.

Appendix 2: Members of the Committee and Statements of Conflict of Interest

Alain Patrick Aina

Alain Patrick Aina is chief executive officer of Technologies Reseaux & Solutions (www.trstech.net), a private company he founded in 2000, which provides networking services and training in Africa. He is a network expert and is one of the pioneers of the Internet in Africa, where he was a founding member of Africa Network Operators Group (AfNOG), forum in which he plays a significant role. He has built and helped build many networking infrastructures on the continent.

Alain Patrick Aina is not involved with VeriSign or with any companies doing business with VeriSign or with any companies competing with VeriSign.

Jaap Akkerhuis

Jaap Akkerhuis is full-time technical advisor for the Dutch not-for-profit top-level domain (TLD) registry SIDN (www.sidn.nl), which he joined after a short time at Surfnet, the Dutch academic ISP. While working at the CWI (Center for Mathematics & Informatics), he was instrumental in introducing Internet technology in the Netherlands and Europe. He then worked for Carnegie Mellon University, Mt. Xinu, AT&T Bell Laboratories and the first Dutch ISP NLnet (now a subsidiary of UUnet/MCI/etc.).

Jaap Akkerhuis has no personal financial interest in VeriSign or its subsidiaries. For the registry operation, SIDN has over 1,700 registrars such as Afilias and Global Registration Services (a VeriSign company). SIDN is also member of the ISC bind forum and receives (secondary) name service from ISC and Autonomica.

Steve Bellovin

Steven M. Bellovin joined AT&T Bell Laboratories in 1982; he is now at AT&T Labs Research, where he works on networks, security and related public policy questions. He is an AT&T Fellow and a member of the National Academy of Engineering. While still a graduate student, he helped create netnews for which he and his collaborators received the 1995 Usenix Lifetime Achievement Award.

Dr. Bellovin is the co-author of *Firewalls and Internet Security: Repelling the Wily Hacker*, and holds several patents on cryptographic and network protocols. He has served on many National Research Council (NRC) study committees, including those on information systems, trustworthiness, the privacy implications of authentication technologies, and cyber security research needs; he was also a member of the information technology subcommittee of an NRC study group on science versus terrorism. He was a member of the Internet Architecture Board (IAB) from 1996 to 2002. He is currently the co-director of the Security Area of the IETF.

Dr. Bellovin’s employer, AT&T, is a DNS registrar and a large ISP. As a member of the IESG, he has participated in IESG and IAB discussions of this issue.

Rob Blokzijl

Robert Blokzijl is a founding member of RIPE, the European open forum for IP networking. Since its foundation in 1989, he has been chairman of this organization, and was instrumental in the creation of RIPE NCC in 1992 as the first Regional Internet Registry in the world. Dr. Blokzijl has been active in building networks for the particle physics community in Europe and is currently employed by the National Institute of Nuclear Physics and High Energy Physics (NIKHEF).

Dr. Blokzijl was selected for the ICANN Board by the Address Supporting Organization. He served on the ICANN Board from October 1999 until December 2002.

David Conrad

David R. Conrad is chief technology officer at Nominum. In this role, he is responsible for Nominum's technical direction and strategy and guides the company's research and development efforts. Prior to joining Nominum, Mr. Conrad served as the executive director of the Internet Software Consortium (ISC) and president and chief executive officer of Internet Engines, Incorporated, was founder and first Director General of the Asia Pacific Network Information Centre (APNIC), and was employee number seven at Internet Initiative Japan (IIJ).

VeriSign is an investor in Nominum. Mr. Conrad was on the VeriSign RRP advisory board some time ago.

Steve Crocker, Chair

Stephen Crocker is chief executive officer and co-founder of Shinkuro, Inc., a start up company focused on controlled, secure, dynamic sharing of information across the Internet. He has been deeply involved in the Internet since its inception and remains active in the Internet standards work through the Internet Engineering Task Force (IETF) and IAB. In recognition of his contributions, which include organization of the Network Working Group, the forerunner of the IETF, and initiation of the Request for Comment (RFC) series, Dr. Crocker was awarded the 2002 IEEE Internet Award. He serves on many advisory boards and is a trustee of the Internet Society.

VeriSign holds the title to the intellectual property Dr. Crocker created during his tenure at CyberCash. Recently, VeriSign asked for his assistance in modifying a patent. Dr. Crocker removed himself from those discussions and asked one of the co-inventors of the intellectual property to interact with VeriSign instead. Those discussions terminated without action.

Johan Ihrén

Johan Ihrén is an employee of Autonomica AB, Sweden, a wholly owned subsidiary of Netnod AB, Sweden. Autonomica provides a number of DNS services, one of which is the operation and management of the Internet root name server i.root-servers.net.

Netnod also provides services to VeriSign, Inc, in the form of computer hosting and Internet connectivity to i.gtld-servers.net in Stockholm, which is an Internet name server managed and run by VeriSign, Inc.

Mark Kosters

Mark Kosters is currently vice president of research at VeriSign. He has been a senior engineer at Data Defense Network (DDN) NIC, chief engineer and Principal Investigator under the National Science Foundation (NSF)-sponsored Internet NIC (InterNIC), and has been involved in application design and implementation of client/server tools, router administration, UNIX system administration, database administration and network security. He has participated in various Internet technical forums and working groups such as the IETF, RIPE, APNIC and NANOG.

Mark Kosters is an employee of VeriSign. He participated in discussions on this topic and responded to questions about technical issues and the availability of pertinent information. He has not contributed to the preparation of this document, provided review comments, or had input into the findings and recommendations.

Allison Mankin

Allison Mankin is a senior research scientist at Bell Labs, Lucent Technologies, where she focuses on transport issues, voice-over-IP and their security. She also conducts research on future routing systems, emphasizing their transport issues. Previously, she was a principal investigator at University of Southern California/ Information Sciences Institute, where she pursued research on Internet topics including congestion control, video applications at very large scales, DNS authentication and IPv6 directions with funding from NSF, DARPA, Sprint Corporation and Microsoft Research. Ms. Mankin was one of the inventors of the MBONE and is very active in the IETF in a number of leadership roles.

Allison Mankin has no financial interest in VeriSign or its subsidiaries.

Ram Mohan

Ram Mohan is chief technology officer and vice president, business operations, for Afilias, a global registry services company. Afilias is the registry operator for the .INFO gTLD and provides registry services for the .ORG gTLD and ten other ccTLDs. Afilias Limited is an Irish corporation that has a broad shareholder base consisting of approximately 16 ICANN-accredited registrars and other firms, including VeriSign, Register.com, Tucows and Schlund. Mr. Mohan led the team that was responsible for the cutover of the .ORG registry from VeriSign Registry to Afilias in 2003. He participates in ICANN’s GNSO (Generic Names Supporting Organization) gTLD Registry Constituency, where he works with VeriSign and all other ICANN mandated registries on policy, technical and domain issues.

VeriSign does not own a controlling interest in Afilias, is not represented on the board of directors or executive committee, and does not influence or direct Afilias or Ram Mohan in any manner resulting from its minority shareholding. Mr. Mohan has owned shares of VeriSign (NASDAQ: VRSN), which were acquired on the public market, but he is not a controlling shareholder, officer or director of VeriSign.

Russ Mundy

Russ Mundy is currently a principal networking scientist at SPARTA, Inc. He performs research in the areas of Internet and network security, high assurance computing systems and protocol development; his primary research area is improving security of the Internet infrastructure. The primary technologies of Mr. Mundy's research are DNS security, secure network management, routing security and secure policy management.

Russ Mundy has no corporate or financial interests in any aspects of this report.

Jun Murai

Jun Murai is professor, Faculty of Environmental Information, Keio University (Japan); adjunct professor at the Institute of Advanced Studies, United Nations University; instructor at Tokyo University of Art and Music; president of the

Japan Network Information Center (JPNIC); general chairperson of the WIDE Project (a Japanese Internet research consortium); vice chairperson of the Japanese chapter of the Internet Society; and vice president of the Japanese Internet Association. Previously, he developed the Keio Science and Technology Network, and the Japan University UNIX Network (JUNET). His research has centered on electronic observation, satellite Internet, multimedia Internet and mobile and ubiquitous computing. Dr. Murai is a member of the board of the Internet Society.

Jun Murai has not provided information on conflicts of interest.

Frederico Neves

Frederico Neves is chief technology officer of Registro.br, the nonprofit registry service for .br ccTLD. He also acts as the engineering manager for LACNIC, the nonprofit Latin American and Caribbean Internet addresses registry.

Frederico Neves has no business dealings with VeriSign or its competitors.

Ray Plzak

Raymond Plzak is currently the president and chief executive officer of the American Registry for Internet Numbers (ARIN) and is a member of the board of trustees of the corporation. ARIN, a nonprofit organization, is one of four Regional Internet Registries (RIRs) worldwide that collectively provide Internet Number Resource registration services and reverse DNS services around the globe. Mr. Plzak has been involved in Internet registry operations since 1991. Prior to assuming his duties with ARIN in 2000, Mr. Plzak managed the DoD NIC. He has extensive experience in managing the allocation of Internet Number Resources and domain names, to include managing the .MIL domain and the “G” root server. Mr. Plzak is a past co-chair of the Domain Name System (DNS) Operation Working Group of the IETF and is the co-author/contributor of several RFCs. He is also a member of the Advisory Committee of the Internet Society and DNS Root Server System Advisory Committee (RSSAC).

Raymond A. Plzak is not and has never been an employee of VeriSign or one of its competitors.

Doron Shikmoni

Doron Shikmoni is co-founder and president of ForeScout Technologies, a private company providing enterprise network security products. He is also co-founder of ISOC-IL, the Israeli Internet Society chapter, where he served as president for a few years and is currently a board member. He leads ISOC-IL's infrastructure functions, managing the domain name registry for the .il ccTLD and the Israeli Internet Exchange. Mr. Shikmoni was instrumental in the creation of academic and later commercial networking in Israel. He consults for the government as well as private sector on security and networking, was the architect of the government's central secured Internet gateway, and serves on a standing advisory committee to the government on digital signatures.

Neither Doron Shikmoni, ForeScout Technologies nor ISOC-IL is affiliated with VeriSign, competes with VeriSign in any way, or has any vested commercial interest with relation to VeriSign.

Ken Silva

Ken Silva is vice president for networks and security for VeriSign, Inc. Since 2000, Mr. Silva has served both Network Solutions and VeriSign as manager of the resources dedicated to maintaining the security of its complex technology assets. He also represents VeriSign on a number of industry leadership capacities, including representing the company on working groups of the President's National Security Telecommunications Advisory Committee -- the "NSTAC", working groups of the NRIC, which advises the Federal Communications Commission, and as a board member of both the Internet Security Alliance and the "IT ISAC" -- the Information Technology sector's Information Sharing and Analysis Center.

Mr. Silva is an employee of VeriSign.

Bruce Tonkin

Bruce Tonkin is the chief technology officer of Melbourne IT. Melbourne IT is a domain name registrar. As a registry operator, VeriSign is a supplier of .com/.net names to Melbourne IT, and Internet services companies that were affected by the introduction of a wildcard in the .com/.net zone files are customers of Melbourne IT for domain name registration services. Mr. Tonkin is also the chair of Generic Names Supporting Organization (GNSO) of ICANN.

Bruce Tonkin chaired a group of internal VeriSign technical staff and external people to collate and address each of the issues that were raised by the community. The details of group can be found at http://www.verisign.com/nds/naming/sitefinder/trp.html

Paul Vixie

Paul Vixie is president of Internet Systems Consortium, Inc. (ISC), a nonprofit public benefit corporation which works in DNS software and operations. He is also a shareholder of Nominum, a commercial entity providing DNS software solutions.

Rick Wesson

Rick Wesson is the chief executive officer of Alice's Registry, Inc. an ICANN-accredited domain registrar, which funds open source projects and other causes. He has been involved in ICANN since its formation and has contributed to implementing IETF developed standards such as CRISP, EPP and RRP registry protocols.

Alice's Registry has several contracts with other domain registrars, ISPs, network providers and hosting providers. Mr. Wesson and Alice's Registry have no financial interest in VeriSign though Alice's Registry is an operational registrar actively registering domains in the VeriSign Com/Net Registry.

Appendix 3: Message from Security and Stability Advisory Committee to ICANN Board, 22 September 2003

Source: http://www.icann.org/correspondence/secsac-to-board-22sep03.htm; downloaded 7 June 2004

Message from Security and Stability Advisory Committee to ICANN Board 22 September 2003

ICANN Security and Stability Advisory Committee

BACKGROUND

On September 15, 2003, VeriSign changed the way its COM and NET name servers respond when presented with a query for a COM or NET domain name for when no name server record exists [1]. This change was reported on September 5, 2003 [2] and September 9, 2003 [3], but the implications of the change were not broadly recognized until it was deployed.

Previously, such queries returned RCODE 3 ("name error"), the negative response defined in the official DNS protocol specification, RFC1035 [4]. VeriSign now returns an IP address for a special server, thereby creating the appearance the requested domain name exists. The special server handles the subsequent requests for application level services, e.g. web, email, etc.

This special server is currently listening on port 80 for HTTP (web) and port 25 for SMTP (email) transactions. The web server returns a page indicating the domain name is not registered and offers search and/or registration services. The email server originally bounced all email with a 550 error code, which indicates a permanent failure and would result in the message being bounced back to the sender. Its precise behavior is still subject to change in response to community feedback, substantially changing the way email is queued, routed, and responded to in the COM and NET domains.

Applications or protocols which previously relied on an RCODE 3 response for a non-existing domain have suffered by this change in behavior for COM and NET. Workarounds at the routing and DNS level have been deployed to stop the effect of these wildcards, and these workarounds are an additional source of potential instability.

SECURITY AND STABILITY ISSUES

The Security and Stability Advisory Committee is examining the situation from several viewpoints.

- Conformance with the protocol specifications as defined by the engineering community.
- Conformance with accepted best practices and operational procedures as defined by the engineering and operational communities.
- Consideration of the technical stability and security of the domain name system and the Internet as a whole in light of the both the change introduced by VeriSign and the corresponding changes being introduced by others.
- Current procedural and governance controls to assure review and analysis of changes to the critical components of the Internet.
- Public confidence in the stability and reliable operation of the Internet. Security and stability is not limited to a narrow interpretation of the technical specifications of the protocol documents; it also includes engineering, operational, business, and policy issues.

To gather information on security and stability implications, we invite inputs from all interested parties. Send inputs to:

secsac-comment@icann.org

Further, we will meet publicly in the Washington, D.C. area on October 7, 2003, for interested parties to present factual information relevant to the security and stability of the Internet. Details will be available shortly.

Although we continue to gather inputs, there is already enough information to support the following opinions and recommendations.

OPINIONS

VeriSign's change appears to have considerably weakened the stability of the Internet, introduced ambiguous and inaccurate responses in the DNS, and has caused an escalating chain reaction of measures and countermeasures that contribute to further instability.

VeriSign's change has substantially interfered with some number of existing services which depend on the accurate, stable, and reliable operation of the domain name system.

- Many email configuration errors or temporary outages which were benign have become fatal now that the wildcards exist.
- Anti-spam services relied on the RCODE 3 response to identify forged email originators.
- In some environments the DNS is one of a sequence of lookup services. If one service fails the lookup application moves to the next service in search of the desired information. With this change the DNS lookup never fails and the desired information is never found.

VeriSign's action has resulted in a wide variety of responses from ISPs, software vendors, and other interested parties, all intended to mitigate the effects of the change. The end result of such a series of changes and counterchanges adds complexity and reduces stability in the overall domain name system and the applications that use it. This sequence leads in exactly the wrong direction. Whenever possible, a system should be kept simple and easy to understand, with its architectural layers cleanly separated.

We note that some networks and applications were performing similar services prior to VeriSign's change. In fact, some user applications and services worked differently depending on the network the user was using. However, VeriSign's change pushes this service to a much lower layer in the protocol stack and a much deeper place in the Internet's global infrastructure, which prevents the user from choosing what services to use and how to proceed when a query is made to a non-existent domain.

RECOMMENDATIONS

Recognizing the concerns about the wildcard service, we call on VeriSign to voluntarily suspend the service and participate in the various review processes now underway.

We call on ICANN to examine the procedures for changes in service, including provisions to protect users from abrupt changes in service.

We call on the IAB, the IETF, and the operational community to examine the specifications for the domain name system and consider whether additional specifications could improve the stability of the overall system. Most urgently, we ask for definitive recommendations regarding the use and operation of wildcard DNS names in TLDs and the root domain, so that actions and expectations can become universal. With respect to the broader architectural issues, we call on the technical community to clarify the role of error responses and on the separation of architectural layers, particularly and their interaction with security and stability.

[1] New York Times Announcement of VeriSign change
[2] Wall Street Journal report of VeriSign change
[3] Computer Business Review report of VeriSign change
[4] RFC1035, Domain Names - Implementation and Specification

Appendix 4: Correspondence between ICANN and VeriSign, Inc.

Source: http://www.icann.org/topics/wildcard-history.html, downloaded 7 June 2004

a. Advisory Concerning VeriSign's Deployment of DNS Wildcard Service (19 September 2003)
b. Advisory Concerning Demand to Remove VeriSign's Wildcard (3 October 2003)
c. Letter from Paul Twomey to Russell Lewis (3 October 2003)
d. Letter to VeriSign Regarding SECSAC Process (6 October 2003)

Appendix 4a: Advisory Concerning VeriSign's Deployment of DNS Wildcard Service (19 September 2003)

Source: http://www.icann.org/announcements/advisory-19sep03.htm

---

Advisory Concerning VeriSign's Deployment of DNS Wildcard Service

On 15 September 2003, VeriSign deployed a "wildcard" service into the .com and .net Top Level Domain zones. VeriSign's wildcard creates a registry-synthesized address record in response to lookups of domains that are not otherwise present in the zone (including restricted names, unregistered names, and registered but inactive names). The VeriSign wildcard redirects traffic that would otherwise have resulted in a "no domain" response to a VeriSign-operated website with search results and links to paid advertisements.

Since the deployment, ICANN has been monitoring community reaction, including analysis of the technical effects of the wildcard, and is carefully reviewing the terms of the .com and .net Registry Agreements.

In response to widespread expressions of concern from the Internet community about the effects of the introduction of the wildcard, ICANN has requested advice from its Security and Stability Advisory Committee, and from the Internet Architecture Board, on the impact of the changes implemented by VeriSign. ICANN's Security and Stability Advisory Committee is expected to release an objective expert report concerning the wildcard later today.

Recognizing the concerns about the wildcard service, ICANN has called upon VeriSign to voluntarily suspend the service until the various reviews now underway are completed.

Appendix 4b: Advisory Concerning Demand to Remove VeriSign's Wildcard (3 October 2003)

Source: http://www.icann.org/announcements/advisory-03oct03.htm

Advisory Concerning Demand to Remove VeriSign's Wildcard

On 15 September 2003, VeriSign unilaterally instituted a number of changes to the .com and .net Top Level Domain zones, including the deployment of a "wildcard" service. VeriSign's wildcard creates a registry-synthesized address record in response to lookups of domains that are not otherwise present in the zone (including reserved names, names in improper non-hostname format, unregistered names, and registered but inactive names). The VeriSign wildcard redirects traffic that would otherwise have resulted in a "no domain" response to a VeriSign-operated website with links to alternative choices and to a search engine.

Since that time, there have been widespread expressions of concern about the impact of these changes on the security and stability of the Internet, the DNS and the .com and .net domains. The Internet Architecture Board concluded that the changes made by VeriSign had a variety of impacts on third parties and applications, including (1) eliminating the display of "page not found" in the local language and character set of the users when given incorrect URLs rooted under these top-level domains, and instead causing those browsers to display an English language search page from a web server run by VeriSign; (2) causing all mail to non-existent hostnames in the .com and .net TLDs to flow to VeriSign's server (in addition to other effects on certain email programs and servers); (3) eliminating the ability of some applications to inform their users as to whether a domain name is valid before actually sending a communication; (4) rendering certain spam filters inoperable or ineffective; (5) affecting interaction with other protocols in a number of ways; (6) adversely affecting the performance of certain automated tools; (7) in some cases (where volume-based charging is applicable) increasing the user cost simply by increasing the size of the response to an incorrectly entered domain name; (8) creating a single point of failure that is likely to be attractive to deliberate attacks; (9) raising serious privacy issues; (10) interfering with standard approaches to reserved names; and (11) generating undesirable workarounds by affected third parties.

The combination of these effects, according to the IAB, "had wide sweeping effects on other users of the Internet far beyond those enumerated by the zone operator, created several brand new problems, and caused other internet entities to make hasty, possibly mutually incompatible and possibly deleterious (to the internet as a whole) changes to their own operations in an attempt to react to the change."

The ICANN Security and Stability Advisory Committee, consisting of approximately 20 technical experts from industry and academia, issued a statement on 22 September 2003 that concluded that:

VeriSign's change appears to have considerably weakened the stability of the Internet, introduced ambiguous and inaccurate responses in the DNS, and has caused an escalating chain reaction of measures and countermeasures that contribute to further instability.

VeriSign's change has substantially interfered with some number of existing services which depend on the accurate, stable, and reliable operation of the domain name system.

- Many email configuration errors or temporary outages which were benign have become fatal now that the wildcards exist.
- Anti-spam services relied on the RCODE 3 response to identify forged email originators.
- In some environments the DNS is one of a sequence of lookup services. If one service fails the lookup application moves to the next service in search of the desired information. With this change the DNS lookup never fails and the desired information is never found.

VeriSign's action has resulted in a wide variety of responses from ISPs, software vendors, and other interested parties, all intended to mitigate the effects of the change. The end result of such a series of changes and counterchanges adds complexity and reduces stability in the overall domain name system and the applications that use it. This sequence leads in exactly the wrong direction. Whenever possible, a system should be kept simple and easy to understand, with its architectural layers cleanly separated.

In addition, ICANN has received communications on this subject from the Internet Society, the .au Domain Administration (the operator of the .au (Australia) top level domain), AFNIC (the operator of the .fr top level domain), Public Interest Registry (the operator of the .org Top Level Domain), Melbourne IT (a large ICANN accredited registrar), the GNSO Registrars Constituency (the body that represents all ICANN-accredited registrars) and ICANN's At Large Advisory Committee, all expressing concerns about the impact and appropriateness of these changes. ICANN is also aware of communications from Register.com (another large ICANN registrar) and Cigref (an association that represents the 117 largest French Internet user companies) to VeriSign expressing similar concerns, and of the fact that at least three lawsuits have been filed challenging the specific changes introduced by VeriSign. Many of these communications are collected on the information page established by ICANN relating to VeriSign's wildcard deployment, http://www.icann.org/general/wildcard-history.htm. Finally, ICANN has established a separate comment list accessed at that same URL, and has received a significant number of comments from users, operators, and members of the business community such as Time Warner.

The scope and magnitude of these concerns would, in and of itself, counsel for return to the prior operation of .com and .net until all these issues can be reviewed and evaluated by those affected and those, like ICANN, charged with promoting Internet security and stability. This was the reason ICANN requested, on 19 September 2003, that VeriSign suspend its changes until these concerns could be properly considered. On 21 September 2003, VeriSign responded, refusing to honor that request.

In the 10 days since that response, ICANN has had further opportunity to consider the technical and practical consequences of these changes, and to evaluate whether these unilateral actions by VeriSign were consistent with its contractual obligations to ICANN. As set forth in today's letter to VeriSign, ICANN's preliminary conclusion is that the changes to .com and .net implemented by VeriSign on 15 September have had a substantial adverse effect on the core operation of the DNS, on the stability of the Internet and the .com and .net top-level domains, and may have additional adverse effects in the future. Further, VeriSign's actions are not consistent with its contractual obligations under the .com and .net registry agreements. The contractual inconsistencies include, violation of the Code of Conduct and equal access obligations agreed to by VeriSign, failure to comply with the obligation to act as a neutral registry service provider, failure to comply with the Registry-Registrar Protocol, failure to comply with domain registration limitations, and provision of an unauthorized Registry Service.

For all these reasons, ICANN has today insisted that VeriSign suspend the SiteFinder service, and restore the .com and .net top-level domains to the way they were operated prior to 15 September 2003. If VeriSign does not comply with this demand by 6:00 PM PDT on 4 October 2003, ICANN will be forced to take the steps necessary to enforce VeriSign's contractual obligations.

ICANN is sympathetic to concerns that have been expressed by VeriSign and others about the process by which proposed changes in the operation of a top-level domain registry are evaluated and approved by ICANN. To deal with these concerns, ICANN's President and CEO Paul Twomey is asking the Generic Names Supporting Organization to formulate a proposal for a timely, transparent and predictable procedure for the introduction of new registry services, including as to how a reasonable determination of the likelihood that a proposed change will have adverse effects. This process, to be conducted under the GNSO's new streamlined policy development process, should be completed by 15 January 2004.

Appendix 4c: Letter from Paul Twomey to Russell Lewis (3 October 2003)
Source: http://www.icann.org/correspondence/twomey-to-lewis-03oct03.htm

---

Letter from Paul Twomey to Russell Lewis
3 October 2003

3 October 2003

Via E-mail and U.S. Mail

Russell Lewis
Executive Vice President, General Manager
VeriSign Naming and Directory Services
21345 Ridgetop Circle LS2-3-2
Dulles, VA 20166-6503

Re: Deployment of SiteFinder Service

Dear Rusty:

This letter is further to the advisory posted by ICANN on 19 September 2003 regarding the changes to the operation of the .com and .net Top Level Domains announced by VeriSign on 15 September 2003, and in response to your letter of 21 September 2003. These changes involved the introduction (for the first time in the .com and .net domains) of a so-called "wildcard" mechanism that changes the expected error response for Internet traffic that would otherwise have resulted in a "no domain" response, and redirects that traffic to a VeriSign-operated webpage with links to alternative choices and to a search engine.

Because of numerous indications that these unannounced changes have had very significant impacts on a wide range of Internet users and applications, ICANN on 19 September 2003 asked VeriSign to voluntarily suspend these changes, and return to the previous behavior of .com and .net, until more information could be gathered on the impact of these changes. On 21 September 2003, VeriSign refused to honor that request. In the time since then, ICANN has had further opportunity to consider the technical and practical consequences of these changes, and to evaluate whether these unilateral actions by VeriSign were consistent with its contractual obligations to ICANN.

Based on the information currently available to us, it appears that these changes have had a substantial adverse effect on the core operation of the DNS, on the stability of the Internet, and on the relevant domains, and may have additional adverse effects in the future. These effects appear to be significant, including effects on web browsing, certain email services and applications, sequenced lookup services and a pervasive problem of incompatibility with other established protocols. In addition, the responses of various persons and entities to the changes made by VeriSign may themselves adversely affect the continued effective functioning of the Internet, the DNS and the .com and .net domains. Under these circumstances, the only prudent course of action consistent with ICANN's coordination mission is to insist that VeriSign suspend these changes pending further evaluation and study, including (but certainly not limited to) the public meeting already scheduled by ICANN's Security and Stability Advisory Committee on 7 October in Washington, D.C.

In addition, our review of the .com and .net registry agreements between ICANN and VeriSign leads us to the conclusion that VeriSign's unilateral and unannounced changes to the operation of the .com and .net Top Level Domains are not consistent with material provisions of both agreements. These inconsistencies include violation of the Code of Conduct and equal access provisions, failure to comply with the obligation to act as a neutral registry service provider, failure to comply with the Registry Registrar Protocol, failure to comply with domain registration provisions, and provision of an unauthorized Registry Service. These inconsistencies with VeriSign's obligations under the .com and .net registry agreements are additional reasons why the changes in question must be suspended pending further evaluation and discussion between ICANN and VeriSign.

Given these conclusions, please consider this a formal demand to return the operation of the .com and .net domains to their state before the 15 September changes, pending further technical, operational and legal evaluation. A failure to comply with this demand will require ICANN to take the steps necessary under those agreements to compel compliance with them.

Various press reports have quoted VeriSign representatives as being concerned about the processes by which changes in the operation of top-level domains are evaluated and approved by ICANN. I share those concerns. The introduction by registry operators of new products or services that do not threaten adverse effects to the Internet, the DNS or the top-level domains which they operate should not be impeded by unnecessary or prolonged processes. On the other hand, VeriSign, like other operators of top level domains, occupies a critical position of public trust, made even more important given the fact that it is the steward for the two largest generic top level domains. This means that VeriSign has both a legal and a practical obligation to be responsible in its actions in operating those top level domains.

To ensure that this obligation is carried out, there must be a timely, transparent and predictable process for the determination of the likelihood that a proposed change in the operation of a generic top-level domain under contract with ICANN will have significant adverse effects. To this end, I will be asking the GNSO to begin to create such a procedure, taking into particular account any comments submitted by other ICANN advisory bodies, liaisons, and constituencies. I will request the GNSO to make its recommendations no later than 15 January 2004.

If, during this period, further technical and operational evaluations of the changes made by VeriSign on 15 September indicate that those measures can be reinstated, or reinstated with modifications, without adverse effects, I will initiate the process to modify the .com and .net agreements to allow those changes to take place. We will use best efforts to complete these evaluations in a timely manner.

If, on the other hand, these ongoing evaluations confirm the claimed adverse effects on the Internet, the DNS or the .com and .net domains that have been publicized to date, or raise new concerns of that type, those concerns will have to be resolved prior to any reintroduction of these changes. If any such concerns cannot be resolved, and VeriSign continues to seek to implement the service, it will be necessary to make recourse to the dispute resolution provisions of the two agreements.

Given the magnitude of the issues that have been raised, and their potential impact on the security and stability of the Internet, the DNS and the .com and .net top level domains, VeriSign must suspend the changes to the .com and .net top-level domains introduced on 15 September 2003 by 6:00 PM PDT on 4 October 2003. Failure to comply with this demand by that time will leave ICANN with no choice but to seek promptly to enforce VeriSign's contractual obligations.

I look forward to VeriSign's compliance by the date specified.

Best regards,

Paul Twomey

President and CEO
ICANN

cc:
Chuck Gomes - Vice President, VeriSign Naming and Directory Services
Kevin Golden, Esq. - Senior Corporate Counsel, VeriSign, Inc.

Appendix 4d: Letter from Paul Twomey to VeriSign (6 October 2003)
Source: http://www.icann.org/correspondence/twomey-to-verisign-06oct03.htm

Letter from Paul Twomey to VeriSign
6 October 2003

Via E-mail and U.S. Mail

Russell Lewis
Executive Vice President, General Manager
VeriSign Naming and Directory Services
21345 Ridgetop Circle LS2-3-2
Dulles, VA 20166-6503

Re: Security and Stability Advisory Committee
- Review of VeriSign's Wildcard Implementation

Dear Rusty,

We are pleased that VeriSign has decided to "temporarily suspend" the core changes to the DNS and the related "SiteFinder" service (referred to collectively herein as the "Service Change") as of 4 October 2003, in response to the Internet community and ICANN's request for the full review of the related issues. As promised, we will now move quickly and carefully into a full technical and operational review of the matter.

This letter is written to explain the next steps in ICANN's technical review and evaluation of the Service Change, specifically as it involves ICANN's Security and Stability Advisory Committee (SECSAC) and the process that ICANN is pursuing so that we may reach conclusions regarding how to proceed in a timely fashion. This letter will respond only to the issues involving the technical review process and SECSAC activities and not to other issues raised in my correspondence to you of 3 October 2003 or the subsequent response by you relating to the same issues that evening.

As you are aware, in response to widespread expressions of concern from the Internet community, ICANN asked SECSAC and the Internet Architecture Board (IAB) to provide advice to ICANN immediately following the sudden introduction of the Service Change by VeriSign on 15 September 2003. SECSAC's responsibilities relating to this issue area are clear. In ICANN's ByLaws, Article XI, Section 2, Paragraph 2(a)(2) one of SECSAC's responsibilities is set out as follows: "To engage 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 to advise the ICANN community accordingly."

SECSAC has recently instituted two activities at the request of ICANN. These activities were commenced prior to VeriSign's agreement to "temporarily suspend" the Service Change, last Friday.

First, SECSAC collected information and sent a message to the ICANN Board of Directors on 22 September 2003 entitled "Recommendations Regarding VeriSign's Introduction of Wildcard Response to Uninstantiated Domains within COM and NET" (SECSAC Preliminary Recommendations). The SECSAC Preliminary Recommendations were issued one week after ICANN's request for a review and recommendation. The SECSAC Preliminary Recommendations of 22 September indicated among other things that:

"VeriSign's change appears to have considerably weakened the stability of the Internet, introduced ambiguous and inaccurate responses in the DNS, and has caused an escalating chain reaction of measures and countermeasures that contribute to further instability."

"VeriSign's change has substantially interfered with some number of existing services which depend on the accurate, stable, and reliable operation of the domain name system."

"Many email configuration errors or temporary outages which were benign have become fatal now that the wildcards exist."

"Anti-spam services relied on the RCODE 3 response to identify forged email originators."

"In some environments the DNS is one of a sequence of lookup services. If one service fails the lookup application moves to the next service in search of the desired information. With this change the DNS lookup never fails and the desired information is never found."

"VeriSign's action has resulted in a wide variety of responses from ISPs, software vendors, and other interested parties, all intended to mitigate the effects of the change. The end result of such a series of changes and counterchanges adds complexity and reduces stability in the overall domain name system and the applications that use it. This sequence leads in exactly the wrong direction. Whenever possible, a system should be kept simple and easy to understand, with its architectural layers cleanly separated."

The speed at which SECSAC evaluated the information available to them was commendable, and, as SECSAC noted itself, the work was preliminary and additional information was to be sought by SECSAC for its subsequent report to the board. Additional information gathering was also required in order to address the additional concerns raised in the document "IAB Commentary: Architectural Concerns on the Use of DNS Wildcards" issued by the IAB on 19 September 2003.

Secondly, SECSAC scheduled a special SECSAC Meeting, which is set for tomorrow, 7 October 2003 (referred to as the "7 October Meeting"), as formally announced by

ICANN on 30 September 2003. Unfortunately, the Service Change was still up and running when the 7 October Meeting was scheduled. If this had not been the case it is likely that additional time might have been provided to allow for a full opportunity for the issues to be reviewed in one SECSAC meeting.

As the Service Change was suspended in such close proximity to the time of the scheduled meeting, we now believe that the SECSAC Meeting should continue as scheduled, but that the data can be collected in multiple parts.

ICANN is setting out that the 7 October Meeting shall remain on schedule, and that a second meeting should be held two weeks later or at such a time as VeriSign is ready to state its full technical position (referred to as the "Second Meeting"). VeriSign is also formally requested to release its testing data from before, during and after the Service Change and to do so well in advance of the Second Meeting.

SECSAC has assured ICANN that the 7 October Meeting will be held with all due fairness, and that VeriSign will be provided an opportunity to ask questions, and to make a presentation. Although questions have been raised regarding the presenters and agenda for the 7 October Meeting, it is important to note that the membership of SECSAC was established prior to this current matter. The SECSAC Members are sufficiently diverse to ensure fairness in developing the agenda and presentations for the 7 October Meeting.

Additionally, it is assumed that during the following two weeks or at VeriSign's election during the latter presentation to SECSAC, VeriSign may offer refutations of the evidence and statements collected and made during the 7 October Meeting. SECSAC will also requests that VeriSign offer the SECSAC Members and other members of the Internet community the opportunity to question and to provide evidence refuting VeriSign's presentation and data during and following the Second Meeting.

Following the Second Meeting, SECSAC will hold open a time period to collect such additional information as might be provided to clarify remaining issues and concerns of VeriSign, SECSAC and the Internet community as a whole. SECSAC will then issue its more formal recommendation to ICANN, which will then decide along with other analysis data and/or dialogue among the relevant technical experts, as may be required, to permit, deny or place additional conditions upon VeriSign before it authorizes a re-launch of the SiteFinder service.

We look forward to continuing dialogue with VeriSign throughout this process to ensure that all issues and technical evaluation information is fully considered and weighed appropriately. We also would like to request that VeriSign consider and propose the most appropriate date and location of the Second Meeting, as soon as practicable.

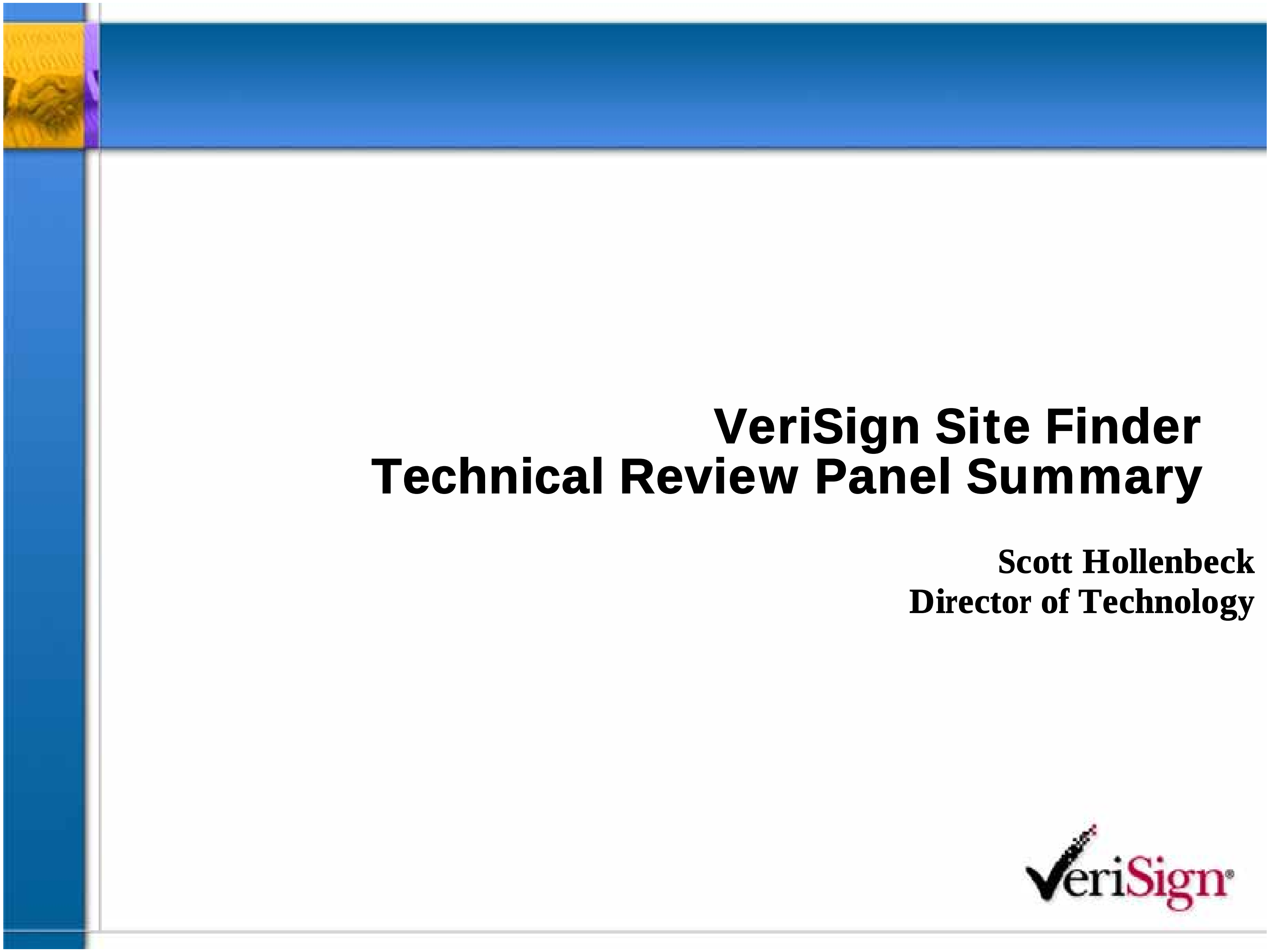
Sincerely,

Dr. Paul Twomey
President and CEO ICANN

cc: Steve Crocker, SECSAC
John Jeffrey, ICANN
James M. Ulam, VeriSign

Appendix 5: VeriSign Site Finder Technical Review Panel Summary

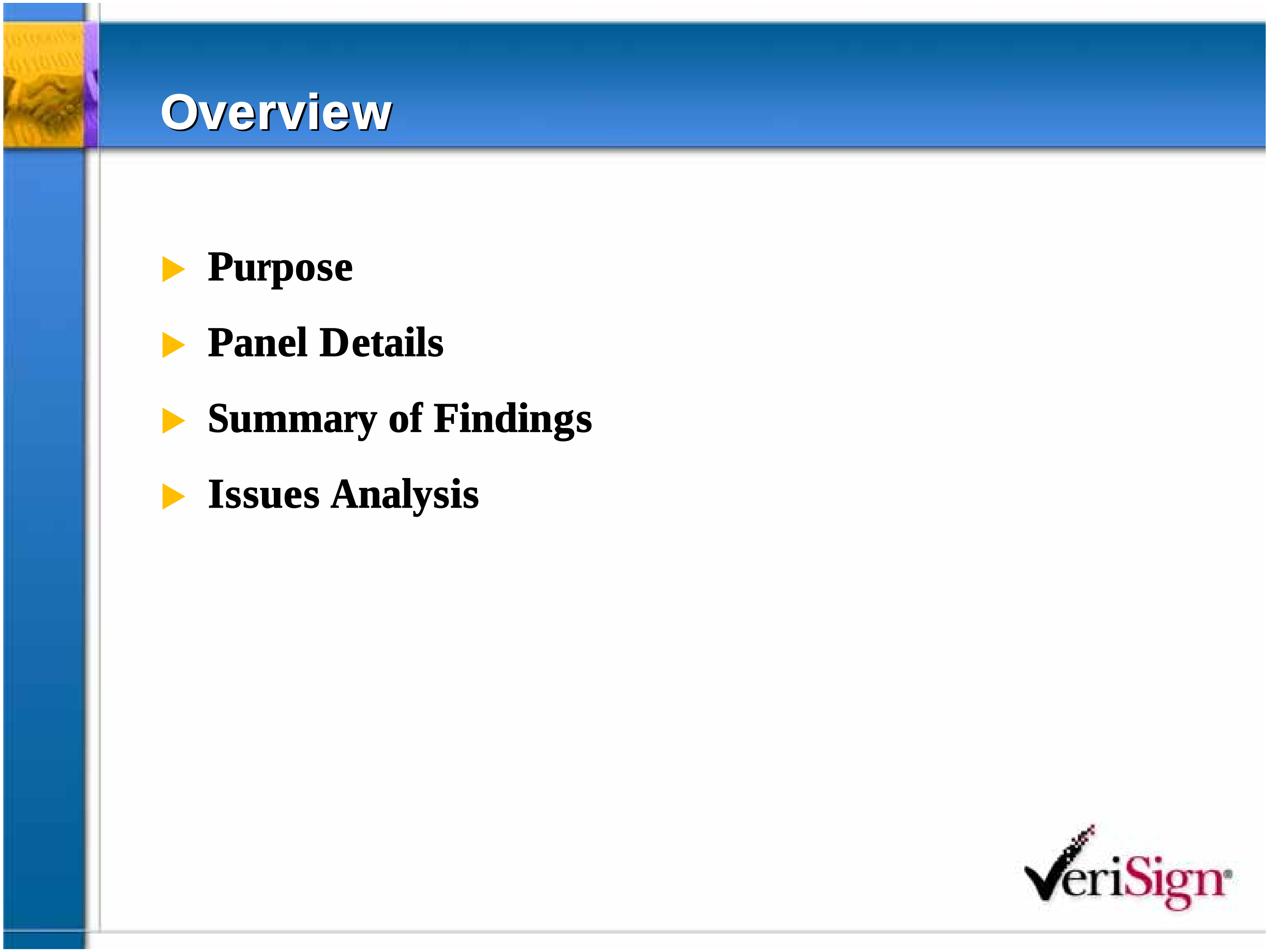
Scott Hollenbeck, Director of Technology, VeriSign, in Site Finder Review, SECSAC Meeting, October 15, 2003, Washington, D.C.
Source: http://www.icann.org/presentations/turner-secsac-dc-15oct03.pdf; downloaded 20 April 2003, verified May 26, 2004



VeriSign Site Finder
Technical Review Panel Summary

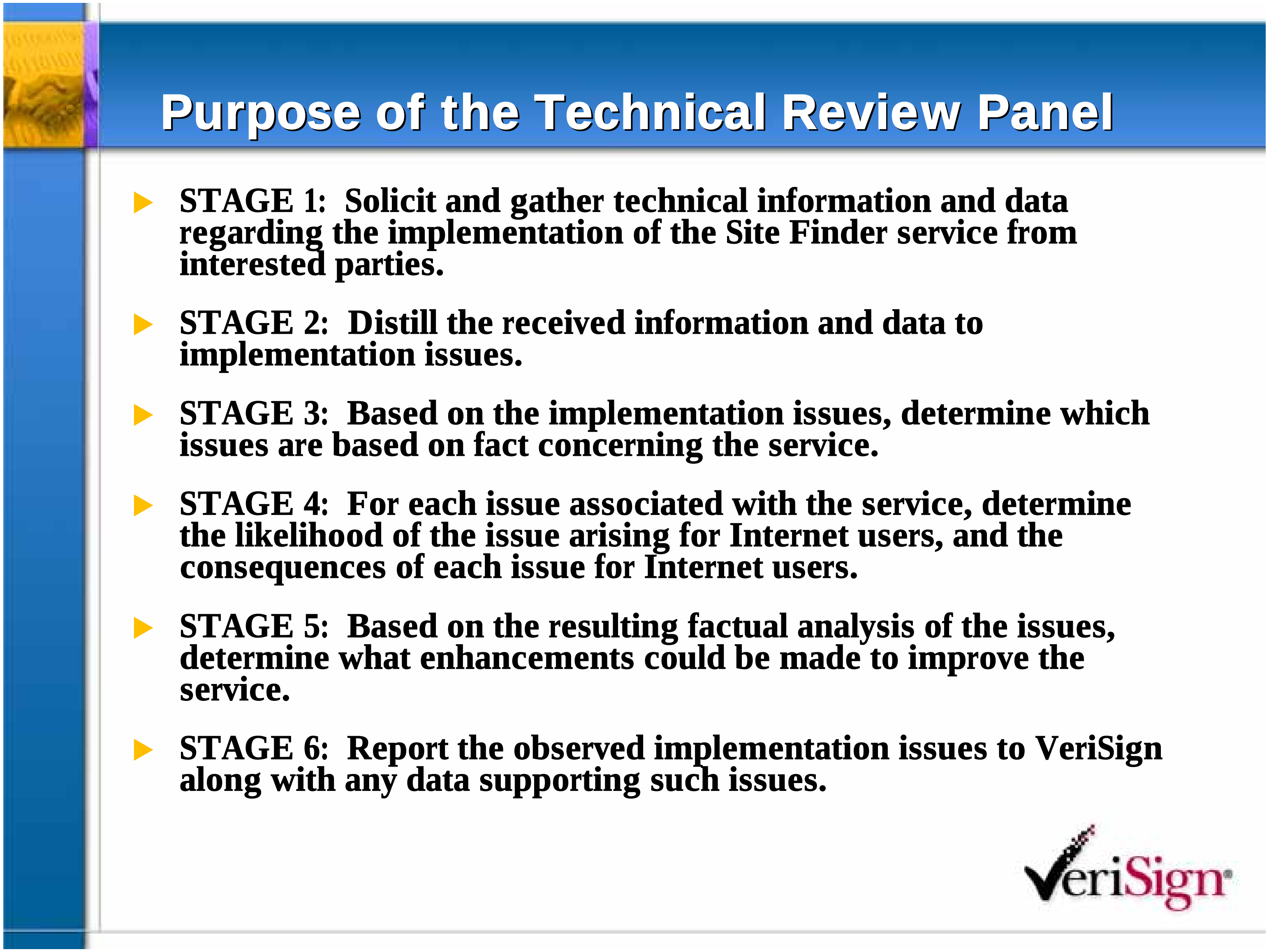
Scott Hollenbeck
Director of Technology

VeriSign®



Overview

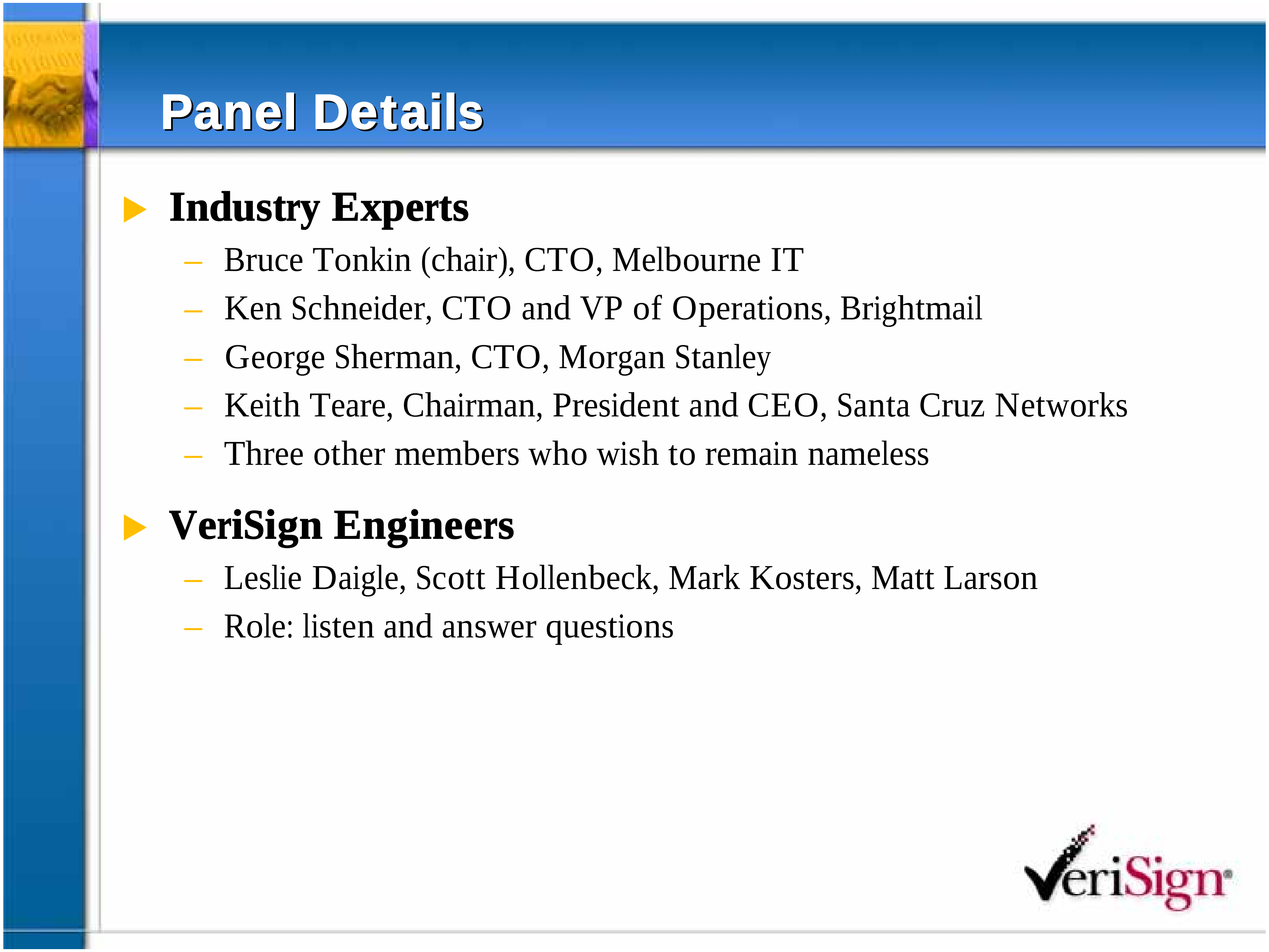
- Purpose
- Panel Details
- Summary of Findings
- Issues Analysis



Purpose of the Technical Review Panel

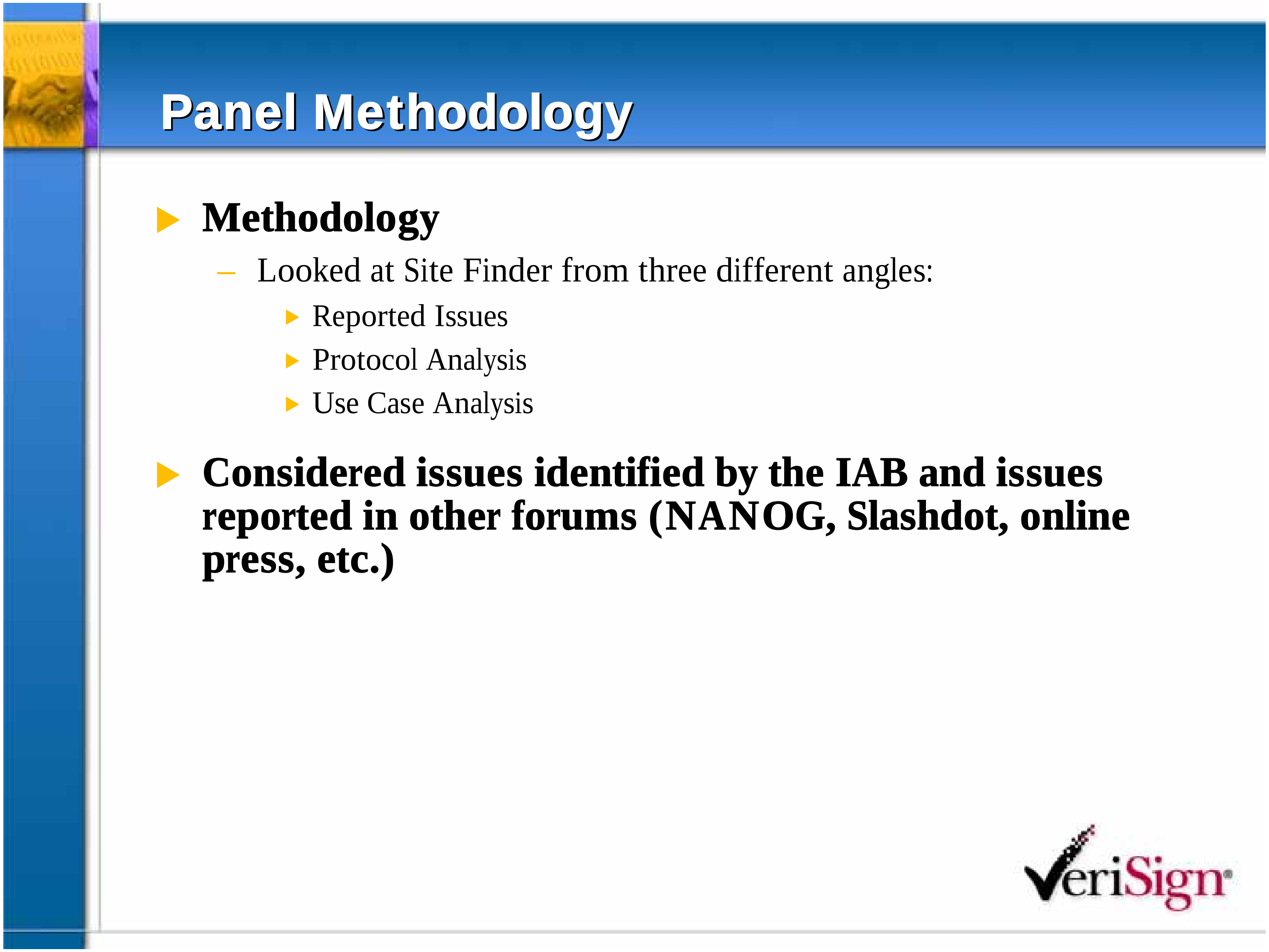
- STAGE 1: Solicit and gather technical information and data regarding the implementation of the Site Finder service from interested parties.
- STAGE 2: Distill the received information and data to implementation issues.
- STAGE 3: Based on the implementation issues, determine which issues are based on fact concerning the service.
- STAGE 4: For each issue associated with the service, determine the likelihood of the issue arising for Internet users, and the consequences of each issue for Internet users.
- STAGE 5: Based on the resulting factual analysis of the issues, determine what enhancements could be made to improve the service.
- STAGE 6: Report the observed implementation issues to VeriSign along with any data supporting such issues.

VeriSign



Panel Details

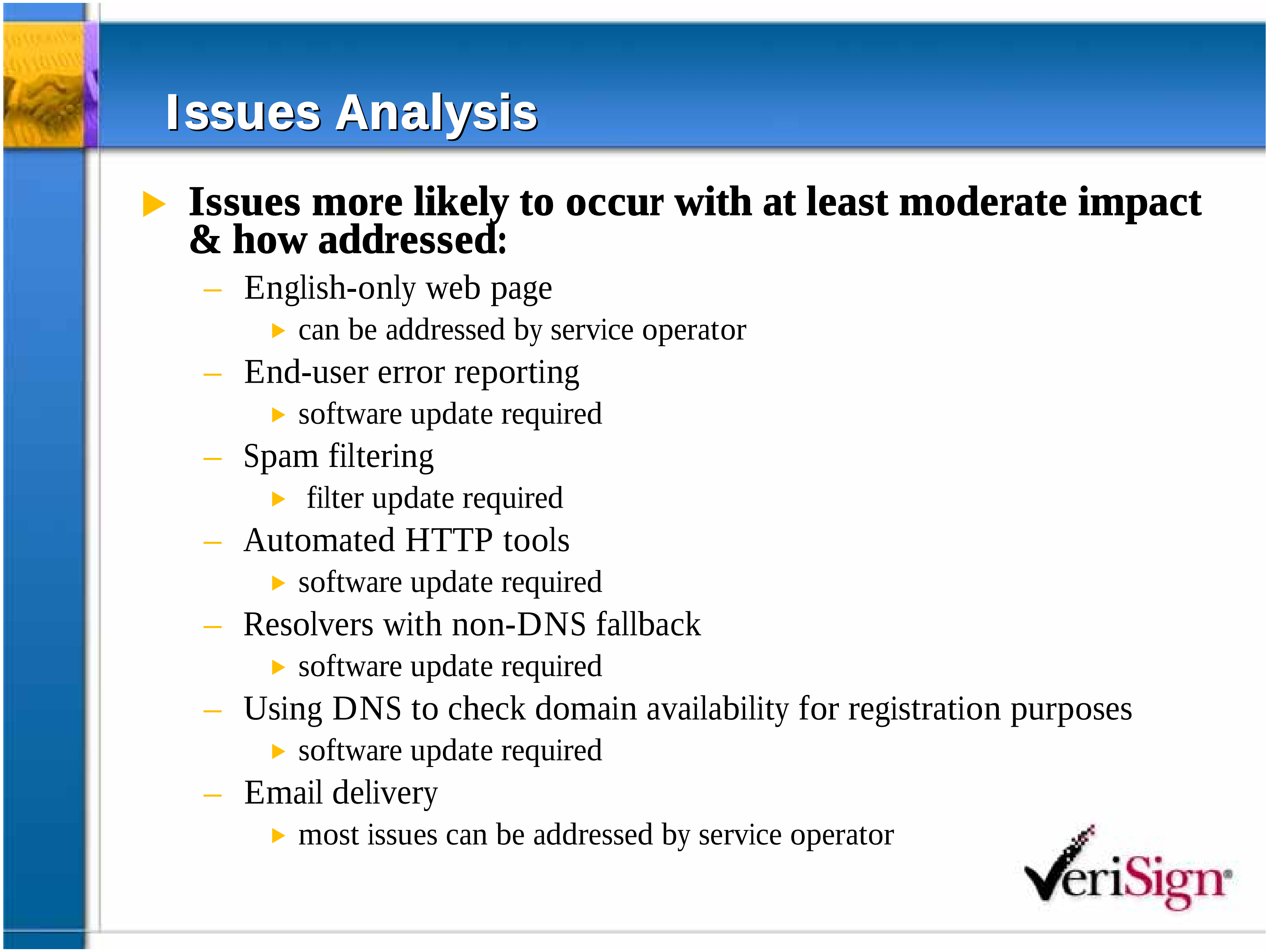
- **Industry Experts**
  - Bruce Tonkin (chair), CTO, Melbourne IT
  - Ken Schneider, CTO and VP of Operations, Brightmail
  - George Sherman, CTO, Morgan Stanley
  - Keith Teare, Chairman, President and CEO, Santa Cruz Networks
  - Three other members who wish to remain nameless
- **VeriSign Engineers**
  - Leslie Daigle, Scott Hollenbeck, Mark Kosters, Matt Larson
  - Role: listen and answer questions



Panel Methodology

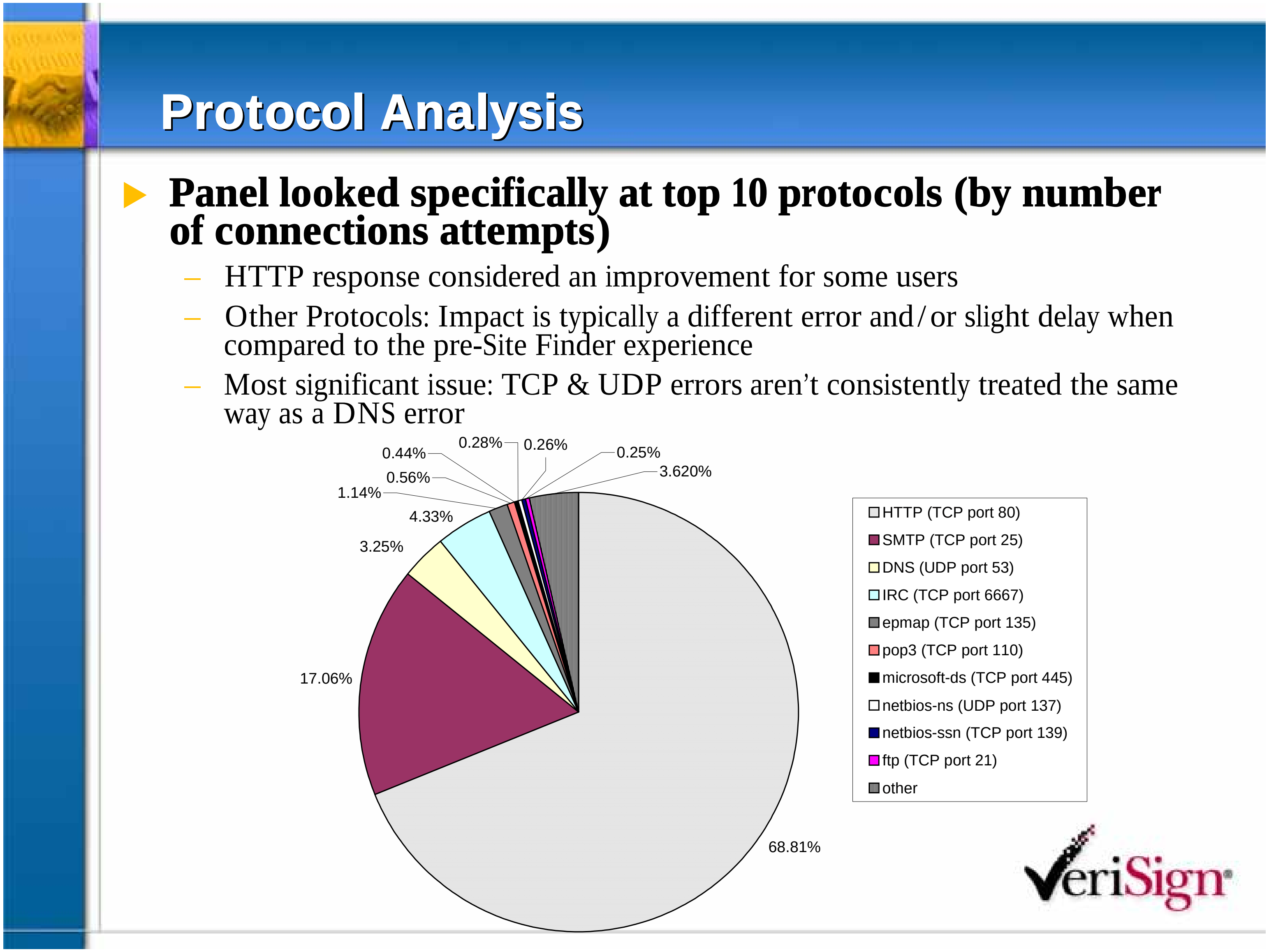
- **Methodology**
  - Looked at Site Finder from three different angles:
    - Reported Issues
    - Protocol Analysis
    - Use Case Analysis
- **Considered issues identified by the IAB and issues reported in other forums (NANOG, Slashdot, online press, etc.)**

VeriSign



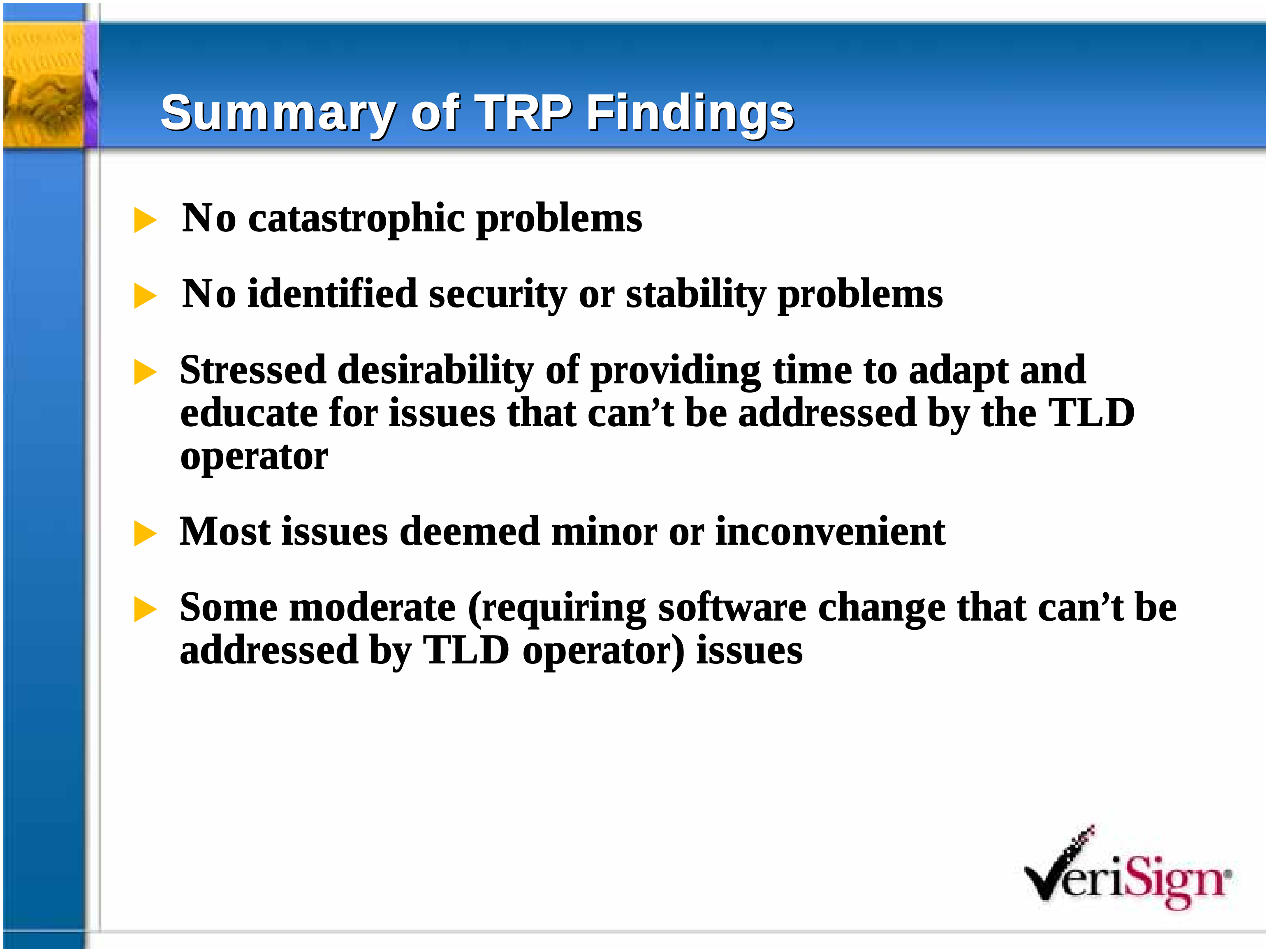
Issues Analysis

- **Issues more likely to occur with at least moderate impact & how addressed:**
  - English-only web page
    - can be addressed by service operator
  - End-user error reporting
    - software update required
  - Spam filtering
    - filter update required
  - Automated HTTP tools
    - software update required
  - Resolvers with non-DNS fallback
    - software update required
  - Using DNS to check domain availability for registration purposes
    - software update required
  - Email delivery
    - most issues can be addressed by service operator



Protocol Analysis

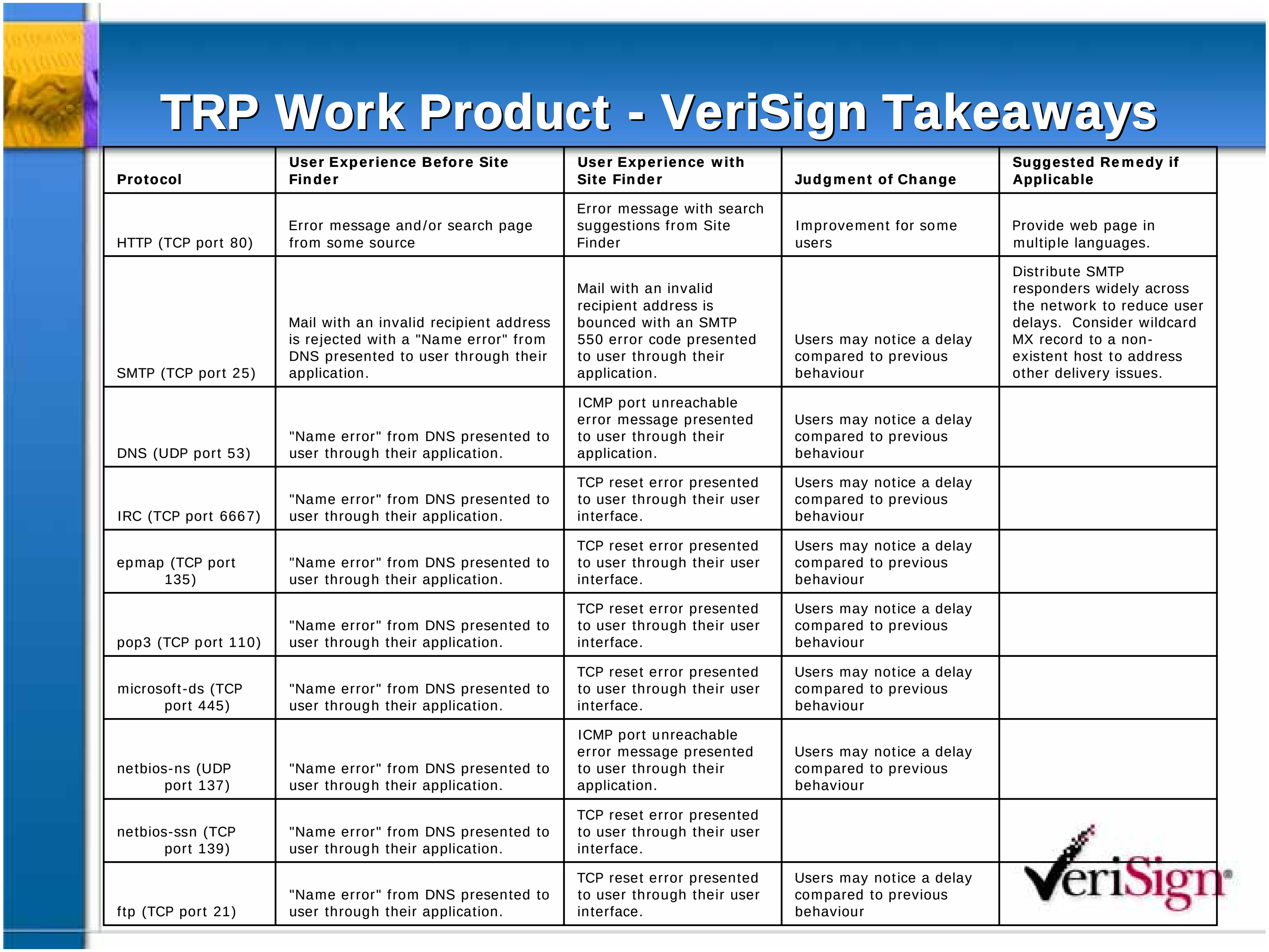
- Panel looked specifically at top 10 protocols (by number of connections attempts)
  - HTTP response considered an improvement for some users
  - Other Protocols: Impact is typically a different error and/or slight delay when compared to the pre-Site Finder experience
  - Most significant issue: TCP & UDP errors aren't consistently treated the same way as a DNS error



Summary of TRP Findings

- No catastrophic problems
- No identified security or stability problems
- Stressed desirability of providing time to adapt and educate for issues that can’t be addressed by the TLD operator
- Most issues deemed minor or inconvenient
- Some moderate (requiring software change that can’t be addressed by TLD operator) issues

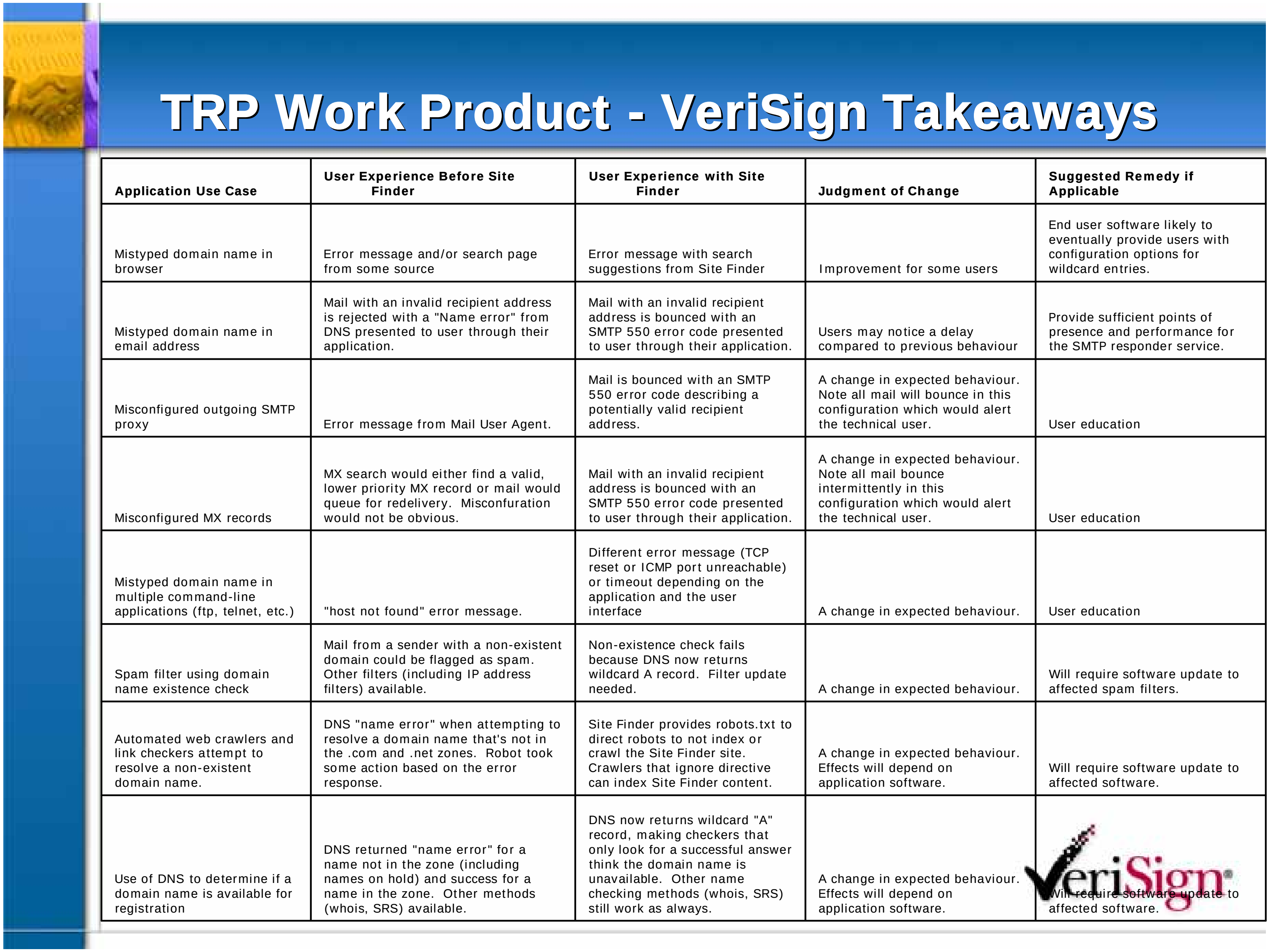
VeriSign



TRP Work Product - VeriSign Takeaways

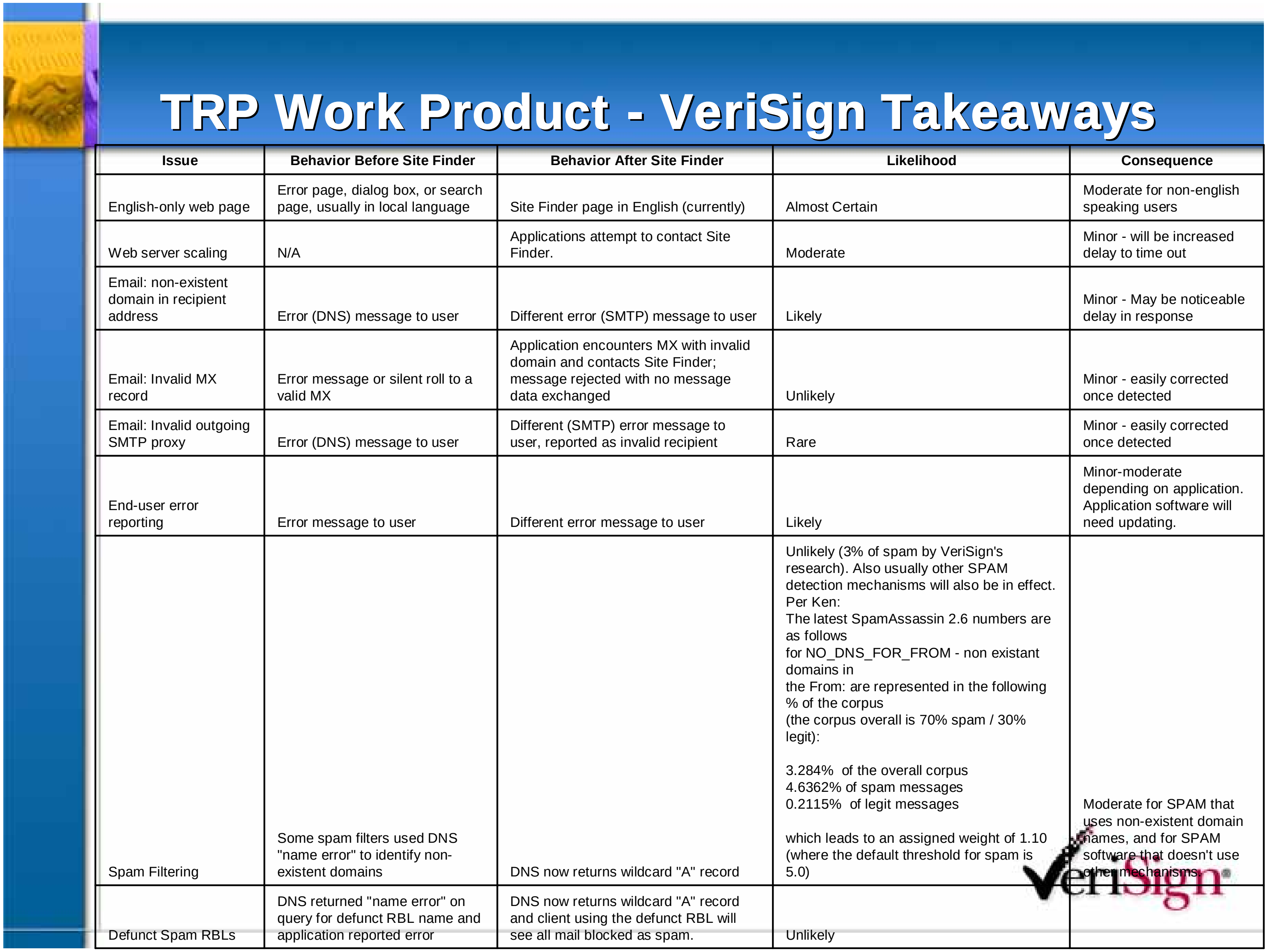
Protocol	User Experience Before Site Finder	User Experience with Site Finder	Judgment of Change	Suggested Remedy if Applicable
HTTP (TCP port 80)	Error message and/or search page from some source	Error message with search suggestions from Site Finder	Improvement for some users	Provide web page in multiple languages.
SMTP (TCP port 25)	Mail with an invalid recipient address is rejected with a "Name error" from DNS presented to user through their application.	Mail with an invalid recipient address is bounced with an SMTP 550 error code presented to user through their application.	Users may notice a delay compared to previous behaviour	Distribute SMTP responders widely across the network to reduce user delays. Consider wildcard MX record to a non-existent host to address other delivery issues.
DNS (UDP port 53)	"Name error" from DNS presented to user through their application.	ICMP port unreachable error message presented to user through their application.	Users may notice a delay compared to previous behaviour	
IRC (TCP port 6667)	"Name error" from DNS presented to user through their application.	TCP reset error presented to user through their user interface.	Users may notice a delay compared to previous behaviour	
epmap (TCP port 135)	"Name error" from DNS presented to user through their application.	TCP reset error presented to user through their user interface.	Users may notice a delay compared to previous behaviour	
pop3 (TCP port 110)	"Name error" from DNS presented to user through their application.	TCP reset error presented to user through their user interface.	Users may notice a delay compared to previous behaviour	
microsoft-ds (TCP port 445)	"Name error" from DNS presented to user through their application.	TCP reset error presented to user through their user interface.	Users may notice a delay compared to previous behaviour	
netbios-ns (UDP port 137)	"Name error" from DNS presented to user through their application.	ICMP port unreachable error message presented to user through their application.	Users may notice a delay compared to previous behaviour	
netbios-ssn (TCP port 139)	"Name error" from DNS presented to user through their application.	TCP reset error presented to user through their user interface.		
ftp (TCP port 21)	"Name error" from DNS presented to user through their application.	TCP reset error presented to user through their user interface.	Users may notice a delay compared to previous behaviour	

VeriSign®



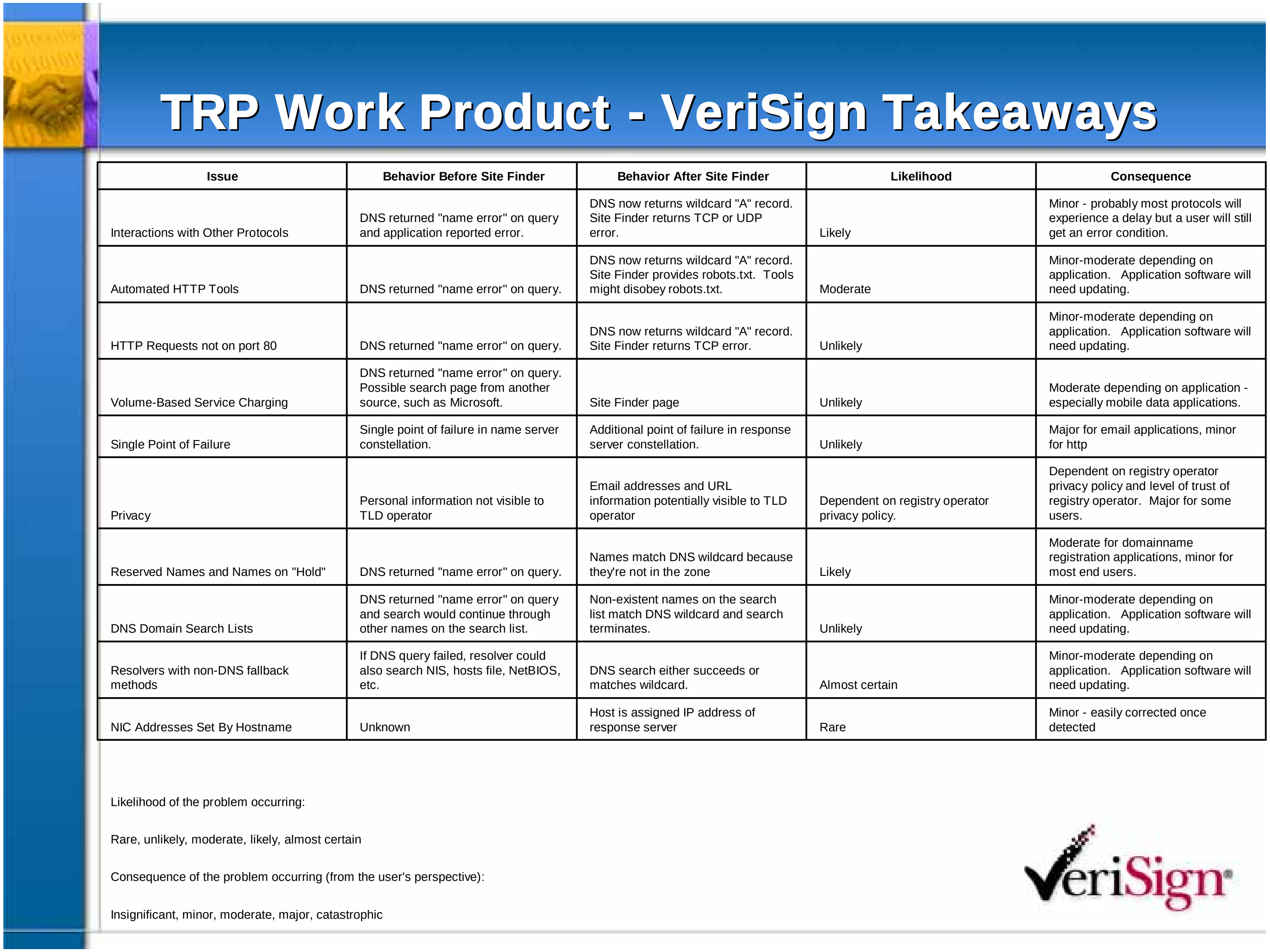
TRP Work Product - VeriSign Takeaways

Application Use Case	User Experience Before Site Finder	User Experience with Site Finder	Judgment of Change	Suggested Remedy if Applicable
Mistyped domain name in browser	Error message and/or search page from some source	Error message with search suggestions from Site Finder	Improvement for some users	End user software likely to eventually provide users with configuration options for wildcard entries.
Mistyped domain name in email address	Mail with an invalid recipient address is rejected with a "Name error" from DNS presented to user through their application.	Mail with an invalid recipient address is bounced with an SMTP 550 error code presented to user through their application.	Users may notice a delay compared to previous behaviour	Provide sufficient points of presence and performance for the SMTP responder service.
Misconfigured outgoing SMTP proxy	Error message from Mail User Agent.	Mail is bounced with an SMTP 550 error code describing a potentially valid recipient address.	A change in expected behaviour. Note all mail will bounce in this configuration which would alert the technical user.	User education
Misconfigured MX records	MX search would either find a valid, lower priority MX record or mail would queue for redelivery. Misconfuration would not be obvious.	Mail with an invalid recipient address is bounced with an SMTP 550 error code presented to user through their application.	A change in expected behaviour. Note all mail bounce intermittently in this configuration which would alert the technical user.	User education
Mistyped domain name in multiple command-line applications (ftp, telnet, etc.)	"host not found" error message.	Different error message (TCP reset or ICMP port unreachable) or timeout depending on the application and the user interface	A change in expected behaviour.	User education
Spam filter using domain name existence check	Mail from a sender with a non-existent domain could be flagged as spam. Other filters (including IP address filters) available.	Non-existence check fails because DNS now returns wildcard A record. Filter update needed.	A change in expected behaviour.	Will require software update to affected spam filters.
Automated web crawlers and link checkers attempt to resolve a non-existent domain name.	DNS "name error" when attempting to resolve a domain name that's not in the .com and .net zones. Robot took some action based on the error response.	Site Finder provides robots.txt to direct robots to not index or crawl the Site Finder site. Crawlers that ignore directive can index Site Finder content.	A change in expected behaviour. Effects will depend on application software.	Will require software update to affected software.
Use of DNS to determine if a domain name is available for registration	DNS returned "name error" for a name not in the zone (including names on hold) and success for a name in the zone. Other methods (whois, SRS) available.	DNS now returns wildcard "A" record, making checkers that only look for a successful answer think the domain name is unavailable. Other name checking methods (whois, SRS) still work as always.	A change in expected behaviour. Effects will depend on application software.	Will require software update to affected software.



TRP Work Product - VeriSign Takeaways

Issue	Behavior Before Site Finder	Behavior After Site Finder	Likelihood	Consequence
English-only web page	Error page, dialog box, or search page, usually in local language	Site Finder page in English (currently)	Almost Certain	Moderate for non-english speaking users
Web server scaling	N/A	Applications attempt to contact Site Finder.	Moderate	Minor - will be increased delay to time out
Email: non-existent domain in recipient address	Error (DNS) message to user	Different error (SMTP) message to user	Likely	Minor - May be noticeable delay in response
Email: Invalid MX record	Error message or silent roll to a valid MX	Application encounters MX with invalid domain and contacts Site Finder; message rejected with no message data exchanged	Unlikely	Minor - easily corrected once detected
Email: Invalid outgoing SMTP proxy	Error (DNS) message to user	Different (SMTP) error message to user, reported as invalid recipient	Rare	Minor - easily corrected once detected
End-user error reporting	Error message to user	Different error message to user	Likely	Minor-moderate depending on application. Application software will need updating.
Spam Filtering	Some spam filters used DNS "name error" to identify non-existent domains	DNS now returns wildcard "A" record	Unlikely (3% of spam by VeriSign's research). Also usually other SPAM detection mechanisms will also be in effect. Per Ken: The latest SpamAssassin 2.6 numbers are as follows for NO_DNS_FOR_FROM - non existant domains in the From: are represented in the following % of the corpus (the corpus overall is 70% spam / 30% legit): 3.284% of the overall corpus 4.6362% of spam messages 0.2115% of legit messages which leads to an assigned weight of 1.10 (where the default threshold for spam is 5.0)	Moderate for SPAM that uses non-existent domain names, and for SPAM software that doesn't use other mechanisms.
Defunct Spam RBLs	DNS returned "name error" on query for defunct RBL name and application reported error	DNS now returns wildcard "A" record and client using the defunct RBL will see all mail blocked as spam.	Unlikely	



TRP Work Product - VeriSign Takeaways

Issue	Behavior Before Site Finder	Behavior After Site Finder	Likelihood	Consequence
Interactions with Other Protocols	DNS returned "name error" on query and application reported error.	DNS now returns wildcard "A" record. Site Finder returns TCP or UDP error.	Likely	Minor - probably most protocols will experience a delay but a user will still get an error condition.
Automated HTTP Tools	DNS returned "name error" on query.	DNS now returns wildcard "A" record. Site Finder provides robots.txt. Tools might disobey robots.txt.	Moderate	Minor-moderate depending on application. Application software will need updating.
HTTP Requests not on port 80	DNS returned "name error" on query.	DNS now returns wildcard "A" record. Site Finder returns TCP error.	Unlikely	Minor-moderate depending on application. Application software will need updating.
Volume-Based Service Charging	DNS returned "name error" on query. Possible search page from another source, such as Microsoft.	Site Finder page	Unlikely	Moderate depending on application - especially mobile data applications.
Single Point of Failure	Single point of failure in name server constellation.	Additional point of failure in response server constellation.	Unlikely	Major for email applications, minor for http
Privacy	Personal information not visible to TLD operator	Email addresses and URL information potentially visible to TLD operator	Dependent on registry operator privacy policy.	Dependent on registry operator privacy policy and level of trust of registry operator. Major for some users.
Reserved Names and Names on "Hold"	DNS returned "name error" on query.	Names match DNS wildcard because they're not in the zone	Likely	Moderate for domainname registration applications, minor for most end users.
DNS Domain Search Lists	DNS returned "name error" on query and search would continue through other names on the search list.	Non-existent names on the search list match DNS wildcard and search terminates.	Unlikely	Minor-moderate depending on application. Application software will need updating.
Resolvers with non-DNS fallback methods	If DNS query failed, resolver could also search NIS, hosts file, NetBIOS, etc.	DNS search either succeeds or matches wildcard.	Almost certain	Minor-moderate depending on application. Application software will need updating.
NIC Addresses Set By Hostname	Unknown	Host is assigned IP address of response server	Rare	Minor - easily corrected once detected

Likelihood of the problem occurring:

Rare, unlikely, moderate, likely, almost certain

Consequence of the problem occurring (from the user's perspective):

Insignificant, minor, moderate, major, catastrophic

VeriSign®

Appendix 6: IAB Commentary: Architectural Concerns on the use of DNS Wildcards, 19 September 2003

Source: http://www.iab.org/documents/docs/2003-09-20-dns-wildcards.html; downloaded 7 June 2004

This document contains a number of observations on the implications of the use of wildcards in DNS zones, and makes some recommendations concerning their use.

The contact person for the IAB on this statement is Harald Alvestrand

19 September 2003

IAB Commentary: Architectural Concerns on the use of DNS Wildcards

There are many architectural assumptions regarding DNS behavior that are not specified in the IETF standards documents describing DNS, but which are deeply embedded in the behavior of Internet protocols and applications. These assumptions are inherent parts of the network architecture of which the DNS is one component.

It has long been known that it is possible to use DNS wildcards in ways that violate these assumptions.

Recent deployments of DNS wildcards with A records at high levels in the DNS tree have shown by experience that the cost of violating these assumptions is significant. In this document we provide an explanation of how DNS wildcards function, and many examples of how their injudicious use negatively impacts both individual Internet applications and indeed the Internet architecture itself.

In particular, we recommend that DNS wildcards should not be used in a zone unless the zone operator has a clear understanding of the risks, and that they should not be used without the informed consent of those entities which have been delegated below the zone.

A brief primer on DNS wildcards

The DNS "wildcard" mechanism has been part of the DNS protocol since the original specifications were written twenty years ago, but the capabilities and limitations of wildcards are sufficiently tricky that discussions of both the protocol details of precisely how wildcards should be implemented and the operational details of how wildcards should or should not be used continue to the present day. This section attempts to explain the essential details of how wildcards work, but readers should refer to the DNS specifications ([RFC 1034] et sequentia) for the full details.

In essence, DNS wildcards are rules which enable an authoritative name server to synthesize DNS resource records on the fly. The basic mechanism is quite simple, the complexity is in the details and implications.

The most basic and by far the most common operation in the DNS protocols is a simple query for all resource records matching a given query name, query class, and query type. Assuming (for simplicity) that all the software and networks involved are working correctly, such a query will produce one of three possible results:

> *success*
> If the system finds a match for all three parameters, it returns the matching set of resource records;
>
> *no data*
> If the system finds a match for the query name and query class but not for the query type, it returns an indication that the name exists but no data matching the given query type is present.
>
> *no such name*
> If the system fails to find a match for the given query name and query class, it returns an indication that the name does not exist.

Ordinarily, matches for all three parameters must be exact. This is where wildcards come into the picture.

A wildcard record is an otherwise ordinary DNS resource record whose leftmost (least significant) label consists of a single asterisk ("*") character, such as "*.bar.example". Conceptually, the asterisk matches one or more labels at the left (least significant) end of the DNS name.

When wildcard records are present, the rules become more complicated. Specifically, if the query class matches, there is no exact match for the query name, and the closest match for the query name is a wildcard, the system in effect synthesizes a set of resource records matching the query name on the fly by treating the resource records present at the wildcard name as if they had been present at the query name. Thus, if the wildcard name has records matching the desired query type, the system will return those records, precisely as in the "success" case above; otherwise, the system will return an indication that the name exists but no data matching the given query type is present, precisely as in the "no data" case above. The response is identical to that of a normal "success" response for the query name, so the resolver which issued the query can not tell that the results it got back were the result of wildcard expansion.

Note that, in the case of a wildcard match, the "no such name" case cannot occur; the wildcard match eliminates this possibility. Note also that only the query name and query class matter for purposes of determining whether a wildcard matches: any record type can produce a wildcard match, regardless of whether or not the record type happens to match the query type.

Problems with Wildcard Records

One of the main known weaknesses and dangers of wildcard records is that they interact poorly with any use of the DNS which depends on "no such name" responses. The list of such uses turns out to be quite large, and will be discussed in some detail in a later section.

Another known weakness and danger of wildcard records stems from the fact that the wildcard label will match anything at all, so long as no non-wildcard name within the zone is a closer match to the query name than the wildcard is. This doesn't sound like a major problem until one considers the number of conventions and, in some cases, protocols, which use labels at the left (least significant) ends of the names of resource records to distinguish between records associated with different services, rather than using different types of records. That is, in these cases, otherwise unrelated services use the same type of record and clients (or users) are expected to use the name corresponding to the particular service desired. This applies both to the ad-hoc naming conventions described in [RFC 2219] such as www.foo.example and also to mechanisms such as the SRV record type [RFC 2782] in which the naming scheme is part of the formal protocol.

When names of this type are covered by wildcards such as an address record named *.bar.example, such a wildcard would hand back the same address record regardless of the service name encoded in the query name, thus ftp.foo.bar.example, mail.foo.bar.example, ntp.foo.bar.example and so forth would all end up with the same synthesized address record. This problem is even worse in the SRV case, both because names such as _finger._tcp.foo.bar.example are part of the protocol and because SRV records include TCP and UDP port numbers, so the client will be confused not only about which host it should contact but also about the port on which it should contact that host. The only way to avoid these problems with names of this type is to add explicit records for such names to the DNS.

Finally, the two factors listed above ("match anything" behavior, and poor interaction with anything that depends on "no such name" responses) interact with normal and predictable human errors to allow wildcards to have effects far beyond their intended scope. Properly speaking, a wildcard record's scope is limited to a single zone, since, by definition, a wildcard record never matches any name that really does exist in the zone, and thus will not match any (non-wildcard) delegation of a portion of the namespace from a parent zone to its child. (Wildcard NS records, while theoretically possible, have sufficiently bizarre semantics that it is probably best to limit their use to torture-tests of DNS software.) So, at first blush, it would seem that the administrator of a zone is free to use wildcards without worrying about effects which this might have on the zone's delegated children. Unfortunately, this turns out not to be the case, because DNS names are heavily exposed in user interfaces, and users, being humans, make mistakes. So, while delegating the bar.example zone will prevent a wildcard record *.example from affecting a user who typed foo.bar.example as foi.bar.example, it will not prevent the same wildcard record from affecting the same user when the error is foo.bat.example. Thus, from the users' point of view, some of the effects of wildcards do leak from a parent zone to its children. This is not a big deal if the parent and child zones are associated with a single organization, but it can become a real problem if the parent and child zones are associated with different organizations whose interests are not perfectly aligned.

The above is probably not an exhaustive list. Even after twenty years of experience with the DNS, the effects of unexpected uses of wildcards can still be quite surprising, because the small but fundamental way in which they change the record lookup rules has a nasty way of violating implicit (or, sometimes, explicit) assumptions in deployed DNS-using software.

For these reasons, almost all use of DNS wildcards has been limited to a relatively small number of reasonably well-understood roles, and most wildcard use has been limited to a single role: the MX records used in mail delivery.

Since MX records are only used for electronic mail delivery, wildcard MX records are relatively safe, and since electronic mail for any particular DNS name is generally handed by the organization that is furthest down the delegation tree, wildcard MX records are most likely to appear in zones where their effects will not cross organizational boundaries. While the latter is not universally true, the primary use of wildcard records has been and remains wildcard MX records for handling an organization's own mail. Given these issues, it seems clear that the use of wildcards with record types that affect more than one protocol should be approached with caution, that the use of wildcards in situations where their effects cross organizational boundaries should also be approached with caution, and that the use of wildcards with record types that affect more than one protocol in situations where the effects cross organizational boundaries should be approached with extreme caution, if at all.

Principles To Keep In Mind

In reading the rest of this document, it may be helpful to bear in mind two basic principles of architectural design which have served the Internet well for many years:

- *The Robustness Principle*: "Be conservative in what you do, be liberal in what you accept from others." [Jon Postel, RFC 793]
- *The Principle Of Least Astonishment*: A program should always respond in the way that is least likely to astonish the user. [Traditional, original source unknown]

We will come back to these points after the next section.

Problems encountered in recent experiences with wildcards

We have recently had the opportunity to observe the results of the introduction of the use of wildcards in large and well-established top-level domains, with some rather undesirable and unintended consequences. This section attempts to detail some of the problems that network users and operators around the world encountered as a result of this deployment.

We must emphasize that, technically, this was a legitimate use of wildcard records that did not in any way violate the DNS specifications themselves. One of our main points here is that simply complying with the letter of the protocol specification is not sufficient to ensure the operational stability of the applications which depend on the DNS: there are protocol features which simply are not safe to use in some circumstances.

The specific change which this operator chose to make was to add a single wildcard address record at the zone apex of each of the affected zones. As a direct result of this change, two things happened:

1. the authoritative servers for these two zones no longer give out "no such name" responses for any possible name in these zones, and
2. every possible name rooted in one of these zones which, until this change, did not exist at all, now has a synthesized address record pointing at a "redirection server" run by the operator of this zone.

The implications of this simple change were many and varied. The list below is almost certainly incomplete:

Web Browsing

Web browsers all over the world stopped displaying "page not found" in the local language and character set of the users when given incorrect URLs rooted under these TLDs. Instead, these browsers now display an English language search page from a web server run by the zone operator.

It should be noted that the language tags in the HTTP protocol do not always match the locale used in the local browser. So, even though the global search page is dynamic and uses the information in the HTTP request to guess what language and script is to be used -- it will never be able to emulate what the user expected. There is, in short, not enough context in the HTTP protocol for the engine which generates the search page.

In many situations, web browsers have been written to provide some assistance to the user, often based on local conventions, directories, and language, when a DNS lookup fails. All such systems are now disabled for URLs rooted under these TLDs, since DNS lookups no longer fail, even when the specified destination does not exist.

Even if these were acceptable changes, the new mechanism has poor scaling properties, and unless the operator chooses to invest significant resources in maintaining a large, robust web server setup, the user experience is going to get even worse: instead of either a local language error message or an English search page, the user is going to get "attempting to connect..." followed by a long wait.

Email

All mail to non-existent hostnames under these TLDs now flows to the registry operator's server, where the registry operator bounces it. Some operators find this intolerable and have changed their mail system configurations to bypass this "bounce service", but the vast majority of mail servers undoubtedly now route mail for nonexistent names under these TLDs to the bounce server rather than just bouncing it directly. This has a number of ramifications:

- If operators choose to allow their mail to go to the bounce server, they now have an increased mail load handling additional routing of messages to the bounce server; if operators choose not to allow this to happen, they have an additional development and maintenance burden configuring their servers to prevent it.
- Operators who allow mail to go to the bounce server are now dependent on the performance of the bounce server. If the bounce server ever slows or fails, mail that previously would bounce will now queue at the SMTP relay for that relay's queue time before bouncing back to the user. This creates a very poor user experience, since typographical errors that in the past would have bounced immediately may now go unnoticed for several days.
- Operators who allow mail to go to the bounce server are also dependent on the correct operation of the bounce server. If the bounce server is buggy (which happened to be the case with this rollout), mail may not bounce at all: it may be reported to the user as having been delivered correctly while actually vanishing without a trace. This also creates a very poor user experience.
- In some cases where the set of MX records associated with a particular DNS name included a misconfigured record pointing to a nonexistent hostname, installing these wildcard records was the last straw that broke a misconfigured-but-functional mail configuration: previously, the nonexistent hostname would have failed to resolve and been ignored, now it bounces.
- The normal flow of data from a client in SMTP when one address has a typo is as follows:

    1. The client looks up the IP address of his outgoing SMTP proxy in DNS.
    2. The client opens a TCP connection to his outgoing SMTP proxy.
    3. The client sends information about himself to the SMTP proxy.
    4. The proxy accepts or rejects the client.
    5. The client sends information about the recipient to the SMTP proxy.
    6. The proxy look up the destination in DNS, and gets "no such name" back.
    7. The proxy sends information to the client that the address is wrong.

With a wildcard for mistyped domain, the following happens:

8. The client looks up the IP address of his outgoing SMTP proxy in DNS.
9. The client opens a TCP connection to his outgoing SMTP proxy.
10. The client sends information about himself to the SMTP proxy.
11. The proxy accepts or rejects the client.
12. The client sends information about the recipient to the SMTP proxy.
13. The proxy looks up the destination in DNS, and gets "success" back.
14. The proxy accepts the message and closes the connection to the client.
15. The proxy opens a TCP connection to the bounce server.
16. The proxy present himself to the bounce server.
17. The bounce server indicates that the recipient address is not acceptable.
18. The proxy generates an error message which is sent back to the sender's email address.

- A different scenario happens if the SMTP client has been misconfigured with the incorrect name of the outgoing SMTP proxy. As the domain name resolves using a wildcard, the client will connect to the bounce server, and start to send mail to it. The result is that the bounce server (at the IP address of the wildcard) says that the recipient address is wrong even though it is in fact correct. The error presented to the user is incorrect, as it is the name of the outgoing proxy which was wrong and not the name of the recipient.

Informing Users of Errors

Many application GUIs check domain names for validity before allowing the user to progress to the next step. Examples include email clients that directly check the domain of the email addresses resolves before sending, and network printer configuration tools that check that the print spooler name is valid before accepting the configuration. Previously the user would be prompted early that they had made an error in the domain name. In the case of email, the error may now not be noticed at the time of sending, but only when email later bounces. In the case of the printer configuration, the error may not be noticed during configuration, but only afterwards when printing fails to work, where the problem diagnosis is more difficult.

Spam Filters

Installing these wildcard records broke several simple spam filters commonly used to front end inbound mail servers, as well as more complex filtering that checks for the existence of a sending domain in order to screen out obviously bogus senders. This technique for spam has diminished as this filtering mechanism has increased, but one sample operator reports that it still equals about 10% of inbound mail attempts on their large shared MX cluster. ISPs who are aware of this problem will probably extend their filtering rules to have special knowledge of the address returned by these wildcard records, but will have to carry the cost of doing so, both in terms of code maintenance and increased execution time for their filtering.

Interactions with Other Protocols

The wildcard address records trap lookups for any network service, but the number of protocols somewhere in use on the Internet (including private protocols used between two or more parties on ports which they may or may not have registered with IANA) is large enough that it simply is not possible for the zone operator (or anyone) to provide a redirection service for every protocol. In this particular example, the zone operator only provided handlers for HTTP (which they directed to a search page) and SMTP (which they attempted to bounce). All other protocols received at best TCP resets, or, in some cases, simply had their packets dropped. Any application that uses the DNS has (or should have) some way of handling "no such name" errors; in almost all cases the error message is sufficiently clear to an experienced user that it is immediately obvious when the application has failed because it was given an incorrect DNS name. With these wildcard records in place, however, incorrect DNS names which are matched by the wildcard record will not show up as DNS name errors at all, but instead will show up as mysterious connection failures or as unreachable destinations for all services that the zone operator does not redirect. Depending on the details of the application protocol and implementation involved, this change may also convert an obvious "hard failure" (incorrect name) into a soft failure which the application thinks it should retry, as seen above in the email case. This may result in very long delays, perhaps of days or weeks, before even trivial errors are brought to the user's attention. Transport protocols using UDP may also retry until the transport protocol retry limit is reached (especially if ICMP messages are being filtered at a firewall), which may be very considerably longer than the time it would have taken to return an error to the user indicating they mistyped the destination.

Automated Tools

Automated or embedded tools which use HTTP but which do not have a user interface may also be confused by this change, since such tools may expect configuration failures to show up as DNS errors and may not realize that the HTTP response they have received from the zone operator's search page is not the page which the tool expected to reach. Such tools may fail in unpredictable ways, and may not be easy to upgrade.

Charging

The current response from the service in question is just over 17 KBytes of data because the client has to open a TCP connection and receive a not insignificant amount of data. A "no such data" response would have fitted in one packet. In the case of volume-based charging for Internet Access (as with most cellular data services) the recipient will have to pay additional charges.

Single Point of Failure

Even for cases in which the redirection service works as intended, such a service creates a very large single point of failure. Single points of failure are obvious targets both for deliberate attacks and for the sort of accidental "attacks" caused by bugs and configuration errors which already generate much of the traffic at the DNS name servers for the root zone. Furthermore, the IP address associated with this single point of failure is a likely target both for routing attacks intended to redirect the IP address to some other server.

Privacy

An interception service with this kind of scope raises significant privacy concerns, since traffic received by the interception service is, pretty much by definition, not going where its sender originally intended. The potential for abuse in this situation is very high, and makes the interception service an even more attractive target, this time for attackers who wish to gain control of it in order to practice such abuse.

Reserved Names

This sort of wildcard usage is incompatible with any use of DNS which relies on reserving names in a registry with the express intent of not adding them to the DNS zone itself. An example of such a use is the JET-derived IDN approach of "registry restrictions" and "reserved names", which depends on the existence of names that are reserved and can be registered only by the holder of some related name, but which do not appear in the DNS. By some readings of the current ICANN IDN policy, support for that "reserved name" approach is required. To accomplish the goal of reduced consumer confusion, the reserved names must not be resolvable at all. This reserved name approach appears to be completely incompatible with this sort of wildcard usage: since the wildcard will always cause a result to be returned, even for a reserved name which does not appear in the zone, one can support either one or the other, but not both.

Undesirable Workarounds

ISPs have responded to the deployment of these wildcards in a number of ways, all of which are both understandable and worrisome. Some ISPs have contemplated modifying their routing systems to drop all packets destined to the zone operator's redirection server into a black hole. Others have deployed patches to their DNS resolvers which attempt to reverse the effects of these wildcard records. Still other ISPs have considered using this as an opportunity to play the same game that the zone operator is playing, but for the ISP's own benefit. All of these responses are both understandable and predictable, but none of them are good. Even more worrisome is that different ISPs are taking different approaches to dealing with this, which may lead to a balkanization problem and create an ongoing headache for anyone having to deal with cross-network DNS or application debugging.

Principles, Conclusions, and Recommendations

The Robustness principle tells us that in some (not all) of the problems detailed above, both parties could be construed as being at fault. In some cases this is hardly surprising: spam filtering in particular, by its nature, tends to be extremely ad hoc and somewhat fragile. No doubt there are lessons here for all parties involved.

The Principle of Least Astonishment suggests that the deployment of wildcards was disastrous for the users. It had wide sweeping effects on other users of the Internet far beyond those enumerated by the zone operator, created several brand new problems, and caused other internet entities to make hasty, possibly mutually incompatible and possibly deleterious (to the internet as a whole) changes to their own operations in an attempt to react to the change.

Note that these considerations apply to any wildcard deployment of this type. The list of problems encountered in this case clearly demonstrates that, although wildcard records are part of the base DNS protocol, there are situations in which it simply is not safe to use them. As noted in an earlier section, two warning flags suggesting that this type of wildcard deployment is dangerous were that

1. it affected more than one protocol, and
2. it was done high enough up in the DNS hierarchy that its effects were not limited to the organization that chose to deploy these wildcard records.

Note also that a significant component of some of the listed problems was not precisely the wildcard-induced behavior per se so much as it was the abrupt change in the behavior of a long established infrastructure mechanism.

In conclusion, we would like to propose a guideline for when wildcard records should be considered too risky to deploy, and make a few recommendations on how to proceed from here.

Proposed guideline: *If you want to use wildcards in your zone and understand the risks, go ahead, but only do so with the informed consent of the entities that are delegated within your zone.*

Generally, we do not recommend the use of wildcards for record types that affect more than one application protocol. At the present time, the only record types that do not affect more than one application protocol are MX records.

For zones that do delegations, we do not recommend even wildcard MX records. If they are used, the owners of zones delegated from that zone must be made aware of that policy and must be given assistance to ensure appropriate behavior for MX names within the delegated zone. In other words, the parent zone operator must not reroute mail destined for the child zone without the child zone's permission.

We hesitate to recommend a flat prohibition against wildcards in "registry"-class zones, but strongly suggest that the burden of proof in such cases should be on the registry to demonstrate that their intended use of wildcards will not pose a threat to stable operation of the DNS or predictable behavior for applications and users.

We recommend that any and all TLDs which use wildcards in a manner inconsistent with this guideline remove such wildcards at the earliest opportunity.

Acknowledgements

The IAB gratefully acknowledges the kind assistance of David Schairer, John Curran, John Klensin, and Steve Bellovin for helpful suggestions and, in some cases, significant chunks of text. None of these contributors bear any responsibility for what the IAB has done with their contributions. We note that Leslie Daigle recused herself from the process of producing this document.

IAB Contact for this Document

The contact person for the IAB on this statement is Harald Alvestrand.

Appendix 7: Museum Domain Management Association, Statement Concerning Wildcard “A” Records in Top-Level Domains, 6 October 2003

http://musedoma.museum/policy/wildcard/; verified May 26, 2004

Museum Domain Management Association
Statement Concerning Wildcard A Records in Top-Level Domains

Summary

The Museum Domain Management Association (MuseDoma) is the non-profit organization responsible for formulating the policies for the .museum top-level domain (TLD). MuseDoma serves in this role under an October 2001 agreement with the Internet Corporation for Assigned Names and Numbers (ICANN) that delegates to MuseDoma the responsibility, within a broadly defined scope, for providing the forum in which the international museum community develops policies to be followed in this special-purpose TLD. Key among the topics within MuseDoma's responsibility is the establishment of "naming conventions" for .museum.

Since it was entered into the DNS nearly two years ago, the .museum TLD zone file has included a wildcard A record, implemented according to conditions in the ICANN-MuseDoma agreement. The immediate purpose of this was to familiarize users with .museum's highly structured three-level namespace and enhance its utility via an ordered index of all names in the TLD. This index is operated on a non-profit basis by MuseDoma and has been continually enhanced to make the namespace more accessible to users. A test-bed precursor of the index was implemented during MuseDoma's consultative policy-development process and was received enthusiastically from the outset by the museum community, which actively supported the further development of the index.

In mid-September 2003, wildcard A records were entered into the .com and .net zone files. This prompted many expressions of concern about the effects that these changes might have on the security and stability of the Internet's operation, as well as the necessity of modification to a variety of systems to accommodate the .com and .net wildcard characteristics. In the ensuing discussions, some have spoken in undifferentiated terms about the use of wildcards in any TLD. The purpose of the present statement is to call attention to key differences in the purposes that the wildcards serve, their benefits and drawbacks, and the processes by which they are introduced.

The .museum wildcard was developed through a consultative process that generated strong support within the museum community. The provisions of the ICANN-MuseDoma agreement on which it is based were posted for public commentary six weeks before the Agreement was entered, with no Internet community comment on the point. The TLD policies that include the wildcard are fully disclosed to every prospective .museum name holder, each of which also agrees to adhere to those policies as part of the registration process.

A sponsored TLD, by definition, is operated for the benefit of a clearly bounded community according to community decisions made through the Sponsor. The museum community determined at the beginning to employ a highly structured three-level namespace, which is made more accessible to users by the .museum index and its associated wildcard. Similar conditions are not relevant to the operation of unrestricted, unsponsored TLDs.

There are also differences of scale and timing. The .museum TLD is small and has had the wildcard since its inception. Approximately 3,000 museum names are currently registered, with a maximum anticipated population one order of magnitude larger (which will be about 1,000th the size of .com). The potential for disruption to applications written in reliance on the lack of wildcards is clearly smaller than in any case where wildcards are introduced into a significantly larger TLD, especially where that introduction occurs after a protracted period of operation without wildcards. Finally, different considerations pertain when the purpose served by a wildcard is restricted to the shared internal objectives of a non-profit community, than is the case when revenue generation is a primary motivating force.

Although the .museum wildcard has broad support in the museum community and there have been no reported technical problems resulting from its use during the nearly two years of its operation, MuseDoma recognizes its responsibility for developing .museum policies in a manner that avoids technically disruptive effect on the Internet. In this regard, MuseDoma values ICANN's investigation of the technical concerns, including those raised by the Internet Architecture Board and the ICANN Security and Stability Advisory Committee. That investigation will undoubtedly provide valuable input to the museum community's assessment of the present benefits and drawbacks of the .museum wildcard, and its development of policies regarding the future of that wildcard.

Process used in establishing the .museum wildcard

During consultations leading up to the launch of the .museum TLD, the museum community displayed keen interest in the establishment of a TLD-wide directory service, operated on a non-profit basis, that would assist users in becoming familiar with and navigating this small TLD's structured namespace. The rationale for this structure was to provide means for labeling resources on the basis of disciplinary focus or physical location. The application of descriptive nomenclatural hierarchies is fundamental to the museum profession and that community's sentiment strongly supported creation of a similar mechanism to order the .museum TLD namespace.

To promote user familiarity with the intricate and unfamiliar structure of this namespace, under MuseDoma's auspices the museum community began the development of a public index of the namespace. To ensure that users benefited from this resource, the community sought a mechanism to direct users requesting unassigned .museum domains to the index. This seemed to present minimal potential for upsetting user expectations, since any deliberate use of the character string ".museum" indicates an attempt at locating a resource provided by a .museum name holder and direction to the .museum index would therefore invariably be consistent with user interests. (The likelihood of a typing error accidentally resulting in the entry of a URL ending with ".museum" is not taken as a serious concern.)

The .museum index was initially conceived as a convenient way for prospective name holders to see the second-level labels already being used in the generic vocabulary. The availability of the index avoided the coincidental appearance of generic terms only slightly differentiated from each other, and fostered convergence on a consensus-based shared descriptive vocabulary. The index at its current state of evolution is located at http://index.museum/.

In addition to its utility as a support device in the formation of names, the index assists the user community in locating resources in .museum. A user with a general interest in museums with a given area of specialization or at a particular location is well served by the availability of listings, for example, of all participating art museums or all museums in a specified city. The index provides a single point of entry into this descriptive hierarchy and enables the direct addressing of, for example, http://art.museum/. The primary current purpose of the wildcard is to enhance the utility of the controlled .museum namespace by supporting community expectations of being able to access the .museum index directly on its second level. When used as a URL, a two-label domain name matching an entry in the index leads immediately to the desired access point; any other two-label name takes the user to the top of the index hierarchy.

Based on the support in the museum community, experts in the Internet technical community were consulted and concrete guidance was provided about essential technical requirements. MuseDoma then requested that its agreement with ICANN authorize inclusion of a wildcard in the .museum zone for the limited purpose of enhancing the effectiveness of the index as a finding aid. In accord with the clear opinion of the community for which the .museum TLD was being created, such a provision was included the ICANN-MuseDoma agreement, specifying the inclusion of the wildcard in a clearly defined and narrowly focused configuration. The wildcard has been included in the .museum zone since the TLD was established, with MuseDoma ensuring that the providers of technical registry services for .museum maintain the required configuration.

The proposed provision of the ICANN-MuseDoma agreement was posted for general Internet community comment at the end of August 2001. No remarks about any potential jeopardy to the stability of the Internet were submitted to the ICANN forum for public commentary, and the provision was included as posted. The wildcard facility has been demonstrated in every one of the numerous presentations of .museum that have since been made to the museum community, which continues to regard its availability as one of the more useful and compelling features of their structured namespace. All prospective .museum domain-name holders indicate their acceptance of the .museum usage policies and naming conventions prior to registering their names. The user community has long since demonstrated expectation of being able to avail itself of the benefits of the index and the wildcard feature.

Recent controversy concerning .com and .net TLD wildcards

On 15 September 2003, wildcard A records were introduced in the zone files for.com and .net. This triggered debate about numerous aspects of that action with particular concern being expressed about the disruption of applications that have relied on the former configuration of the .com and .net zones. The Internet Architecture Board (IAB) has published a commentary describing several technical issues caused by the changed configuration, and stating the guideline: "If you want to use wildcards in your zone and understand the risks, go ahead, but only do so with the informed consent of the entities that are delegated within your zone."

The ICANN Security and Stability Advisory Committee (SECSAC) also published a paper concerning the introduction of .com and .net wildcards, noting that the change "has caused an escalating chain reaction of measures and countermeasures that contribute to further instability." SECSAC has launched a review of the technical implications of the changes to the operation of the .com and .net TLDs, and has scheduled a meeting on 7 October 2003 to gather input regarding them.

The present statement is presented as a support document for the SECSAC review. MuseDoma believes that the circumstances of .museum highlight the need for differentiating between TLDs when assessing the effect of including wildcards in them. The manner in which the .museum wildcard was introduced and has subsequently been operated are fully consistent with the IAB guideline (quoted above). The consequences of the "measures and countermeasures" noted by SECSAC are of particular relevance to the effective operation of the .museum wildcard and MuseDoma wishes to indicate its interest in assisting in the examination of these secondary effects.

Key differences between the .museum wildcard and those in .com and .net

Although some have drawn parallels between the .museum wildcard with those in .com and .net, in fact the two situations are very different. Expanding on the points indicated above:

(a) The .museum wildcard was developed in extensive consultation with the museum community, through an organization to which explicit responsibility for that process had been delegated;

(b) There was full public notice of the implementation of the wildcard both prior to its authorization in the .museum Sponsorship Agreement between ICANN and MuseDoma, and as a component of the .museum operational policies to which each prospective registrant agrees during the application process;

(c) The prior notice of the wildcard made to, and consented by, all registrants fully complies with the IAB guideline;

(d) The .museum wildcard meets a special need of that TLD that is directly related to the detailed structure of its naming conventions;

(e) The .museum index facility supported by the wildcard is operated as a public service, without expectation of it generating additional revenue;

(f) There is no accumulation of TLD-specific applications relying on an established practice of no wildcards;

(g) The .museum TLD is four orders of magnitude smaller than .com and any comparison of the disruptive potential for wildcard implementation in them must be similarly weighted;

(h) During the almost two years in which a wildcard A record has been resolving in the .museum zone file, there have been no complaints about its having any undesired secondary effects.

The conditions underlying the .museum wildcard lack counterpart in any domain that is not restricted to a clearly bounded community. Any discussion of extensibility of the .museum wildcard application must take this into account. Although reasonable precedent might be seen for similar implementations in other bounded domains operated by agencies originating and residing within the community encompassed by that domain, any discussion of grounds for the inclusion of a wildcard in an unrestricted gTLD needs to be conducted from its own first principles.

Future of the .museum wildcard

In its deliberations since 2001, the museum community has enthusiastically endorsed the use of the .museum wildcard to enhance the accessibility of a public index of the TLD namespace. The benefits of the index were viewed as significantly overriding any drawbacks that might result from the use of a wildcard to direct attention to the index. The wildcard implementation strictly adheres to the clearly defined and narrowly focused configuration developed in consultation with technical experts. MuseDoma has ensured further adherence to this through its supervision of the provider of .museum registry services, CORE.

Despite its broad support of the .museum wildcard, the museum community recognizes its responsibility for developing .museum policies in a manner that avoids technically disruptive effect on other parts of the Internet. The use of the .museum wildcard is most effective as a user-familiarization tool in the TLD's initial stages and, as the .museum TLD grows in acceptance, it is appropriate periodically to review the use of the wildcard. MuseDoma expects the ongoing investigation by the ICANN Security and Stability Advisory Committee of the technical concerns raised by wildcards to illuminate the museum community's assessment of the present benefits and drawbacks of the .museum wildcard, and its development of policies regarding the future of that wildcard. MuseDoma looks forward to the insights this process will provide and to continuing to work with ICANN in ensuring that the Internet's infrastructure continues to be operated stably, securely, and in the interest of the global community.

6 October 2003 - 1500 UTC