Sandia National Laboratories

Operated for the U.S. Department of Energy by
Sandia Corporation

Dr. Leonard M. Napolitano, Jr.
Director, Center for Computer Sciences & Information Technologies

P.O. Box 969, MS 9151
Livermore, CA 94551-0969

Phone: (925) 294-3218
Fax: (925) 294-6600
Internet: lmnap@sandia.gov

November 16, 2011

The Honorable Zoe Lofgren
Member of Congress
401 Longworth House Office Building
Washington, D.C. 20515

Dear Representative Lofgren:

Thank you for your letter requesting the expertise of Sandia National Laboratories to provide a technical assessment of the Domain Name Service filtering provisions in H.R. 3261 and S. 968.

My staff and I have reviewed H.R. 3261 and S. 968 and believe the Domain Name Service (DNS) filtering/redirection mandates in the bills 1) are unlikely to be effective, 2) would negatively impact U.S. and global cybersecurity and Internet functionality, and 3) would delay the full adoption of DNSSEC and its security improvements over DNS. One staff member characterized the proposed DNS filtering mandate as a "whack-a-mole" approach that would only encourage users and offending websites to resort to low cost workarounds.

A recent report entitled "Security and Other Technical Concerns Raised by the DNS Filtering Requirements in the PROTECT IP Bill" by Steve Crocket et al. raises some of the concerns you mention in your letter.[i] We agree with the conclusions of that report, with the exception of the following statement: "Quite simply, a DNSSEC-enabled browser or other application cannot accept an unsigned response; doing so would defeat the purpose of secure DNS." In practice, DNSSEC-enabled applications have to be able to accept unsigned responses because the vast majority of domains are still unsigned. This transition period of coexistence of signed and unsigned domains will likely persist for some time, but we agree that the security of Internet users will improve the faster DNSSEC is adopted.

Background

DNS is a lookup service for translating a website name (e.g., www.house.gov) to an Internet Protocol (IP) address (e.g., 143.228.181.132), a *resource* utilized by applications to connect to other Internet hosts (e.g. a Web browser to a Web server). The DNS does not *itself* provide services for such applications--only the lookup service. Thus, any name-based transaction to the Internet involves first a DNS lookup, followed by a connection made by the application to the IP address returned.

DNS filtering at its simplest returns an error status, simply disallowing the application from trying to connect to the resource. However, DNS *redirection* is required to give the user a message indicating the problem (e.g., the "Text of Notice" referenced in H.R. 3261 and S. 968). Two steps are necessary to enable DNS redirection: 1) a DNS resolver must return a response substituting the legitimate IP of the filtered domain with the IP of a server that has been explicitly set up to return the message to the user; and 2) the application must subsequently connect to the service on the falsified IP and receive the response.

Q: Would DNS filtering be effective in blocking U.S. access to targeted foreign websites?

It is not likely DNS filtering would be effective in blocking U.S. access to targeted foreign websites. There are several challenges with DNS filtering and a determined user can circumvent filtering with minimal effort. Even non-technical users could learn to bypass filtering provisions by learning through forums, social networking, or (as Crocker et al. suggest)[i] downloadable plugins.

The DNS filtering specified by H.R. 3261 requires DNS redirection, as described above. A number of service providers currently perform DNS-based Web redirection, but only for DNS names that would otherwise return negative DNS responses (i.e., the names don't exist), so the user arrives at a synthesized page with sponsored ads related to the non-existent name or something similar. Ultimately, the user can correct his or her mistake and navigate to the correct page.

The result of DNS filtering with a name that exists is more challenging for several reasons. First, HTTP (the protocol used by Web browsers) isn't the only protocol used by applications for accessing content on the Internet. Other common examples are BitTorrent, FTP, rsync, and HTTP over SSL (HTTPS)--which presents additional challenges due to its secure nature. Thus, compliance with H.R. 3261's "Text of Notice" would require that the Internet host corresponding to the redirected IP address returned by the DNS resolver understand and respond to all such protocols. Also, clients for other protocols do not have provisions for displaying text as does a Web browser using HTTP.

In the case of Web requests, the user can get around the filter using a variety of tactics. These include, but are not limited to: 1) using a different DNS resolver, including a foreign DNS server, which is not under the same laws or obligations as a filtering DNS resolver located in the United States; 2) bypassing the DNS for the filtered domain name by going to the IP address directly in the address bar; or 3) using an application "proxy" (e.g., an HTTP proxy) operated by a third party that both uses its own DNS resolver and proxies the request to the remote server.

Q: What, if any, are the technical risks of imposing a DNS filtering requirement in the United States, to cybersecurity and to the functionality of the Internet?

The biggest risks to cybersecurity are to users who circumvent the DNS filtering by using foreign DNS servers or HTTP proxies, which could allow untrusted foreign servers to handle critical DNS lookups and Internet traffic. Using untrusted servers puts the user in dangerous circumstances by routing their sensitive DNS lookups and other Internet traffic through devices potentially controlled by criminals.

There are also potential consequences to DNS filtering that might adversely affect proper functionality of the Internet. In particular, it is possible that the resolution of some domain names could be negatively affected by the filtering of other domain names under the provisions of these bills. Domain

names often rely on other names to be resolved, and the failure of these dependencies can cause partial or complete failure of the dependent names. The most common examples of this are: authoritative DNS servers hosting DNS data for third-party domains (e.g., example.net servers hosting example.com data); third-party mail servers receiving mail for DNS domains (e.g., mail.example.com receiving mail for the example.net domain); and aliases for domain names in third-party namespace (e.g., www.example.com aliasing www.example.net). If non-filtered names are dependent on filtered names, then legitimate resources might become unavailable. It's difficult to determine in advance of implementing filtering how widespread such effects would be.

Q: Would the authentication technology known as DNSSEC be disrupted by a DNS filtering mandate? If so, what would the practical consequences be for U.S. cybersecurity?

A DNS filtering mandate likely will slow DNSSEC adoption overseas, and use of DNSSEC will make it more difficult for ISPs to comply with the filtering mandate in the bills. The consequences to U.S. cybersecurity from discouraging widespread adoption of DNSSEC will be negative, since DNSSEC fixes fundamental security flaws in the DNS protocol.

At this point in time, there are relatively few signed domains, and many of those are inconsequential. Likewise, there are relatively few validating resolvers. However, we expect an increase in both signed domains and validation, which would prevent discreet tampering of DNS responses, as required by the present versions of the bills. But in a world of validating resolvers, signing a filtered domain disallows DNS redirection as mandated by the bills.

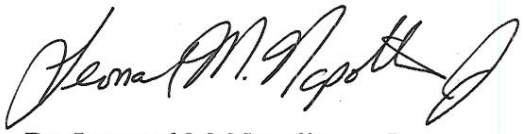
The answer also depends in part on where DNSSEC validation happens. At the moment, DNSSEC validation is typically performed at the DNS resolver. For most users, this is the DNS resolver provided by their Internet Service Provider (ISP). Since the user relies on the ISP's resolver to authenticate DNS responses, the resolver could technically manipulate the response however it would like--even that of signed domains--and the user would not know the response had been manipulated.

However, the long-term goal is to enable DNSSEC validation in every client application (e.g., Web browsers), rather than having that application trust the DNS resolver, or even the host on which it is running. Because DNS requests are issued for nearly every network communication, performance is crucial, and DNS caching is used to minimize DNS lookup times. We anticipate that this caching will continue to be done at the DNS resolver run by the ISP. In this case, manipulation at the ISP's resolver, which is subsequently passed on to a validating resolver in the application, breaks the chain of trust and thus disallows DNS redirection.

Requiring or encouraging the disablement of DNSSEC validation (e.g., to support DNS redirection) would be detrimental to the security and safety of Internet users, as would any measure that hinders the adoption of DNSSEC. The reasons for this are enumerated ably by Crocker et al. [i] but boil down to this: DNSSEC aims to ensure that information associated with domain names comes only from the owners of the domain names. Ability to trust the legitimacy of this associated information (such as IP addresses) would remove a major source of vulnerability and uncertainty from the Internet, and enable applications (such as online banking and e-commerce) to avoid costly workarounds to the present insecure DNS.

I am grateful for your attention to this matter and appreciate the opportunity to address some of your technical concerns. If you have any further questions or would like to discuss this issue further, please do not hesitate to contact me.

Sincerely,



Dr. Leonard M. Napolitano, Jr.
Director, Computer Sciences and Information Systems

---

[i] Crocker, S., Dagon, D., Kaminsky, D., McPherson, D., & Vixie, P. (n.d.). Security and Other Technical Concerns Raised by the DNS Filtering Requirements in the PROTECT IP Bill. Retrieved November 15, 2011, from http://www.circleid.com/pdf/PROTECT-IP-Technical-Whitepaper-Final.pdf