Analysis of SOPA's impact on DNS and DNSSEC

DNS Overview

We would like to reiterate some facts about how the Internet, and in particular, DNS, works. There is no centralized control or authority for the Internet. The designs of most protocols have been by international consensus, and are implemented by the vendors and parties that connect to the network. Many of those protocols have been designed to be fault-tolerant[1]. Various faults, misconfigurations, and attacks thus result in only localized failures, with the majority of systems reconfiguring to ignore the problems. Unfortunately, not all of those base protocols have been designed with security in mind, so there are ways to exploit them to degrade service, and attack connected systems and users.

Connections to the Internet are defined by **Internet Protocol addresses** (IP addresses). An IP address is either a 32-bit or 128-bit number (for IPv4 or IPv6, respectively, which are two generations of Internet protocols) that is unique within the scope of the visible network. Packets destined for a site on the Internet are routed based on these numbers. The addresses may change without notice as machines are moved, rebooted, shut down, or shared. That dynamism, coupled with the difficultly for people to remember specific numeric addresses, means that people generally do not use the raw IP addresses in their normal day-to-day behavior. A single computer may have more than one IP address, similar to the way that a home may have more than one telephone number.

The **Domain Name System (DNS)** is a protocol through which computers connect domain names with corresponding Internet Protocol (IP) addresses. A single DNS name may resolve to multiple IP addresses (e.g., Representatives have multiple offices in their home district but they all operate under the Representative's name), and a single IP address may have multiple DNS names (e.g. all mail addressed to any House member goes to the same postal facility): these are common techniques for load balancing and fault recovery, among other reasons.

The entire DNS system is truly *global* in nature, with no single controlling node. It is in active use on all seven continents. The protocol has been designed such that there may even be alternative, competing DNS systems, although this has not yet happened.

---

[1] "Fault-tolerant" in this context means that an error or attack can occur and the overall system will continue to operate in alternative manners to achieve its objectives; imagine how battery-backed lights automatically take over in a power failure as an example of fault-tolerance.

The Role of Resolvers

Most Internet users deal with DNS *resolvers* rather than domain name servers. These are intermediate hosts that provide cached results, for efficiency (e.g., writing oft-used phone numbers on a pad near the phone is "caching" them, but when the pad is full, it is cleared). In short, when a user's system is presented with a domain name, such as www.house.gov, a query is sent to resolvers, usually at the ISP or central server, to map that name to one or more IP addresses (similar to how a name may be used to find a corresponding phone number in a phone book). If one DNS resolver cannot find an IP address for a domain by consulting its local cache, it can query other servers or resolvers to determine the proper IP address. This continues until either a timeout occurs, or a definitive DNS server returns a message that no such domain name exists. This whole process is more complex than simply looking for a match in a database as there are multiple levels of indirection, caching, and forms of response. This also does not address obtaining the domain name: names may be returned by search engines, included in email or programs, or even present in print media and on billboards.

DNS Contamination

The nature of the DNS system is such that it allows end-users to access systems without knowing any current numeric IP addresses. Systems may change IP addresses for many reasons, so having this system is fundamental to current Internet operation. It has been refined over many years and currently works almost invisibly.

The system may be abused, however, by criminals or totalitarian regimes (e.g, Syria, North Korea) to insert DNS resolution information into particular servers, such as the "resolvers" associated with a particular ISP. Any DNS lookups consulting this altered information may result in mappings to IP addresses for "false-flag" sites that may resemble the real sites, but are instead instrumented to capture personal information or feed false results. In other cases, the mappings simply fail, as if the desired site does not exist. (To continue the telephone analogy for both of these possibilities, the real phone book has been replaced with one with falsified phone numbers that are answered by impostors, or with entries omitted.) Examples include recent instances where Iran set up servers with altered addresses to capture the email and addresses of dissidents, and Chinese servers that block connectivity with the U.S. version of Google servers. These are a form of DNS Contamination. To address this DNS contamination problem, which presents significant criminal, espionage and human rights threats, the **Domain Name System Security Extensions (DNSSEC)** were designed.

DNSSEC Basics

DNSSEC includes chained cryptographically-signed responses[2], which enable the recipient to verify that the response is valid. The owner of a *zone* (one or more domains, or a partial domain) is able to provide a cryptographic signature on the response to any domain query to prove it is valid. There are also chained signatures from higher-level authorities to prove that the owner of the domain is legitimate, and that its signature should be believed. This signing process provides additional assurances that resolved domain names are properly represented, and that any "not found" error represents a real miss rather than someone simply trying to hide the valid response.[3]

Thus, only the owner of a domain can cryptographically sign responses resolving a hostname, or sign a response that a given name is not defined. An entity without the cryptographic key (a non-owner) cannot provide either of these valid responses. A client, seeking to resolve a name, should contact different servers until it receives a signed mapping or signed "not found" error, and should treat any other response as either a temporary failure or an attempted attack.

DNSSEC is important to securing the Internet, and reflects the efforts of scores of people over more than 15 years to develop and refine the protocols and assist in their implementation. It is being rolled out worldwide, and is a "best practice" for Internet security and safety. Elements of the U.S. government are currently using DNSSEC, or are committed to switching to DNSSEC in the near future, including the Department of Defense.

RPZ

The RPZ (Response Policy Zones) protocol has been identified by some as a mechanism for blocking classical DNS traffic that is already compatible within portions of the DNS system. This is correct for DNS, but incorrect for DNSSEC.

RPZ works by providing a "blacklist" of domains within a resolver. Attempts to resolve hostnames within one of those domains (such as one connected with the Russian

---

[2] A cryptographic signature uses encryption to generate a unique value based on some data to be signed and a secret key. Someone else with a corresponding public key can check that the unique value presented — and the underlying value from which it was defined — are authentic and unaltered. Anyone else trying to provide false information or alter the data does not have the secret key, and therefore cannot generate a signature that will stand up to scrutiny. This technique is used in everything from distributing software patches to validating on-line stock purchases

[3] A criminal might try to elide the DNSSEC response for a particular merchant, and thus cause the customers to use unsecured, plain DNS entries delivered by a compromised site. Thus, it is important to know when a valid mapping exists but is not being returned.

Business Network, a well-known criminal enterprise) would receive negative results. This is consistent with the "not found" behavior in regular DNS. However, in the case of DNSSEC, unless the RPZ server is able to provide a verified cryptographically-signed response, by standard the client host will not accept the response as valid and should continue to search for a properly signed result. This would be the case with a domain blocked using RPZ. The DNSSEC protocol should eventually result in a query to a nameserver outside the U.S. that will return a valid signed result. Thus, RPZ is not a solution under DNSSEC.

It has been suggested that the "Refused" reply provided by some DNS servers could be used for purposes of blocking. This fails to differentiate between hop-by-hop and end-to-end behavior, and operation of DNS and DNSSEC. The "Refused" reply is from a nearby resolver, and not the zone owner of a domain. Under DNSSEC, the "Refused" answer is not cryptographically signed and is thus treated as non-authoritative or as an attempt at an attack, and is ignored. Under DNS, a host may choose to seek another resolver upon receiving a "Refused" result. In either case, the "Refused" is simply a local negative response and not a conclusive one.

Opposing View

The Committee has received an analysis[4,5] stating that many of these technical concerns, as stated by others, are unfounded. We, respectfully, disagree with that analysis and here present technical reasons why SOPA and PIPA's approaches are flawed. In particular:

> **Circumvention of DNS blocking is technically simple and universally available.** Whether connection to alternate and backup DNS (and DNSSEC) servers would be legal under SOPA is not a technical issue. However, it is effectively impossible to bar access to alternate DNS servers around the globe because all Internet connected devices have the capability to refer to them, and there are millions of them on the Internet. Use of those servers allows for bypassing DNS blocking. Furthermore, a standards-compliant DNSSEC implementation should automatically circumvent the blocking using these alternate mechanisms.
>
> **Circumvention efforts against contemplated court-ordered blocks already exist.** Browser add-ons to counteract SOPA have already been developed, and other programs have been developed to bypass potential court ordered blocks. More are in development. These will be made available from outside the U.S.,

---

[4] http://www.hightechforum.org/my-dns-filtering-research-before-house-sopa-panel/

[5] http://thehill.com/blogs/congress-blog/technology/201755-refusing-to-answer-to-policy-reasons

beyond the jurisdiction of this legislation, but easily available to U.S. users. Additionally, existing software, developed in the U.S. and elsewhere to allow political activists simplified, unrestricted access to the Internet from within totalitarian countries can be (and will be) used inside the U.S. to circumvent DNS blocking.

DNS Blocking will necessarily interfere with legitimate Internet traffic. While targeted sites may represent a small percentage of total websites on the Internet, blocking orders will affect more than those targeted sites, and may impact users of domains who are committing no infringing behavior. DNS resolvers do not act in isolation, and DNSSEC involves communication with several computers when checking the legitimacy of website certificates. Furthermore, multiple users, multihoming, redirection, load-balancing, and other common hosting operations will make it difficult or impossible to appropriately limit the scope of blocking.

"DNS Fracturing" does not require a replacement of the official DNS service. Private DNS services that might spring up, separate from the mainstream DNS system (especially those outside the United States), may decide to sell their service as being free from U.S. government interference. Users switching to these services would "fracture" the DNS. The provisions in the manager's amendment will allow ISPs to take divergent paths to comply with SOPA, thus enhancing the chance of fracture. Also, DNS can be avoided entirely by workarounds that patch in domain names or that simply use the IP addresses. These are all methods that may work in parallel with the real DNS service. The assumption that working around the 'official' DNS service requires replacing it is incorrect.

Summary of Concerns

The basic concern prompting SOPA (and PIPA) is that malicious operators outside the United States are setting up Internet sites that serve material that is in violation of copyright and trademark laws of the United States. As they are beyond the immediate reach of U.S. law, there is concern about how best to stop their continued violation of the law. This is a valid concern. The solution embodied in the proposed legislation is intended to impede U.S. entities from finding, connecting to, and conducting transactions with those sites. The proposed solution is to purposely interfere with the DNS mapping of those sites, prevent them from being found in search engines, and to disable financial transactions via U.S. services. This proposed solution will not work, and any attempt to make it work will result in a significant degradation of Internet security.

The following are specific issues we have identified with the legislation in the SOPA:

- DNSSEC is designed to go around non-responses or unsigned "not valid" errors. A website whose DNSSEC information is blocked under a legal order would present a result not having an appropriate signed certificate. DNSSEC should treat such a response as it would any fraudulent website for which no or an invalid certificate is returned. It will check other DNS servers and chained responses to confirm the DNSSEC credentials of a website, without regard to the physical location of the server. DNS servers outside the United States would not be subject to the proposed legislation or blocking orders, and if contacted, would return the correct information. This behavior is an example of how the protocols and network are designed to work around failure and damage. It also illustrates why the fundamental design of the protocol will prevent some anticipated blocking from working.

- DNSSEC conflicts with anti-circumvention provisions of the bill. DNS and DNSSEC are designed to circumvent servers that present questionable results. This appears to conflict with Section 102(c)(3), which allows the Attorney General to seek injunctive relief against parties that provide products or services that circumvent blocking. Thus, a sensitive site running DNSSEC might be viewed as contravening the bill, even though it is adhering to best practices for security.

- Interfering with DNS routing or DNSSEC may harm legitimate national interests. Law enforcement and national security investigations often use DNS monitoring to combat crime and defuse potential security risks. In the case of the *Ghost Click Network* (a recent criminal case)[6], a more widely deployed DNSSEC would have blunted the impact of this botnet and the $14 million stolen through it by manipulating DNS. Ongoing industrial espionage from other nations may be enhanced if DNSSEC is not allowed to operate normally.

- Several parties — including many outside the U.S. — have already built software add-ons for browsers and end-system hosts to bypass U.S. DNS servers to seek DNS and DNSSEC resolution of names outside the U.S., and to perform searches in non-U.S. search engines. Given the global nature of the Internet, this will allow anyone using these features full access to sites that are blocked inside the U.S. More of these workarounds are being developed and distributed by those worried about the impact of SOPA and PIPA.

- Anyone with the direct IP address of a site may connect to it without involving the DNS system at all. Given the ability of many criminal enterprises to register multiple systems and take advantage of dynamic routing protocols, eliminating or blocking DNS entries for these sites will have minimal impact.

---

[6] http://www.fbi.gov/news/stories/2011/november/malware_110911/malware_110911

- Sometimes, criminals will hijack portions of a legitimate domain, or add criminal content to an existing, legitimate site to increase the trust victims may have in the legitimacy of the site (imagine a con man selling items inside a shopping mall rather than at the side of the road). Given the current state of security on the Internet, this approach is not difficult for those with moderate skills. Blocking the DNS entries for these sites and/or their domains will inconvenience legitimate businesses and agencies (e.g., preventing access to that mall for everyone because a pickpocket was reported to be present).

- Registering and activating a new domain name takes only a matter of minutes. Criminals intent on keeping a site active will be able to activate new DNS names and entries far faster than court orders and blocking can occur.

- Criminalizing the development and use of circumvention technologies will criminalize efforts to provide anti-censorship tools and connections for political dissidents in China, Iran, Myanmar, Cuba, and other countries where free speech is restricted. Tools developed in the U.S., and resolver/anonymizer sites in the U.S. are actively developed for the oppressed in other countries. However, there is no way to differentiate the use of those tools from those that might circumvent SOPA blocking.

- Some new protocols intended for enhanced security and to cut cybercrime use the DNS system as a base. Interfering with the DNS system may impair the adoption and use of those protocols. One example is the DANE protocol (DNS-based Authentication of Named Entities) designed to authenticate websites to prevent fraud by misrepresentation — ironically, one of the problems SOPA is intended to address. (C.f. http://www.fbi.gov/news/stories/2011/november/malware_110911/malware_110911)

For these reasons, we do not believe that attempts to block or alter DNS or DNSSEC look-ups will be particularly effective in stopping individuals who wish to connect to criminal sites outside the U.S., and will be less effective over time for all users. However, the costs and overhead associated with maintaining blocks and responding to orders will remain.

In conclusion, we offer two specific suggestions related to the current legislation, should some form of it move forward.

- The costs of complying with blocks in search engines and DNS lookups could be substantial, especially for smaller ISPs and companies that will need extra technical expertise to accommodate them. These are innocent third parties that will effectively be taxed for the benefit of the owners of the intellectual property.

This not only raises questions of fairness, but of competitiveness, especially during a time of increased economic stress.

- We suggest that legislators include language that would require any entity seeking an order under this legislation to pay all reasonable expenses incurred by the parties forced to carry out that order. This would not only be fair to those innocent third parties, but would help reduce any incidence of overly broad actions against sites committing minor infractions.

- There is already legislation in place, in the form of international trade agreements and the DMCA (Digital Millennium Copyright Act, P.L. 105-304), that could be used to fight some of the violations. Allocating more resources to pursue these avenues more effectively might produce better, more targeted results.