Implications of Security Enhancements and Interventions for Core Internet Infrastructure

Sharon Goldberg
Computer Science Department
Boston University

Stephanie Forrest
Computer Science Department
University of New Mexico

First posted August 15, 2014. Last revised September 9, 2014.

Abstract

Security enhancements to the Internet are often implemented as hierarchical and centralizing structures grafted onto what is fundamentally a decentralized design. Hierarchical structures, such as DNSSEC and RPKI, provide a convenient way to enforce consistency and prevent important categories of security violations. They also provide a locus of control for trusted authorities who have access to the higher levels of the hierarchy. These control points can be used to enforce many kinds of policy interventions, including local laws and censorship.

This paper considers three security enhancements, DNSSEC, SSL PKI, and RPKI, which provide secure translation infrastructures through a hierarchical authentication system. It reviews the design of each system, describes the security vulnerabilities that they protect against and how attackers have responded, explains how centralized authorities have used them to exercise unilateral control, and discusses the tradeoffs and risks associated with these interventions. The paper then considers the policy implications of these interventions and proposes some guiding principles to mitigate negative consequences.

1 Introduction

Over the past three decades, the Internet has matured into a worldwide platform that is essential for modern life. As with most complex systems, a variety of self-interested actors have also emerged who seek advantage, whether for making money, committing crimes, or exerting political power. In response, a variety of technical and policy defenses have been devised, many of which involve manipulations of the Internet's core protocols and operations. These core infrastructures were originally designed by engineers to be reliable and efficient, serving as a kind of neutral substrate on which a wide variety of applications could be hosted. However, with the advent of technical security structures, such as DNSSEC, RPKI and SSL, and legal interventions, such as DNS takedowns, these core infrastructures are rapidly becoming a battleground for legal and political disputes. This working paper discusses three examples, the Domain Name System (DNS), interdomain routing, and the SSL PKI, first describing the systems themselves, which are quite complicated; second, reviewing the technical defenses that have been devised to protect them from exploitation (DNSSEC and RPKI); third, discussing how policy interventions (takedowns) interact with these systems; and finally, highlighting some of the unintended consequences arising from these developments. Taken together, these examples illustrate a security tradeoff between centralized hierarchical systems, which are easy to control but more vulnerable to misuse, and decentralized designs, which are more robust to abuse but harder to manage.

2 The Impact of Interventions on Internet Security

End-to-end encryption and authentication are both essential to the security of network traffic, but these techniques rely on the security of the systems that establish a secure communication channel in the first place, and this first step is a common point of attack [27,35,42,49,60,75,85–87,91, 92]. Three crucial security infrastructures for protecting the process of establishing communication channels are: The Domain Name System Security Extensions (DNSSEC) [20–22] for the Domain Name System (DNS); the Resource Public Key Infrastructure (RPKI) [55] for interdomain routing; and the Secure Socket Layer (SSL) public key infrastructure (PKI) [32,33,37]) for the Transmission Control Protocol (TCP). As shown in Table 1, each of these three systems provides a service that *translates* from one namespace to another—allowing a resource in one namespace (*e.g.,* a hostname like `www.bu.edu`) to be accessed by translating it to a value in another namespace (*e.g.,* an IP address like 128.197.27.7).

These namespaces are key supporting infrastructures for all Internet operations, enabling global communications by providing globally-resolvable identifiers for all online entities. The DNS provides a translation from domain names to IP addresses, and is secured by DNSSEC. The interdomain routing system translates destination IP addresses to routes, and then delivers packets along those routes; it is secured by the RPKI. Finally, the Secure Sockets Layer (SSL) allows end users could establish encrypted connections, e.g., for secure web transactions; the SSL public key infrastructure (PKI) facilitates this by securely translating from a hostname (`www.bu.edu`) to its cryptographic keys. Each of these translation services enable global interoperability, acting as the glue that binds separately administered networks into a single Internet, allowing users and programs around the world to communicate seamlessly. Correct translation is crucial and when it fails, whether by accident or intentionally, the consequences can include denial of service, redirection to an alternate location that serves malware, bogus information, or intercepts and surveillance.

Security system	Underlying system	Translation	Deployed?	Defends against...
SSL PKI [32, 33, 37]	SSL/TCP	hostname → public key	Widely used.	An adversary that binds its own cryptographic key to a victim's hostname in order to decrypt or alter the victim's SSL messages [42, 85, 86, 92].
DNSSEC [20–22]	DNS	hostname → IP address	Since 2006 [70]	An adversary that tampers with DNS responses to block/censor a host [19,38,39,89,90] or redirect users to an adversarial host [49, 87, 91].
RPKI [55]	BGP routing	IP prefix (*i.e.,* block of IP addresses) → Origin AS	Since 2011 [23, 83]	Prefix & subprefix hijacks, where a hijacker sends a routing announcement for the victim's IP prefix, causing traffic for the victim to flow to the hijacker's network [27, 35, 60, 75].

Table 1: Secure translation infrastructures: Security infrastructures (Col. 1) enforce correct translations for the underlying service (Col. 2). The particular translation provided by each service is shown in Col. 3. Col. 4 lists how widely each security system is deployed today, and Col. 5 summarizes the protections that each security system provides.

Each of the three secure translation infrastructures shown in Table 1 was designed to add protection to an insecure legacy protocol (*i.e.,* DNSSEC is layered on top of the DNS [20–22], SSL and its public key infrastructure (PKI) on top of TCP [32, 33, 37], and the RPKI on top of interdomain routing [55]). The original protocols were each designed with the assumption of trust, relying on translations received from other parties and assuming that the received translations would be correct. The newer security infrastructures, however, accept only information that is cryptographically authorized by *trusted centralized authorities*: certificate authorities (CAs) in SSL and the RPKI, and zone administrators in DNS and DNSSEC. Indeed, each security infrastructure shown in Table 1 is roughly built around the following hierarchical blueprint: an authority, or *root-of-trust* allocates portions of its input namespace to other authorities, which either (a) recursively allocate subsets of their namespaces to other authorities (*e.g.,* in the DNS, the authority responsible for `.edu` delegates the name `bu.edu` to Boston University), or (b) return the proper translation for the name being queried (*e.g.,* in the DNS, Boston University maps the name `www.bu.edu` to its Internet Protocol (IP) address 128.197.27.7). *Relying parties* located anywhere on the Internet can then use translations provided by the security infrastructure to locate online entities, thus enabling reliable communications that transcend national, commercial, or other geopolitical boundaries. The hierarchical structures of DNSSEC and RPKI have a number of attractive properties, including concise summaries of names, easy searching through the namespace, and clear delineation of authority and delegation of responsibility for different names.

The security systems listed in Table 1 were designed to prevent external attackers from introducing bogus translations into the system. The result in each case, however, is a design that concentrates power in the hands of a few *insiders*; namely, the trusted centralized authorities. Indeed, in each of the systems in Table 1, an insider, or small coalition, has the power to *unilaterally* revoke or modify any of the allocations or translations that it issued. Because relying parties worldwide depend on the secure translation infrastructure, revoking or modifying an allocation or translation has global impact. Thus, the question of when and how an authority should revoke or modify the information it certifies has broad policy implications. For example, if a DNS authority (*e.g.,* the operator of the `.com` domain) revokes or *takes down* a translation (*e.g.,* the translation from domain `rojadirecta.com` to its IP address 209.44.113.148), the impact is global; Internet users worldwide will not be able to access the website at the affected domain (`rojadirecta.com`). Each of the three example security systems thus highlights the tradeoff between decentralized trust models, where no one actor has total control but security guarantees are weaker, and centralized models, where control is centralized but trusted authorities can provide cryptographically secure authorizations. Although each of the security mechanisms arose from technical design considerations, they each have significant policy implications.

One policy issue arises from conflicting legal jurisdictions. As an example, modifications and revocations made by centralized authorities—in today's Internet, these are typically private entities governed by local laws of the nation in which they operate—can be used to control the distribution of objectionable content. DNS takedowns, *e.g.,* can block access to illegal gambling websites [78], to websites selling products [10] or showing content [59] that violate copyright, or to sites providing travel services to restricted countries [56]. DNS takedowns are also used to control country code top-level domains (TLDs); see, for example, Norway's policy for the `.no` TLD [8] and Italy's policy for `.it` [36]. This use of the DNS to enforce local laws can lead to conflicts between the legal jurisdiction in which the takedown is mandated and other legal frameworks where it may have impact. To illustrate this point, consider the `rojadirecta.com` example, which compiles links to live broadcasts of sports events such as the NBA, NFL, and MLB. In 2011, U.S. Immigration and Customs Enforcement (ICE) used the DNS to take down `Rojadirecta.com` and `Rojadirecta.org` for copyright violations, even though Spanish courts found that this Spanish company had not violated the law. The takedown of `rojadirecta.com` was authorized by a district court in New York because the `.com` domain, based in the U.S., is governed by U.S. laws, but it punished behavior that was legal in the country where the online entity (website) was based (i.e. the `rojadirecta.com` website, based in Spain). The conflict arose because the DNS authorities were physically located within U.S. jurisdiction, but the namespace they authorized was global and used by parties in other legal jurisdictions. The borderless nature of the Internet creates similar conflicts in other technical domains as well. For example, there is an increasing number of legal requirements imposed on Google, with countries requiring it to delete content as part of the "the right to be forgotten" [68]. In a similar vein, a Canadian judge recently decided that Canadian courts can ask Google to delete content not just from the `www.google.ca` homepage, but from *all* Google homepages [13].

A related policy issue concerns the deployment strategy, or adoption path, for the three security infrastructures. These systems are useful only to the extent that they are widely used, but adoption is voluntary, so they will only become widely deployed if most network operators believe that they provide some security benefits. The increasing frequency of court-ordered takedowns has led to debate among practitioners about deploying new security infrastructures with trusted centralized authorities [12, 18, 45, 53, 54, 65, 88]. Although the SSL PKI is used widely in the Internet today, DNSSEC and the RPKI are still in their infancy with ongoing international campaigns (supported by the U.S. [14, 58] and other governments [3]) to promote their adoption by network operators. These campaigns have been undermined by the concerns of network operators, who fear subordinating control of their network's traffic-forwarding decisions to judgements made by centralized authorities, some of which may operate in different legal jurisdictions. In addition to network operators, it is also important to convince Internet users that they can trust the relevant authorities, and there is evidence that this could be problematic. For example, recent projects built as a response to DNS takedowns suggest that users might be willing to migrate off [2] or circumvent [5] the DNS when they disagree with decisions made by DNS authorities. Thus, there is a risk that online entities and regular Internet users will lose trust in the system and its trusted authorities, stop using the DNS altogether, and in so doing, trade the enhanced security of DNSSEC for enhanced access and autonomy.

These considerations point to a tradeoff, or dilemma. On the one hand, it is crucial to maintain integrity and trust in core Internet translation systems and the security architectures layered on top of them; this will ensure that Internet communications can continue to transcend geopolitical borders, and it will prevent external attackers from subverting the establishment of communication channels. On the other hand, these security infrastructures empower centralized authorities, and with online cybercrime increasing everyday, they have become an important tool for enforcing local laws, censoring objectionable content, or achieving other political ends. Sections 3, 4, and 5 explore the particulars of this tradeoff for the systems listed in Table 1. For each systems, we review the technical details of the security infrastructure and highlight the security vulnerabilities that they protect against. Next, we explain why their centralized authorities can and have exercised unilateral control over the names they translate and finally discuss how Internet users and online entities have reacted to these issues. Then, in Section 6 we summarize some of the policy implications posed by this tradeoff and propose some guiding principles to inform policy discussions going forward.

3 DNS and DNSSEC

The DNS. The domain name system (DNS) is a hierarchical distributed database that provides a variety of translation services, the most important of which is the translation of domain names (*e.g.,* `rojadirecta.com`) to IP addresses (185.34.216.226). The highest level node, or root, is controlled through a complex set of agreements between the U.S. Department of Commerce, ICANN and Verisign [64]. The root delegates responsibility for managing DNS entries for each top-level domain (TLD). For example, the `.ca` TLD is operated by the Canadian Internet Registration Authority (CIRA), which then subdelegates `google.ca` to Google. Similarly, the `.edu` TLD, which is operated by EDUCAUSE, subdelegates `bu.edu` to Boston University and `unm.edu` to the University of New Mexico. Boston University then translates `www.bu.edu` to IP address 128.197.27.7, while the University of New Mexico translates `www.unm.edu` to IP address 129.24.168.32. The DNS enables global communication because the hierarchical structure provides a single point of entry to the DNS system at its root, from which domain names are *resolved* by recursively walking down through the tree until the complete entry is found. It also ensures that lookups are resolved consistently because a single organization (*e.g.,* EDUCAUSE) is responsible for delegating and/or translating a particular namespace (*e.g.,* all domains ending in `.edu`), regardless of the geopolitical or physical location of the user or system that requests the translation by querying the DNS. Thus, EDUCAUSE serves as the *centralized authority* for the namespace `.edu`.[1]

Attacks on DNS. Although the DNS consists of a hierarchy of authorities, each of which is responsible for its delegated namespace, the messages sent by these authorities, *e.g.,* to answer queries, are not cryptographically authenticated. As a result, the DNS is vulnerable to external attacks located either *on path* (*i.e.,* that can intercept traffic sent on the network path between the recursive resolver and a relevant server) or *off path* [26,49] (*i.e.,* located anywhere on the Internet). An external attacker who tampers with a DNS message to alter a translation can redirect a domain (`www.bu.edu`) to an IP address (6.6.6.6) controlled by the attacker; the attacker can then intercept user traffic that is redirected to the IP address (6.6.6.6) it controls. Alternatively, an external attacker could replace the legitimate translation with a DNS message that states that "no such domain exists" ('NXDOMAIN'), and the user will be effectively prevented from communicating

[1] This is a simplified explanation of the DNS hierarchy, which omits several complexities that have been introduced over time; for a more complete overview of the DNS hierarchy see *e.g.,* [82].

with the domain, because it lacks a translation to its IP address. Both of these techniques have been demonstrated on the production DNS and are often observed in the wild as mechanisms for performing network censorship [6, 93].

DNSSEC. DNSSEC (Domain Name System Security Extensions) was proposed to protect against these attacks, and deployment began in about 2006. DNSSEC is a secure extension of the DNS that provides each DNS authority with a cryptographic public key, which it uses to digitally sign its own messages, preventing forging or tampering. The key of a DNS authority is certified by (*i.e.,* digitally signed by the key of) its parent authority in the DNS hierarchy, with all TLD keys ultimately certified by the root's key. The cryptographic signatures on DNSSEC messages prevent an external attacker without access to the relevant private keys from modifying or injecting bogus messages to subvert domain-name-to-IP-address translations.

DNS takedowns. The hierarchical structure of the DNS facilitates interventions, even in the absence of DNSSEC. In a typical scenario a court order is obtained, which compels a DNS authority to remove/redirect a subdelegation/translation for an offending domain from its records. Such a DNS takedown either (1) blocks users from accessing the domain completely, or (2) redirects users to a server that displays a *blockpage* explaining that the website has been taken down.[2] State-sponsored modifications to the DNS are common enough that ICANN (part of the root-of-trust for DNS and DNSSEC) has published a step-by-step guide for officials wishing to use DNS/DNSSEC to seize and takedown websites [76, 77]. In 2012, the Stop Online Piracy Act (SOPA) was proposed in the U.S. to formalize DNS takedowns as a legal instrument for the purpose of preventing copyright violations; although the bill never passed, similar proposals continue to surface both in the U.S. and other countries But, as noted by Venkat Balasubramani in 2011,"the fight against SOPA may be a red herring in some ways, since IP plaintiffs are fashioning very similar remedies in court irrespective of the legislation" [24].

Takedowns are used to disrupt cybercriminal activity; for example, in June 2014, the FBI, the UK's National Crime Agency and other law enforcement agencies took down domains used to command and control the Gameover Zeus trojan (which intercepts banking transactions) and Cryptolocker (which encrypts a user's data and demands a ransom payment from victims that want to recover their encrypted data [16]). Governments have also used DNS takedowns in more complex and ambiguous situations:

- **3322.org takedown.** In 2012, Microsoft initiated a takedown of `3322.org` to disrupt the Nitol botnet [9]. `3322.org` is a Chinese hosting provider that, in addition to hosting cybercriminals, also provides legitimate services to legitimate sites. Although `3322.org` is a Chinese site, Microsoft took advantage of the fact that the `.org` TLD is operated by an American organization to obtain a U.S. court order to take down the domain. This incident raises some interesting issues. First, it caused collateral damage by preventing legitimate users from accessing `3322.org`. Indeed, collateral damage to legitimate users by DNS takedowns is now so frequent that ICANN, the organization involved in managing and operating the root of the DNS, provides guidance on collateral damage for governments seeking to take down domains [77]. Second, the efficacy of this takedown is questionable; the Nitol botnet simply switched to other domains after `3322.org` was taken down [69]. Finally, this example raises

[2] See `http://www.nflfavourite.com/` for a sample blockpage. This website was taken down in November 2013 because it sold counterfeit NFL products.

a jurisdictional issue, because U.S. courts were used to take down a domain used by a foreign organization [11, 80].

- **Cuban travel agency takedown.** In 2008, the U.S. Dept. of Treasury blacklisted 80 `.com` websites offering travel to Cuba [56]. The websites had been maintained for a decade by a British national operating through a Spanish travel agency, and they marketed to tourists in France and Italy. However, the domain names (*e.g.,* `www.cuba-hemingway.com`) were registered by eNom, a U.S.-based organization. In this instance, the operation depended on Treasury's Office of Foreign Assets Control, or OFAC, which publishes a terrorist watch list. The sites were added to the watchlist, and then taken down without going through a court or a judge, even though all of the affected parties, except for the DNS registrar, were not located or doing business in the US.

- **Counterfeit luxury goods.** In 2013, Project Cyber Monday IV seized 297 domain names that were determined to be selling counterfeit goods during the Christmas shopping season [71]. Working with at least ten law enforcement organizations worldwide U.S. Immigration and Customs Enforcement's (ICE) Homeland Security Investigations located and seized domains including `nflfavourite.com`, `Designerjeansforcheap.com`, and `seattle-seahawks-team-jersey.com` a "Cyber Monday bust." Takedowns such as these are not led only by ICE, as documented in a new research paper [15], which found that in 2012-2014 over 40,000 domains selling counterfeit luxury good were seized by "third-party brand protection services." In addition, luxury brands including Chanel [24], Oakley, and Uggs have undertaken such efforts on their own, filing bi-weekly court cases that seek to take down counterfeiters' domains. These court cases must be filed at regular intervals, because counterfeiters routinely circumvent the copyright holders' efforts, *e.g.,* by registering new domain names and manipulating search engine results [15]. These examples are striking because they resemble the controversial proposals made in the Stop Online Piracy Act (SOPA) [24,84].

These are just three examples of how takedowns have become an important tool for law enforcement, which also highlight the complexities and unintended consequences that arise when different legal frameworks are involved. Because the Internet transcends geopolitical borders, the DNS registry, the business corresponding to the domain that is registered, the people conducting business, and their customers could each be governed by a different set of laws. Complexities arise even when the activity is easily recognized as undesirable or criminal, *e.g.,* destructive malware, child pornography, or counterfeit goods. In the future, however, we can expect new challenges and disputes, especially internationally, if takedowns are adopted to achieve more controversial goals, such as censorship, political control, or economic advantage.

DNS takedowns are still possible with DNSSEC. The authority performing the takedown (*e.g.,* Verisign, which operates the `.com` TLD) holds the cryptographic secret keys used to delegate and translate names in its namespace (*e.g.,* all domain names ending in `.com`), so in the event of a takedown request it can simply sign entries cryptographically, which indicate that the domain either does not exist or has been redirected to a different IP address. DNSSEC does, however, introduce a few structural changes to the DNS hierarchy, which could make takedowns easier. Specifically, the DNS root currently consists of thirteen different root servers, managed by thirteen independent entities, which agree on delegations of names to top-level domains (TLDs). DNSSEC, however, is built around a single root of trust that holds the DNSSEC root key. This single root of trust could unilaterally decide to remove a TLD (*e.g.,* `.com`, `.ca`, `.cn`, `.xxx`) from the system; while in the absence of DNSSEC, the thirteen root zone operators would have to agree on the removal of a TLD [45].[3]

Reactions. The effectiveness of DNS takedowns may be limited, as several strategies have been devised to counteract their effects. These include methods for moving a site to a new domain, bypassing the DNS altogether, and dynamic methods for redirecting users to new sites.

As a first example, `www.wikileaks.org` was taken down by the U.S.-based `.org` TLD in 2010 but remained online by moving to the Swiss TLD as `www.wikileaks.ch`; the move was announced on Twitter, allowing Wikileaks readers to find the site at its new domain [72]. Similar techniques are used by botnets, which frequently use multiple domains for their command and control channels, updating them frequently and dynamically to avoid the effect of DNS takedowns [44, Sec 2.3.2]. As hundreds or thousands of new global TLDs (gTLDs) become available over the next several years, this strategy will become even more appealing.

As a second example, if a user already knows the IP address for the offending domain, then it can bypass the DNS altogether by typing the IP address directly into its browser; this is how Internet users in Turkey were able to circumvent local censorship [47]. Alternatively, Internet users can use browser plugins like MAFIAAFire [5], which provides browsers with a database of translations from domains that have been seized by governments to their original IP addresses, thus entirely circumventing the DNS. In a different vein, several projects seek to move from the DNS translation service to an entirely new translation mechanism [2, 4, 30, 81].

In a third strategy, it now appears that counterfeiters are responding to takedowns by factoring in that risk as part of their business plans [15]. It is not uncommon for users to be enticed to visit "stores" by flooding search engine results with "doorway" sites hosted on hacked webservers; the doorways then redirect the users to the counterfeit stores. In this scenario, as soon as a store's domain site is taken down, the doorways simply redirect users to the new domains hosting the stores. Meanwhile, it more difficult for plaintiffs to takedown the doorways, firstly, because they are hosted on legitimate domains that were subsequently hacked (and it is more difficult to seize legitimate domains), and secondly, because there are so many of them (and more can be easily purchased through underground forums) [15]. There are many variations on this theme, but they all involve various automated methods for "moving away" from the blocked DNS entry in a way that is as seamless as possible [15, 57, 61–63].

A different sort reaction poses a threat to DNSSEC itself. The fact that DNSSEC moves the DNS from thirteen autonomous root to a single logical root has detered some from deploying DNSSEC [45]. More speculatively, we can imagine scenarios in which different countries might decide to operate their own roots, their own copies of the TLDs, or at least take over the decision about when to forward requests to the actual TLD. This future balkanization of the Internet is not so farfetched; China, Indonesia and several other countries [6] already inject bogus responses to DNS queries for domains they wish to censor, block, or otherwise redirect. However, widespread deployment of DNSSEC would prevent the localized tampering with DNS responses that are used for filtering objectionable content in many countries.[4] In this situation, one could imagine a scenario in which DNSSEC is fully deployed, but authorities turn to DNS takedowns as a method for filtering web content.

[3] More detail on the organizational structure of the DNS and DNSSEC roots is given in [17, 54, 64].

[4] Because DNSSEC cryptographically authenticates DNS responses, DNS resolvers using DNSSEC will reject bogus DNS responses injected by third parties on the communication path that seeks to censor web content.

4 Interdomain routing and the RPKI

Interdomain routing systems allow Autonomous systems (ASes) to communicate with one another. A key part of this process is discovering routes to destination IP prefixes.

IP prefixes. An IP prefix is a set of Internet Protocol (IP) addresses with a common prefix. IP prefixes are allocated hierarchically to different organizations, with the root, IANA, delegating IP prefixes to Regional Internet Registries (RIRs), who then subdelegate to individual organizations.[5]

ASes and interdomain routing. An autonomous system (AS) is an independent network operated and controlled by a single organization. The Internet today is comprised of over 30,000 ASes, each controlled by an independent organization. Interdomain routing provides the glue that allows users in different ASes to communicate seamlessly. Each AS has an assigned AS number, *e.g.,* AS 15169 (Google), AS 3356 (Level3), and is allocated a set of IP prefixes; an AS is the *origin* for an IP prefix that is allocated to it. Importantly, the allocation of IP prefixes to organizations and origin ASes is handled entirely out of band (*i.e.,* external to the routing protocols), through procedures managed by the IANA, the RIRs and individual organizations. Thus, there is no technical means for an RIR to enforce, authenticate, or revoke the allocation of IP prefixes to an origin AS.

ASes are interconnected, creating a graph in which the nodes are ASes and the edges are the physical links between them. ASes then use the Border Gateway Protocol (BGP) to discover routes through the AS-level graph to a destination IP prefix. The routes specify how packets will travel through the Internet to reach the destination IP prefix at its origin AS.

Attacks on BGP. The design of BGP assumes that ASes will be honest about which prefixes are allocated to them, and this assumption creates an opportunity for attackers. Although most routing problems are localized and transient, arising from errors and misconfigurations, there have been several routing incidents that caused widespread outages [27, 73] or traffic interception [35, 74]. These incidents are enabled by BGP's lack of mechanisms to authenticate the allocation of IP prefixes to ASes. Thus, BGP is vulnerable to *prefix hijacks*, where a rogue AS originates a victim's IP prefix (that is not legitimately allocated to the rogue AS); this causes traffic intended for the victim IP prefix to flow to the rogue AS instead of the legitimate origin AS. The rogue AS can then drop, delay, tamper with, or silently intercept the traffic before sending it on to its intended destination.

The RPKI. The resource public key infrastructure (RPKI) is designed to prevent prefix hijacks by authenticating the allocation of IP prefixes to ASes. Like the DNS, the RPKI is based on a hierarchy of authorities; in the RPKI, this hierarchy mirrors the IP address allocation hierarchy. Each authority has a *Resource Certificate (RC)*, signed by its parent, containing its allocated IP address space and cryptographic public key. An RC can sign (a) other RCs to suballocate address space, or (b) *Route Origin Authorizations (ROAs)* can authorize an AS to originate an IP prefix in BGP. Routers can use then use the RPKI to distinguish between legitimate BGP routes, and bogus ones originated by hijackers; to prevent prefix hijacks, the router should discard (*i.e.,* ignore) routes the RPKI classifies as bogus [55].

[5] The set of IP addresses {8.8.8.0,8.8.8.1.,...,8.8.8.255} all the have the common prefix "8.8.8."; this prefix is 24-bits in length, and is written as 8.8.8.0/24 and pronounced as "eight dot eight dot eight dot zero slash twenty four." To illustrate IP prefix allocation, an RIR, the American Registry of Internet Numbers (ARIN), allocates IP prefix 8.0.0.0/8 to Level3, who further allocates a subprefix 8.8.8.0/24 to Google. The IP prefix 8.0.0.0/8 consists of the set of IP addresses {8.0.0.0,8.0.0.1,...,8.255.255.255}.

Takedowns. In the absence of the RPKI, BGP is completely decentralized with no loci of control. For this reason, RIRs have traditionally lacked the technical means to revoke or modify the IP prefixes they have allocated to an organization. In several cases an RIR received instructions from a court concerning an IP prefix it had allocated [43, 79], but in each case the RIR lacked the technical means to prevent routers from routing traffic to the disputed prefix. The RPKI addresses this issue by empowering its authorities to revoke or modify any ROA or resource certificate that they have issued. Because the ROAs determine the routes that routers select, an RPKI authority can take down an IP prefix by revoking the ROA that authorizes routing to this prefix [34]. In the absence of RPKI, this process of reclaiming an IP prefix requires costly, bilateral negotiation or even litigation, which limits the power of the delegator of address space. With RPKI, however, an authority can instantly and unilaterally takedown an IP prefix, simply by revoking the RCs or ROAs that it issued.

Reactions. Some operators and policy groups are cautious about adopting the RPKI and some have recommended against adopting it at all [12,18,79]. As one example, the European RIR, Rseaux IP Europens Network Coordination Centre (RIPE), held a plenary session in which its members almost rejected the adoption of the RPKI [66], and some have proposed technical mechanisms to harden the RPKI against authorities that abuse their power [28, 46, 52]. These mechanisms could make RPKI takedowns more transparent and easier to detect, but they would not eliminate completely the possibility of takedowns from the RPKI. Others have proposed methods for securing BGP that are decentralized and do not rely on an authentication mechanism at all [29, 50, 51]. Decentralized approaches such as these avoid the trust hierarchy and its associated locus of control, while providing a comparable level of security.

5 Encryption and the SSL Public Key Infrastructure (PKI).

The SSL Public Key Infrastructure (PKI) illustrates a less hierarchical, but still somewhat centralized, approach to securing the Internet.

The SSL PKI. The Transmission Control Protocol (TCP), which underlies the vast majority of today's Internet connections, does not support mechanisms for ensuring confidentiality or integrity. The Secure Sockets Layer (SSL) was devised to address this issue by providing end-to-end encrypted connections and authentication on top of TCP. SSL uses digital certificates to securely translate between a hostname (*e.g.,* `www.bankofamerica.com`) and its cryptographic public key, which is then use for encryption and authentication in SSL. The SSL Public Key Infrastructure (PKI), which is widely used today, prevents an adversary from binding its own cryptographic key to a victim's hostname, thereby allowing the adversary to decrypt or alter the SSL messages sent to or received from the victim.

The SSL PKI uses a flat allocation scheme, where every authority, known as a *certificate authority* or *CA*, is authorized to allocate or translate any hostname. Today, the SSL PKI consists of thousands of authorities, each potentially presiding over the entire space of all possible hostnames [40]. This flat architecture is nicely democratic, providing the holder of a name with a choice of multiple CAs that it can use to securely translate its hostname to a cryptographically secure public key. This prevents a single entity from controlling the entire system and eliminates the threat of takedowns—if a CA unilaterally revokes (*i.e.,* takes down) a certificate it issued, the subject of the revoked certificate can simply obtain another one for its hostname from a different

CA.

Attacks on the SSL PKI. On the other hand, the flat architecture of the SSL PKI means that compromising even a single CA in this system can compromise the security of *any* hostname. The unlimited scope of each CA in the SSL PKI means that such compromises can have serious implications outside the border of a single country or legal jurisdiction. In 2011, for instance, Iranian hackers compromised the Dutch certificate authority Diginotar and began issuing bogus certificates for `www.google.com` and other websites based in the U.S.. Although Diginotar usually issued certificates for entities based in the Netherlands, the structure of SSL PKI allowed Diginotar to issue certificates for websites anywhere in the world, and this vulnerability was exploited by the Iranian hackers [42].

Interventions CAs are vulnerable to government intervention. For example, a government could lawfully compel a CA operating in its jurisdiction to issue phony certificates for a target hostname. Because CAs are now spread throughout the world, such interventions could occur for myriad reasons. Again, because the SSL PKI does not limit the scope of the names that can be translated by a given CA, it is technically feasible for such actions can be undertaken even when the target's hostname is outside of the government's jurisdiction. Although this risk is still speculative, one research paper found evidence that law enforcement agencies have considered exploiting this capability by importing "a copy of any legitimate key [law enforcement agencies] obtain (potentially by court order)" [85]. Also, authorities have apparently "circumvent[ed] encryption by impersonating security certificates" for Google [41]. Although it is not clear how this occurred, one possibility is that some CAs were compelled to issue phony certificates for Google's hostnames.

Reactions. Although attacks on the SSL PKI have caused alarm in the network security community, the SSL PKI is arguably too entrenched in the web ecosystem to be replaced, wholesale. Going forward, the SSL PKI is likely to become even more important as network protocols (*e.g.,* HTTP [31]) migrate towards using encryption by default. As such, a variety of technical remedies have been proposed to harden the SSL PKI against attack [67].

One approach is called Certificate Transparency [1], which calls for a new set of centralized authorities to maintain auditable logs of which CAs issue certificates for which hostnames. The logs would be publicly visible and could be used to detect when a hacked or misbehaving CA (*e.g.,* Diginotar) issues a phony certificate for a hostname (`www.google.com`) that is outside its usual purview [1]. Importantly, these authorities and logs are designed so that they are easily audited by relying parties that use them, allowing for easy detection of compromises or misbehavior by these new centralized authorities. Another proposal, called DANE [48], suggests using DNSSEC as a parallel infrastructure for issuing SSL certificates. The key idea here is to impose hierarchical structure on the flat SSL PKI architecture, thus preventing an authority (*e.g.,* Boston University) from issuing certificates for names that are outside the authority's scope in the DNS hierarchy (names that do not end in `bu.edu`). Both approaches would add hierarchy and centralization, potentially increasing the risk of takedowns in the SSL PKI.

6 Discussion

The examples discussed in Sections 3-5 illustrate some of the ways in which the core infrastructures of the Internet have become points of leverage, whether as tools for local law enforcement, loci of security and privacy mechanisms, or as control points for political ends, such as censorship, surveillance, and cyberwarfare. Two of these control points—the DNS root and the RPKI—are in the early stages of their deployment, and each of them grafts a hierarchical/centralized structure onto the decentralized Internet design.

Hierarchies such as the DNS and RPKI are appealing because they are easy to manage and maintain through top-down control by appropriately limiting the scope of each authority. As we have seen, however, both of the hierarchical structures we described are double-edged swords, providing opportunities to improve Internet security for all while similarly providing opportunities to selectively isolate nodes. The U.S. is a strong proponent of an open interoperable Internet, but it also uses the infrastructure to enforce its laws, often in cooperation with the international law enforcement community. These actions can disrupt criminal activities, at least in the short run, *e.g.,* by cutting off purveyors of illegal goods and services from their customers. As we discussed earlier, however, the effectiveness of these approaches may be waning [15], and there is also potential for collateral damage [9, 11, 69, 80]. Importantly, these actions also set a precedent for governments to intervene in the Internet infrastructure. Other governments are already actively blocking applications (*e.g.,* Turkey's block of Twitter [47]) and censoring content (as China has done for years), although today most of these actions use mechanisms other than those described here. Also, the blocking is limited in scope to relying parties in the country's own networks and does not block access for *all* relying parties worldwide, like the takedowns we have discussed. A concern is that interventions via the core Internet protocols (DNS, DNSSEC, RPKI, the SSL PKI, *etc.*) will continue to escalate, especially as more of the Internet infrastructure moves outside U.S. control.

The U.S. currently enjoys a privileged position with respect to many of these law enforcement actions. Much of the Internet infrastructure is owned by U.S.-based companies and is, therefore, governed by U.S. law. This situation is changing, and the pace of change is likely to accelerate for several reasons: ICANN's planned rollout of thousands of new generic TLDs; the March, 2014 announcement of the U.S. intention to transition the IANA functions to a global multistakeholder community; and continuing buildout of Internet access and supporting infrastructure throughout the developing world. As other countries gain legal authority over gTLD registries, develop their own Internet Exchange Points and networking infrastructure, control portions of the RPKI hierarchy or fail to adopt it altogether, and rely on their own CAs, there is potential for an ever-escalating path of activities that promote political and commercial objectives—both legal and illegal, and both benign and harmful—by manipulating the core infrastructures of the Internet.

Although we do not have a single proposal to resolve these issues, there are some general principles, which if followed, could help mitigate the negative impacts of these manipulations:

1. International restraints that discourage using core Internet infrastructures to enforce policy or local laws, except under well-defined and mutually agreeable circumstances. For example, a small initial step would be an established practice that whenever a website is taken down, the responsible party puts up a blockpage explaining why, who did it, and under what authority, similar to those currently displayed when ICE takes down a page.

2. Where possible, interventions should be pushed out to the network edge and up to the application layer, moving away from the core and lower layers of the network architecture [25]. This would minimize the risks of collateral damage, and disagreements could be addressed on a local rather than a global scale. Thus, rather than enforcing a copyright violation by forcing the `.com` registrar to remove an entry from the global DNS table, enforcement actions could

be taken at the local ISP or user level. One alternative to manipulating the DNS directly might be opt-in blacklists that are external to the Internet core, similar to those used by search engines or for detecting spam [7]. One complication to this principle is the advent of global platforms such as Google, Facebook, and Twitter, each of which has global extent. These applications increasingly provide the only point of access for users, and in some cases are even building out their own networking infrastructures. In this setting, interventions by a local entity (*e.g.,* Canada) that have global impact (*e.g.,* removing content globally [13]) are problematic in the same way a DNS takedown can be.

3. Where possible, design new security structures that are decentralized and resist the temptation to introduce new hierarchical structures or to use the existing ones for new purposes. The Internet succeeded in large part because of its decentralized robust design. We should expect the same out of the security mechanisms that we use to enhance our experience on the Internet. Although challenging, distributed security solutions are technically feasible and could be investigated much more aggressively.

7 Conclusion

In this paper we described the basic design of three important enhancements to the Internet, DNSSEC, RPKI, and SSL PKI, which provide secure translation infrastructures through a hierarchical authentication structure. We also discussed how hierarchical structures in the Internet afford authorities a point of control for intervention, posing a security tradeoff, and finally, how these two uses of hierarchy in the Internet are in tension, exacerbating existing threats to a global, open, and interoperable Internet. Our focus here has been primarily technical, but in future work, we plan to explore the legal and policy frameworks that could mitigate some of the unintended negative consequences that we have described.

It was inevitable that money, law, and politics would discover the Internet. This is not a genie that can be put back in the bottle. Given the Internet's central role in virtually all human activities today—economic, personal, social, and political—it is not surprising that governments have found compelling reasons to mediate these interactions. How they do so, however, will determine whether or not the Internet can remain an open, interoperable platform, that continues to support economic growth and stimulate human creativity. As many have observed, our current financial, legal, and political institutions, which are nation-centric, are a poor fit for the decentralized borderless design of the Internet. Resolving these tensions in a way that satisfies governments without destroying the proverbial *goose that laid the golden egg*, with all of the economic prosperity, creativity, and human interchanges that it has brought, is the major Internet challenge for the immediate future.

Acknowledgements

We thank Robert Axelrod, Kyle Brogle, Danny Cooper, Ethan Heilman, Michele Markoff, Danny McPherson, Leonid Rezyin and Tony Tauber for discussions and earlier research collaborations that motivated this work. SF gratefully acknowledges the partial support of DARPA (P-1070-113237), NSF (SHF-0905236), DOE (DE-AC02-05CH11231), the Santa Fe Institute, and the National Academies of Science Jefferson Science Fellowship. SG gratefully acknowledges the support of the NSF (1017907, 1350733) and the Sloan Foundation.

References

[1] Certificate transparency. http://www.certificate-transparency.org/.

[2] dot-bit. namecoin wiki. https://dot-bit.org/Namecoin.

[3] European Union Agency for Network and Information Security. Good practices guide for deploying DNSSEC. http://www.enisa.europa.eu/activities/Resilience-and-CIIP/networks-and-services-resilience/dnssec/gpgdnssecp.

[4] Github: namecoin repository. https://github.com/namecoin/namecoin.

[5] MAFIAAFire Redirector :: Add-ons for Firefox. http://www.mafiaafire.com/.

[6] The open network initative. http://opennet.net/.

[7] The spamhaus project. http://www.spamhaus.org/.

[8] Domain conflicts and the legal system: A guide for lawyers, judges, prosecuting authorities and the police. UNINETT Norid AS, 2012. http://www.norid.no/publikasjoner/domenejus-en.pdf.

[9] Microsoft disrupts nitol botnet in piracy sweep, September 2012. http://krebsonsecurity.com/2012/09/microsoft-disrupts-nitol-botnet-in-piracy-sweep/ (downloaded 7/15/14).

[10] Special agents and officers seize more than $4.8 million in fake nfl merchandise and seize 307 websites during 'operation fake sweep'. U.S. Immigration, Customs, and Enforcement (ICE) News Release, February 2 2012. https://www.ice.gov/news/releases/1202/120202indianapolis.htm.

[11] Microsoft v. john does 1-18, controlling a computer botnet thereby injuring microsoft and its customers. Complaint filed in the United States District Court for the Eastern District of Virginia, January 2013. http://noticeofpleadings.com/images/Complaint.pdf (downloaded 7/15/14).

[12] Working group 6, secure bgp deployment, final report. Technical report, FCC CSRIC Working Group 6, March 2013.

[13] Canadian court to the entire world: No links for you! Electronic Freedom Foundation, June 2014. https://www.eff.org/deeplinks/2014/06/canadian-court-entire-world-no-links-you (Downloaded July 17, 2014).

[14] Domain Name System Security (DNSSEC). Official website of the Department of Homeland Security, January 3 2014. http://www.dhs.gov/domain-name-system-security-dnssec.

[15] Search and Seizure: The Effectiveness of Interventions on SEO Campaigns. In *Proc. of ACM Internet Measurement Conference (IMC)*, 2014.

[16] Symantec mss threat landscape update gameover zeus and cryptolocker takedown. Symantec Managed Security Services Blog, June 2014. http://www.symantec.com/connect/blogs/symantec-mss-threat-landscape-update-gameover-zeus-and-cryptolocker-takedown (downloaded July 14, 2014).

[17] Joe Abley, David Blacka, David Conrad, Richard Lamb, Matt Larson, Fredrik Ljunggren, David Knight, Tomofumi Okubo, and Jakob Schlyter. DNSSEC root zone high level technical architecture. Technical report, Root DNSSEC Design Team http://www.root-dnssec.org/wp-content/uploads/2010/06/draft-icann-dnssec-arch-v1dot4.pdf.

[18] Shane Amante. Risks associated with resource certification systems for internet numbers, 2012.

[19] Anonymous. The collateral damage of internet censorship by DNS injection. *ACM SIGCOMM Computer Communication Review*, 42(3), 2012.

[20] R. Arends, R. Austein, M. Larson, D. Massey, and S. Rose. DNS Security Introduction and Requirements. RFC 4033 (Proposed Standard), 2005. Updated by RFC 6014.

[21] R. Arends, R. Austein, M. Larson, D. Massey, and S. Rose. *RFC 4034: Resource Records for the DNS Security Extensions.* Internet Engineering Task Force (IETF), 2005. http://tools.ietf.org/html/rfc4034.

[22] R. Arends, R. Austein, M. Larson, D. Massey, and S. Rose. *RFC 4035: Protocol Modifications for the DNS Security Extensions.* Internet Engineering Task Force (IETF), 2005. http://tools.ietf.org/html/rfc4035.

[23] ARIN. ARIN resource certification. https://www.arin.net/resources/rpki.html.

[24] Venkat Balasubramani. Court oks private seizure of domain names which allegedly sold counterfeit goods "chanel, inc. v. does". Technology & Marketing Law Blog, November 2011. http://blog.ericgoldman.org/archives/2011/11/court_oks_priva.htm.

[25] R. Barnes, A. Cooper, and O. Kolkman. Technical considerations for internet service filtering. IETF Informational Draft, January 2014. tools.ietf.org/html/draft-iab-filtering-considerations-06.

[26] Steven M. Bellovin. Using the domain name system for system break-ins. Proceedings of the Fifth USENIX UNIX Security Symposium, 1995.

[27] Martin A Brown. Rensys Blog: Pakistan hijacks YouTube. http://www.renesys.com/blog/2008/02/pakistan_hijacks_youtube_1.shtml.

[28] R. Bush. *RPKI Local Trust Anchor Use Cases.* Internet Engineering Task Force (IETF), 2013. http://www.ietf.org/id/draft-ymbk-lta-use-cases-00.txt.

[29] K Butler, T Farley, P McDaniel, and Jennifer Rexford. A survey of BGP security issues and solutions. *Proceedings of the IEEE*, 2010.

[30] Christian Cachin and Asad Samar. Secure distributed dns. In *Dependable Systems and Networks, 2004 International Conference on*, pages 423–432. IEEE, 2004.

[31] Richard Chirgwin. Mandatory HTTP 2.0 encryption proposal sparks hot debate. *The Register*, November 14 2013. http://www.theregister.co.uk/2013/11/14/http_20_encryption_proposal_sparks_hot_debate/.

[32] S. Chokhani, W. Ford, R. Sabett, C. Merrill, and S. Wu. *RFC 3647: Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practices Framework.* Internet Engineering Task Force (IETF), 2003. http://www.ietf.org/rfc/rfc3647.txt.

[33] D. Cooper, S. Santesson, S. Farrell, S. Boeyen, R. Housley, and W. Polk. *RFC 5280: Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile.* Internet Engineering Task Force (IETF), 2008. http://www.ietf.org/rfc/rfc5280.txt.

[34] Danny Cooper, Ethan Heilman, Kyle Brogle, Leonid Reyzin, and Sharon Goldberg. On the risk of misbehaving rpki authorities. In *HotNets XII*, November 2013.

[35] J. Cowie. Rensys blog: China's 18-minute mystery. http://www.renesys.com/blog/2010/11/chinas-18-minute-mystery.shtml.

[36] Mariano Cunietti. Notification and takedown from an isp standpoint. ECTA Conference, November 2012. http://www.slideshare.net/MarianoCunietti/ecta-notification-and-takedown-in-italy.

[37] A. Deacon and R. Hurst. *RFC 5019: The Lightweight Online Certificate Status Protocol (OCSP) Profile for High-Volume Environments.* Internet Engineering Task Force (IETF), 2008. http://tools.ietf.org/html/rfc5019.

[38] DNS Nawala. http://www.nawala.org/.

[39] Maximillian Dornseif. Government mandated blocking of foreign web content. *CoRR*, cs.CY/0404005, 2004.

[40] Zakir Durumeric, James Kasten, Michael Bailey, and J. Alex Halderman. Analysis of the HTTPS certificate ecosystem. In *Proceedings of the 13th Internet Measurement Conference*, October 2013.

[41] Ryan Gallagher. New snowden documents show nsa deemed google networks a "target". *Slate*, September 9 2013. http://www.slate.com/blogs/future_tense/2013/09/09/shifting_shadow_stormbrew_flying_pig_new_snowden_documents_show_nsa_deemed.html.

[42] Eva Galperin, Seth Schoen, and Peter Eckersley. A post mortem on the iranian diginotar attack. *EFF Blog*, September 2011.

[43] Eric Goldman. Sex.com an update, 2006. http://blog.ericgoldman.org/archives/2006/10/sexcom_an_updat.htm.

[44] James Graham, Ryan Olson, and Rick Howard, editors. *Cyber Security Essentials*. CRC Press, 2010.

[45] Phillip Hallam-Baker. http://www.ietf.org/mail-archive/web/ietf/current/msg59240.html. IETF Discussion mailing list, November 6 2009.

[46] Ethan Heilman, Danny Cooper, Leonid Reyzin, and Sharon Goldberg. From the Consent of the Routed: Improving the Transparency of the RPKI. *Proc. ACM SIGCOMM Conference*, 2014.

[47] Megan Hess. Fighting turkey's twitter ban with dns graffiti. Mashable Blog, March 2014. http://mashable.com/2014/03/21/twitter-ban-turkey-graffiti/.

[48] P. Hoffman and J. Schlyter. *RFC 6698: The DNS-Based Authentication of Named Entities (DANE): Transport Layer Security (TLS) Protocol: TLSA*. Internet Engineering Task Force (IETF), 2012. http://tools.ietf.org/html/rfc6698.

[49] Dan Kaminsky. Black ops 2008: Its the end of the cache as we know it. *Black Hat USA*, 2008.

[50] J. Karlin, J. Rexford, and S. Forrest. Pretty good bgp: Improving bgp by cautiously adopting routes. In *Proc. of the 2006 International Conference on Netowrk Protocols (CNP)*, 2006.

[51] J. Karlin, J. Rexford, and S. Forrest. Autonomous security for autonomous systems. *Computer Networks*, 52:29082923, 2008.

[52] S. Kent and D. Mandelberg. *Suspenders: A Fail-safe Mechanism for the RPKI*. Internet Engineering Task Force (IETF), 2013. http://tools.ietf.org/html/draft-kent-sidr-suspenders-00.

[53] Brenden Kuerbis and Milton Mueller. Securing the root: A proposal for distributing signing authority. *Paper IGP07-002*, 2007.

[54] Brenden Kuerbis and Milton Mueller. Securing the root. *Opening standards: The global politics of interoperability*, page 45, 2011.

[55] M. Lepinski and S. Kent. *RFC 6480: An Infrastructure to Support Secure Internet Routing*. Internet Engineering Task Force (IETF), 2012. http://tools.ietf.org/html/rfc6480.

[56] Adam Liptak. A wave of the watch list, and speech disappears. New York Times, March 2008. http://www.nytimes.com/2008/03/04/us/04bar.html?_r=0.

[57] He Liu, Kirill Levchenko, Márk Félegyházi, Christian Kreibich, Gregor Maier, Geoffrey M Voelker, and Stefan Savage. On the effects of registrarlevel intervention. *Proc. of 4th USENIX LEET*, 2011.

[58] Carolyn Duffy Marsan. Will feds mandate internet routing security? *NetworkWorld*, December 10 2010.

[59] Corynne Mcsherry. U.s. government seizes 82 websites: A glimpse at the draconian future of copyright enforcement? Electronic Frontier Foundation, November 29 2010. https://www.eff.org/deeplinks/2010/11/us-government-seizes-82-websites-draconian-future.

[60] S.A. Misel. "Wow, AS7007!". Merit NANOG Archive, April 1997. http://www.merit.edu/mail.archives/nanog/1997-04/msg00340.html.

[61] Tyler Moore and Richard Clayton. Examining the impact of website take-down on phishing. In *APWG eCrime Researchers Summit*, pages 1–13, 2007.

[62] Tyler Moore and Richard Clayton. The consequence of non-cooperation in the fight against phishing. In *APWG eCrime Researchers Summit*, pages 1–14. IEEE, 2008.

[63] Tyler Moore and Richard Clayton. The impact of incentives on notice and take-down. In M.E. Johnson, editor, *Managing Information Risk and the Economics of Security*, pages 199–223. Springer, 2009.

[64] Milton Mueller. *Ruling the root: Internet governance and the taming of cyberspace.* The MIT Press, 2004.

[65] Milton Mueller and Brenden Kuerbis. Negotiating a new governance hierarchy: An analysis of the conflicting incentives to secure internet routing. *Communications and Strategies*, (81):125–142, 2011.

[66] Michele Neylon. Ripe members vote to continue rpki work. CircleID, November 2011. http://www.circleid.com/posts/20111103_ripe_members_vote_to_continue_rpki_work/.

[67] NIST. Workshop on Improving Trust in the Online Marketplace, 2013. http://www.nist.gov/itl/csd/ct/ca-workshop-agenda2013.cfm.

[68] The European Union Court of Justice. Judgment of the court (grand chamber). InfoCuria - Case-law of the Court of Justice, May 13 2014. http://curia.europa.eu/juris/document/document.jsf?text=&docid=152065&pageIndex=0&doclang=EN&mode=lst&dir=&occ=first&part=1&cid=510076.

[69] Gunter Ollman. Nitol and 3322.org takedown by microsoft. CircleID Blog, September 2012. http://www.circleid.com/posts/20120913_nitol_and_3322org_takedown_by_microsoft/.

[70] E Osterweil, M Ryan, and D Massey. Secspider. http://secspider.cs.ucla.edu/.

[71] Gregory Palmore. Ice, international law enforcement agencies seize 706 domain names selling counterfeit merchandise. Dept. of Homeland Security, 2013. http://thepolicenews.net/default.aspx/act/newsletter.aspx/category/news+1-2/MenuGroup/home/NewsLetterID/41825.htm.

[72] Mahendra Palsule. Everydns.net terminates wikileaks.org dns services, wikileaks.ch back up in switzerland. Skeptic Geek Blog, December 2010. http://www.skepticgeek.com/miscellaneous/everydns-net-terminates-wikileaks-dns-services/.

[73] Tom Paseka. Cloudflare blog: Why google went offline today., November 2012. http://blog.cloudflare.com/why-google-went-offline-today-and-a-bit-about.

[74] Andrea Peterson. Researchers say u.s. internet traffic was re-routed through belarus. thats a problem. *The Washington Post*, November 20 2013. http://www.washingtonpost.com/blogs/the-switch/wp/2013/11/20/researchers-say-u-s-internet-traffic-was-re-routed-through-belarus-thats-a-problem/.

[75] A. Pilosov and T. Kapela. Stealing the Internet: An Internet-scale man in the middle attack, 2008. DEFCON’16.

[76] Dave Piscitello. Guidance for preparing domain name orders, seizures & takedowns. Technical report, ICANN, March 2012.

[77] Dave Piscitello. The value of assessing collateral damage before requesting a domain seizure. Technical report, ICANN, January 2013.

[78] Nathaniel Popper and Tiffany Hsu. Fbi shuts down internet poker sites. Los Angeles Times, April 15 2011.

[79] Internet Governance Project. An important case, RIPE-NCC seeks legal clarity on how it responds to foreign court orders, 2011. http://www.internetgovernance.org/2011/11/23/in-important-case-ripe-ncc-seeks-legal-clarity-on-how-it-responds-to-foreign-court-orders/.

[80] Suresh Ramasubramanian. Microsoft's takedown of 3322.org - a gigantic self goal? CircleID, September 2012. http://www.circleid.com/posts/20120917_microsoft_takedown_of_3322_org_a_gigantic_self_goal/ (downloaded 7/15/14).

[81] V Ramasubramanian and EG Sirer. The design and implementation of a next generation name service for the internet. *ACM SIGCOMM Computer Communication Review*, 34(4):331–342, 2004.

[82] Venugopalan Ramasubramanian and Emin Gun Sirer. Perils of transitive trust in the domain name system. In *Proceedings of the 5th ACM SIGCOMM conference on Internet Measurement*, pages 35–35. USENIX Association, 2005.

[83] RIPE. RIPE NCC Resource Certification. http://www.ripe.net/certification/.

[84] Lamar S. Smith. *H.R.3261 – Stop Online Piracy Act.* 2011.

[85] Christopher Soghoian and Sid Stamm. Certified lies: Detecting and defeating government interception attacks against ssl (short paper). In *Financial Cryptography and Data Security*, pages 250–259. Springer, 2012.

[86] Marc Stevens, Alexander Sotirov, Jacob Appelbaum, Arjen Lenstra, David Molnar, Dag Arne Osvik, and Benne De Weger. Short chosen-prefix collisions for md5 and the creation of a rogue ca certificate. In *Advances in Cryptology-CRYPTO 2009*, pages 55–69. Springer, 2009.

[87] Joe Stewart. Dns cache poisoning–the next generation, 2003.

[88] The President's National Security Telecommunications Advisory Committee. Nstac report to the president on communications resiliency, 2011.

[89] J.P. Verkamp and M. Gupta. Inferring mechanics of web censorship around the world. In *Usenix FOCI*, 2012.

[90] ViewDNS.info. DNS cache poisoning in the People's Republic of China, 2011. http://viewdns.info/research/dns-cache-poisoning-in-the-peoples-republic-of-china/.

[91] Paul Vixie. Dns and bind security issues. In *Proceedings of the 5th USENIX UNIX Security Symposium, USENIX Association, Berkeley, CA*, 1995.

[92] Chester Wisniewski. Turkish certificate authority screwup leads to attempted google impersonation. Naked Security Blog, January 4 2013.

[93] J. Zittrain and B. Edelman. Internet filtering in China. *IEEE Internet Computing*, 7(2):70–77, 2003.