Accelerating DNSSEC Deployment: The Opportunity for an FCC Bully Pulpit

Eric Mannes, Kesiena Owho-Ovuakporie, Clark Wood

{mannes, kesiena, cl24536}@mit.edu; The Massachusetts Institute of Technology

ABSTRACT

The Federal Communications Commission (FCC) has a unique opportunity to leverage its statutory authority and community relations to push forward implementation of the Domain Name System Security Extensions (DNSSEC). DNSSEC prevents DNS spoofing attacks, which attackers can use to hijack Internet traffic. This type of attack has been used in real-world attacks like DNSChanger[1], a clickjacking campaign estimated to have caused over $14 million in damages. Further, the vulnerability of DNS allows attackers to redirect any user's Internet session to a malicious web page. Such redirection has been used in campaigns like the Brazilian Boleto Fraud Scheme, which has caused $3.75 billion in damages so far[2]. Many users would be unable to tell a genuine web page from a counterfeit, and may give personal data to criminals.

We consider the reasons why key stakeholders, like recursive nameserver operators, top level domain registries, and domain registrars have not implemented DNSSEC, despite its positive, incremental benefits for Internet security. We argue that the FCC can leverage its authority over Internet Service Providers (ISPs) to enact positive change, not by passing

[1] Biggest Cybercriminal Takedown in History. (2011, November 9). Retrieved from http://krebsonsecurity.com/2011/11/malware-click-fraud-kingpins-arrested-in-estonia/

[2] Kovacs, E. (2015, February 10). Cybercriminals Use DNS Poisoning in Brazilian Boleto Fraud Scheme. Retrieved from http://www.securityweek.com/cybercriminals-use-dns-poisoning-brazilian-boleto-fraud-scheme

regulations, but by proposing non-legislative policy statements, similar to the Anti-Botnet Code[3], which ISPs voluntarily agreed to, or the Internet Policy Statement, which ISPs have committed to uphold as part of recent merger agreements approved by the FCC[4]. The FCC can then dictate future policy, and hold ISPs responsible for their promises. Lastly, we provide a draft of such a document.

CONTENTS

[3] Federal Communications Commission. (2013d). *U.S. Anti-Bot Code of Conduct (ABC) for Internet Services Providers (ISPs)* (Final Report). CSRIC III Working Group 7. Retrieved from https://transition.fcc.gov/bureaus/pshs/advisory/csric3/CSRIC_III_WG7_Report_March_%202013.pdf

[4] See FCC APPROVES SBC/AT&T AND VERIZON/MCI MERGERS. (2005, October 31) and FCC APPROVES MERGER OF AT&T INC. AND BELLSOUTH CORPORATION. (2006, December 29).

INTRODUCTION

The FCC has a unique opportunity to push forward implementation of the Domain Name System Security Extensions (DNSSEC) by working through the Communications Security, Reliability, and Interoperability Council (CSRIC). This council, composed of members from the FCC, but also from private software companies and ISPs, has a history of persuading ISPs to address internet security issues, as when they developed a voluntary Anti-Bot code of conduct[5]. ISPs adopted the Code, agreeing not only to take meaningful action against botnets, but also to share information with other ISPs who signed the pledge, with the FCC offering only to list complying ISPs on a publicly available web page[6]. This is an excellent example of a bully pulpit for Internet security, where the FCC directed action from ISPs not by creating rules and regulations, but by calling attention to an area of need.

We believe the FCC can replicate its prior success with the Anti-Botnet code by leveraging another CSRIC Working Group's proposal. Along with an Anti-Botnet Code, ISPs also agreed to take substantive steps toward implementing the Domain Name Service Security Extensions (DNSSEC) recommended by Working Group 5. This technology cryptographically signs DNS records, so that their integrity can be verified. This makes it impossible for a malicious DNS resolver to lie about the Internet Protocol (IP) address to which a hostname resolves, thereby preventing attacks like DNSChanger[7], a clickjacking campaign estimated to

---

[5] Federal Communications Commission. (2013). *U.S. Anti-Bot Code of Conduct (ABC) for Internet Services Providers (ISPs)* (Final Report). CSRIC III Working Group 7. Retrieved from https://transition.fcc.gov/bureaus/pshs/advisory/csric3/CSRIC_III_WG7_Report_March_%202013.pdf

[6] ABCs for ISPs. (n.d.). Retrieved from https://www.m3aawg.org/abcs-for-ISP-code

[7] Biggest Cybercriminal Takedown in History. (2011, November 9). Retrieved from http://krebsonsecurity.com/2011/11/malware-click-fraud-kingpins-arrested-in-estonia/

have caused over $14 million in damages, or the 2009 Twitter hacking by the Iranian Cyber Army[8].

The FCC, with authority derived from congressional mandates, legal precedents, and an ongoing, two-way relationship with Internet stakeholders, possesses an opportunity to improve global Internet infrastructure security by publicly championing the adoption of best practices by Internet Service Providers (ISPs). In particular we address an opportunity for the FCC to push forward DNSSEC adoption. In this paper we:

1. Explain the technology underpinning DNSSEC and assess the harm caused by the lack of DNSSEC adoption.
2. Consider the market costs and economic feasibility of DNSSEC adoption from various stakeholders' points of view.
3. Detail the FCC's authority over ISPs, and its ability to direct attention to security improvements like DNSSEC through councils like CSRIC.

After assessing the technical, stakeholder market, and legal situations, we detail a concrete plan of action that the FCC could implement, paying attention to how this plan could be generalized to future Internet security efforts studied by other Working Groups, like BGPsec implementation or the adoption of the 20 Critical Security controls. Our proposal leverages the work of CSRIC and its Working Groups, which bring together diverse stakeholders that are uniquely suited to identifying problems like DNS attacks and developing solutions. We suggest that the FCC go further by issuing non-legislative policy statements that request ISP participation and hint at possible future regulation should they dally, and we draft an example statement in the Appendix.

[8] Beaumont, C. (2009, December 18). Twitter hacked by "Iranian Cyber Army." Retrieved from http://www.telegraph.co.uk/technology/twitter/6838993/Twitter-hacked-by-Iranian-Cyber-Army.html

Why DNSSEC

The Internet was not designed with security in mind, but consumers, private companies, and public government agencies all share an interest in the confidentiality, integrity, and availability of their data. Thus, the FCC may improve Internet infrastructure security by encouraging the adoption of DNSSEC. First introduced in 1997 and codified over several RFCs[9], DNSSEC cryptographically signs DNS records using public-key cryptography. DNSSEC guarantees the integrity of a response for a given DNS query, which would prevent certain network attacks like DNS spoofing. While not a panacea, we demonstrate that this would provide an incremental improvement in security for end users, and may also provide a platform upon which future services may be implemented[10].

For a host of reasons, however, DNSSEC has failed to gain traction. Chief among these issues is the complexity of deployment and the many stakeholders who must work in concert to successfully implement DNSSEC. ISPs are the least incentivized stakeholders because of the difficulty in transferring the implementation cost of DNSSEC to their consumers. Most small-office and home internet users do not fully appreciate the benefit of DNSSEC because they do not understand that after typing a domain name in a web browser, they may be redirected to a malicious website. For this reason, they do not demand DNSSEC-validating resolvers from their ISPs, hence there is little or no pressure on ISPs to implement DNSSEC. ISPs are currently undermining the efforts made by other key stakeholders by being reluctant to implement DNSSEC in their DNS resolvers. If the DNS resolvers of ISPs are not DNSSEC compliant, clients using such resolvers will be exposed to DNS attacks in spite of the

[9] Request for Comments by the Internet Engineering Task Force. Among others, RFC 4033, 4034, 4035, and 5155 pertain to DNSSEC. RFCs about DNS date back to RFC 882, written in November 1983.
[10] See RFC 6698: DNS-Based Authentication of Named Entities (DANE), a proposal for using DNSSEC to encrypt emails.

investments that may have been made by website administrators, domain name registries, DNS zone operators, and other key stakeholders that implement DNSSEC. We believe that the FCC could play a key role (through regulatory action or threat of regulation) in motivating the ISPs to implement DNSSEC. We show that much of the work has already been done by other key stakeholders and even some ISPs that have already implemented DNSSEC. Further, we argue the FCC should consider this an important issue because full DNSSEC deployment would lead to improved Internet security and help prevent some of the DNS attacks we have experienced in recent years.

To motivate our case, we first explain some of the technical underpinnings of routing and switching technology, and the DNS. We outline the DNS and DNSSEC protocols. We then focus our attention on DNS spoofing attacks, which DNSSEC is designed to prevent, and, citing specific attacks in the past few years, discuss the harms to consumers and website operators when users receive wrong DNS records. We also discuss existing alternatives that can mitigate the risks of DNS cache poisoning attacks, and then explain why DNSSEC is still an essential technology in spite of these alternatives. As an example, while HTTPS works well, it is inadequate on its own, and fails to prevent denial-of-service attacks that leverage DNS cache poisoning. In addition, a 2013 study by Google revealed that about 70% of Google Chrome users click through SSL warnings on web browsers, thereby leaving them vulnerable to cyber attacks resulting from invalid certificates when a website's DNS entry gets compromised[11]. DNSSEC will shield users from such attacks because if the DNS record of a signed domain is invalid, users will not receive any option that allows them to bypass DNSSEC security protection. We also review and address technical criticisms of DNSSEC, including that it allows

[11] Devdatta, Akhawe, and Felt Adrienne Porter. 2013. Alice in Warningland: A Large-Scale Field Study of Browser Security Warning Effectiveness. http://research.google.com/pubs/pub41323.html

for enumeration of the entire DNS zone file. Finally, we review the current status of DNSSEC deployment and what TLD operators, website operators, and DNS resolver operators (mostly ISPs) need to do in order for DNSSEC to be widely used.

After familiarizing the audience with the key technologies involved and presenting possible attack scenarios that DNSSEC resolves as motivation, we discuss some of the case law involving ISPs and the FCC, such as Verizon v. FCC[12], wherein the court upheld parts of the FCC Open Internet Order 2010 but struck down others which applied only to common carriers, and also examine the various authorities claimed by the FCC.

DNSSEC adoption could be significantly sped up by an FCC mandate because the DNS recursive resolver operators (mostly operated by ISPs and public DNS resolvers) are currently a significant bottleneck in DNS adoption. Full implementation of DNSSEC requires collective action from various stakeholders such as the top level domain (TLD) registries, domain name registrars, domain name registrants (i.e. website administrators), DNS zone operators and DNS recursive resolver operators. Although collective action is required from various stakeholders, the associated costs and benefits of DNSSEC implementation are not equally distributed amongst these stakeholders and they do not all have equal ability to transfer the implementation cost to the beneficiaries of DNSSEC implementation. Home internet users and website administrators are the main beneficiaries from improved Internet security. However, the recursive resolver operators (a service commonly provided by ISPs) have the least incentive to adopt DNSSEC due to market failure. The ISPs play a pivotal role in DNSSEC adoption because they need to take action in order for other key stakeholders to reap the benefits of DNSSEC implementation. We note, however, that some ISPs and public DNS resolvers, such

[12] Verizon Communications Inc. v. FCC (D.C. Circuit January 14, 2014).

as Comcast[13] and Google[14] have implemented DNSSEC, thereby implying that it is economically feasible and future adopters can piggyback on previous work, which could lead to reduced costs.

We tie together our technological, legal, and economic arguments into a plan of action for the FCC to implement. There exists a prime opportunity for the FCC to establish a cyber bully pulpit, wherein the FCC directs attention to insecurities that threaten to diminish the Internet as an open platform. The CSRIC Working Groups provide several opportunities. DNSSEC, chief among them and half finished for years, has powerful stakeholders with sunk costs which we can rally, and provides an incremental security and quality benefit to the consumer. We propose a detailed plan for what the FCC should request of ISPs and other stakeholders.

1 TECHNOLOGY AND THREATS

The *Domain Name System* (DNS) functions as an "address book" for the internet and is critical to its use. Users depend on DNS's accurate answers whenever they access any website. However, DNS is fundamentally insecure. Attackers can exploit flaws in DNS in order to direct users to malicious websites when they seek to access the internet. These attacks expose users to harm to phishing and identity theft, malicious computer software, spying, and censorship. These attacks can deny users access to the websites they seek to use and essentially take websites down from the internet.

In section 1.1, we provide an overview of the DNS protocol as it currently stands and explain why ISPs are central to any changes in its use. In section 1.2, we summarize the kinds of attacks available on the DNS protocol, the costs of these attacks, and existing non-DNSSEC

[13] http://corporate.comcast.com/comcast-voices/comcast-completes-dnssec-deployment
[14] https://googleonlinesecurity.blogspot.com/2013/03/google-public-dns-now-supports-dnssec.html

mitigations to these attacks. In section 1.3, we examine DNSSEC, a proposed set of changes to DNS, and explain how it will eliminate many of these attacks.

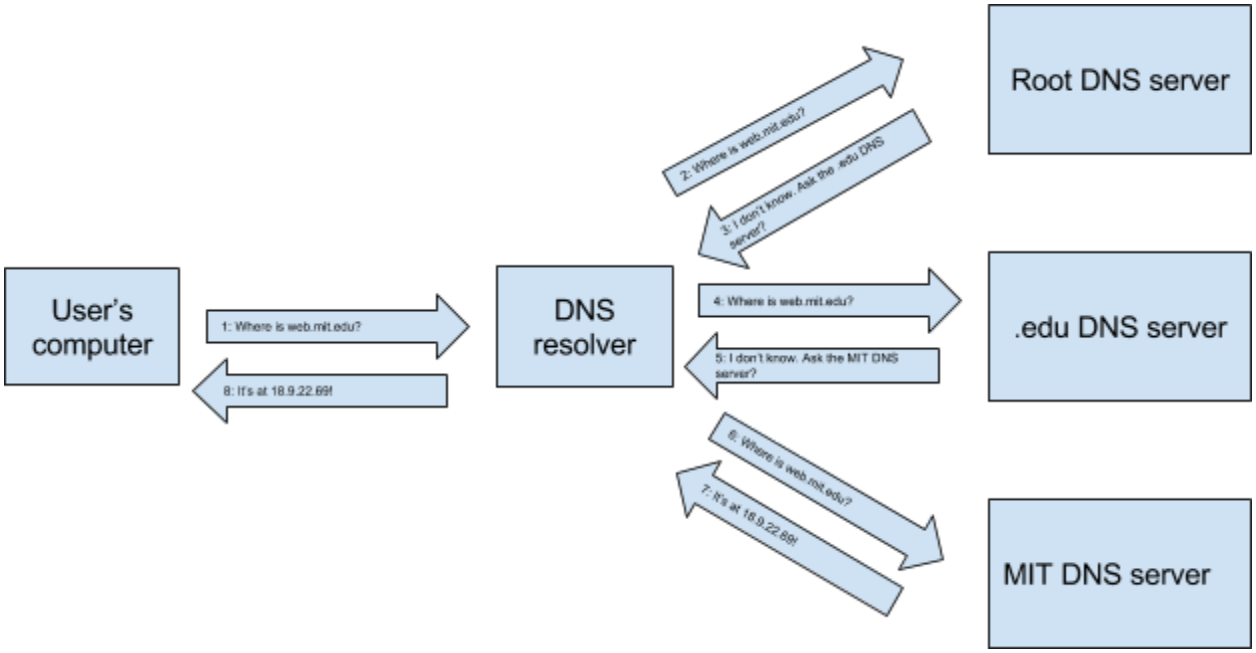
1.1 Overview of DNS

When a user wants to access a website, they generally remember only a human-readable domain name, such as “web.mit.edu”. However, in order for the user’s computer to connect to the website’s server, it needs the server’s *Internet Protocol (IP) address*, four numbers between 0 and 255 separated by periods (e.g., 18.9.22.69).[15] DNS is the system that bridges this gap. To get the server’s IP address, a program known as a *DNS resolver* contacts a DNS server (also known as a *name server*), which might send back a response that in part includes the following:

```
WEB.MIT.EDU.          60    IN    A     18.9.22.69
```

[15] This is an Internet Protocol version 4 (IPv4) address. The internet is migrating to IPv6, which has addresses that are made of six blocks of up to four hexadecimal digits each, separated by colons. For example, 2001:4860:4860:0000:00e1:f000, might be an IPv6 address, although it would usually be written as 2001:4860:4860::e1:f000, with leading zeros in each block omitted.

The returned record is of type “A,” which means the line is an address record, therefore implying that 18.9.22.69 is the IP address for web.mit.edu.[16]



DNS queries can be answered by recursively querying a hierarchy of name servers. Some name servers are responsible for a *zone*, which is a portion of the space of possible domain names. These servers are *authoritative* name servers for that zone. For example, to find the IP address for web.mit.edu, a resolver might start by querying one of the *root* name servers, which are at the top of the hierarchy and authoritative for all domains. The root server could refer the resolver to a name server authoritative for the “.edu” zone (the zone of domains ending with the “.edu” TLD), which could in turn refer the resolver to a name server authoritative for the “mit.edu” zone, which would return the desired address record. This hierarchy of name servers exists in part because there are too many domains for any single server to maintain the list of IP addresses of all of them. Importantly, DNS resolvers generally maintain a cache of recent answers to DNS queries so that they don’t have to be repeated.

[16] The number 715 is the “time to live,” in seconds, of the record: the amount of time until the answer expires.

We estimate here that 98% of all internet users depend on a DNS resolver operated by their ISP, which is why ISPs are so critical to DNSSEC deployment. Most personal computers and phones contain only a small program called a *stub resolver*, which typically relies on another resolver that performs recursive queries to answer queries on its behalf. When a user connects to the internet, their ISP gives them the address of a DNS resolver to use. However, users can manually change their DNS settings to use a resolver not operated by an ISP, the two largest of which are Google Public DNS and OpenDNS. In March 2013, Google announced that Google Public DNS received on average 130 billion DNS queries daily from 70 million unique IP addresses.[17] Over a 30-day period ending in November 2015, OpenDNS responded to almost 80 billion DNS queries daily.[18] Google's DNS-query-to-unique-IP ratio suggests that OpenDNS handles the requests of 50 million unique IP addresses a day. The number of internet-connected devices approximately doubled to about 10 billion between 2013 and 2015.[19] If Google Public DNS's market share remained the same, assuming a 1:1 ratio of devices per IP address (which is lower than the actual ratio), perhaps 190 million devices use Google Public DNS or OpenDNS today, or about only 2% of devices. The other 98% uses ISP-supplied DNS. Though significant, non-ISP DNS resolvers only resolve a small fraction of DNS queries, and any changes to DNS on the internet require the cooperation of ISPs.

1.2 Attacks on DNS

The DNS protocol, by design, is unauthenticated. This opens up the risk of hijacking attacks in which an attacker causes a DNS server to return a result of their choosing. When DNS resolver queries an authoritative name server, it has no way of verifying that the response

[17] https://googleblog.blogspot.com/2012/02/google-public-dns-70-billion-requests.html
[18] https://system.opendns.com/, accessed November 15, 2015.
[19] http://www.businessinsider.com/internet-of-everything-2015-bi-2014-12

that comes back is from the server that it queried. DNS is thus vulnerable to hijacking. There are three primary types of DNS hijacking attacks:

1. An attacker forges a malicious response to a DNS query, causing a resolver to cache the wrong address for a domain, in what is known as a *cache poisoning attack*. Anyone who uses the resolver with the poisoned cache to look up that domain will then be directed to an IP address of the attacker's choosing.
2. The attacker hacks a zone operator or domain registrar and alters the DNS records for a website.
3. The attacker is the resolver operator and returns malicious answers to queries.

DNS hijacking attacks occur in the real world. In 2008, Dan Kaminsky found a fundamental vulnerability in the DNS protocol that made it possible for an attacker to easily poison the cache of most DNS servers in use on the internet. Though the affected DNS server implementations released patches to make it difficult to exploit this fundamental flaw in DNS, cache poisoning attacks still happen: in 2011, users of several Brazilian ISPs who tried to access Google, Youtube, and other websites were instead sent to malicious pages that directed them to install a Trojan on their computers.[20]

There are many scenarios in which internet users can be and are hurt by DNS hijacking:

- **Fraud**: DNS hijacking can cause users to load a malicious version of a financial institution's website and steal their money. DNS cache poisoning was used as one component of a Brazilian fraud ring discovered in 2014 that stole as much as $4 billion from consumers.[21]
- **Phishing and identity theft:** A user attempting to access a domain is directed by a compromised DNS record to a malicious page that steals their credentials. For example,

[20] https://securelist.com/blog/incidents/31628/massive-dns-poisoning-attacks-in-brazil-31/
[21] https://blogs.rsa.com/dns-poisoning-used-boleto-fraud/

on December 25, 2010, DNS in Tunisia redirected users to fake versions of major websites, including Facebook and GMail, that stole users' passwords when they tried to log in.[22]

- **Email interception**: By compromising a domain's *MX records*, an attacker can choose the IP address that emails for users at that domain will go to. In 2013, a hijack of MIT's DNS redirected emails to mit.edu domains to a server at the Korea Advanced Institute of Science and Technology.[23] The attacker could just have easily sent all MIT emails to a server he controlled. Because nearly every user ties all of their accounts on the internet, including online banking, to their email address, attackers could use this vector to steal billions of dollars.
- **Infecting users' computers:** A user sent to an attacker's server by a compromised DNS record could be tricked into downloading malicious software. One example of this was the 2011 attack in Brazil, mentioned above.
- **Website defacement and denial of service:** Activist hackers (sometimes called "hacktivists") may hijack the DNS records of domains in order to gain publicity or to retaliate against the website's operators. This makes the website inaccessible to users. In 2009, Twitter's DNS records were compromised and directed users to a webpage declaring that it had been hacked by the "Iranian Cyber Army."[24] Service was restored after a few hours.
- **Censorship:** A repressive government that controls a DNS resolver can return no result or a fake result for a website that it wants to block. The Chinese government

---

[22] http://costarica43.icann.org/meetings/sanjose2012/presentation-dns-hijackings-marquis-boire-12mar12-en.pdf

[23] http://tech.mit.edu/V132/N63/hack.html

[24] http://techcrunch.com/2009/12/17/twitter-reportedly-hacked-by-iranian-cyber-army/

manipulates DNS in this way to block a massive number of websites, from the New York Times to Facebook to domains that include the string “falungong.”[25]

DNS was initially designed in 1983 for an internet very different from the one that exists today. DNS is a notable work of computer systems engineering, and it is remarkable how it has been able to adapt and remain effective as the decades have gone by. However, without changes like DNSSEC to fix the authentication problem, DNS cannot be robust against today’s attacks--it can only mitigate the risk of them. Successful DNS attacks can cost consumers financially, violate their privacy, and break their trust in the reliability of the internet.

1.3 DNSSEC

DNSSEC, or the Domain Name Security Extensions, are modifications to DNS that are meant to make DNS results more verifiable. Under DNSSEC, each zone cryptographically signs its DNS records. Each zone’s keys are themselves signed by the parent zone. Finally, the root zone, which contains all domains on the internet, issues keys that are trusted by all DNSSEC-enabled resolvers. By verifying the chain of signatures from the root down to the returned address record, the resolver can confirm that the result actually comes from the correct zone operator. In the above example, the root zone would sign EDUCAUSE’s key (EDUCAUSE is the .edu TLD manager) and the referral to EDUCAUSE’s name servers, EDUCAUSE would sign MIT’s key and the referral to MIT’s name servers, and MIT would sign the address record of web.mit.edu.[26]

Properly implemented, DNSSEC would eliminate some DNS hijacking issues. Cryptographically signed records would prevent cache poisoning, because attackers would be

[25] https://www.usenix.org/system/files/conference/foci14/foci14-anonymous.pdf
[26]The reality is slightly more complicated in that zones have two pairs of keys that are used for different purposes, but the guarantees are the same.

unable to forge DNS records from authoritative name servers that have malicious answers. If the end user's stub resolver requested and verified the chain of signatures itself from the resolver it used, it would be able to confirm that its resolver isn't giving false results either. DNSSEC would not, however, eliminate the class of attacks in which a zone operator is hacked or tricked into signing the wrong record. In the 2013 redirection of MIT's internet traffic, the attacker logged into MIT's account at EDUCAUSE and changed the DNS record through EDUCAUSE's website.[27] This wouldn't have been prevented by DNSSEC: had MIT been implementing DNSSEC (it currently doesn't), the fake records would have been signed by EDUCAUSE. It is incumbent on domain registrars and website operators to follow other security best practices in order to avoid attacks like this.

Some opponents of DNSSEC argue that it is made unnecessary by other protocols for securing the internet, like HTTPS and HSTS. This is not true. While DNSSEC isn't enough on its own to protect users from attackers, it would provide benefits that other protocols do not. First, DNS cache poisoning attacks allow for denial of service and defacement that HTTPS and HSTS wouldn't protect against. Second, the Certificate Authority (CA) system upon which HTTPS is based has many points of failure--every single trusted CA, to be precise--and redundant safeguards will only make internet users more protected. Third, HSTS poses privacy risks[28] and does not normally protect a user's first connection to a website, while DNSSEC does. Finally, HTTPS is not always effective: DNS attacks (such as the 2011 Brazilian hack above) currently succeed in spite of HTTPS protection, which users sometimes ignore

DNSSEC is not without drawbacks. It allows for enumerating domains within a zone. While the current DNS system allows people to find domain names they already don't know about by guessing them one by one, DNSSEC would allow those domain names to be

[27] https://transition.fcc.gov/bureaus/pshs/advisory/csric3/CSRIC-III-WG5-Final-Report.pdf
[28] https://zyan.scripts.mit.edu/sniffly/

discovered much faster. Enumeration could allow malicious actors to find lots of new websites to target, many of which would not be secure against attack.

DNSSEC-signed zones allow for enumeration because they provide an *authenticated denial of existence*, or verification that a domain doesn't exist. An initial version of DNSSEC did so by providing signed *NSEC records* for each domain, which contained the next domain in the zone. For example, an NSEC record for "alfa.example.com" would be

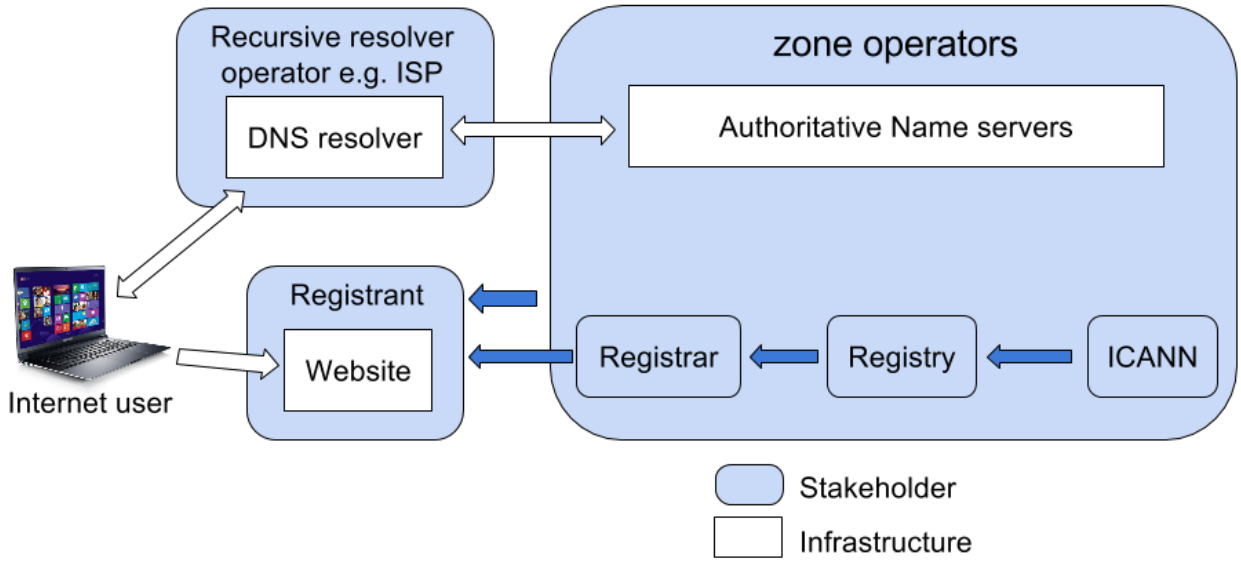
```
alfa.example.com. 86400 IN NSEC host.example.com. (A MX RRSIG NSEC TYPE1234)
```[29]

In particular, this record indicates that there are no domains between alfa.example.com and host.example.com. By returning this record in response to a query for beta.example.com, DNSSEC would allow the resolver to verify that beta.example.com does not exist. An attacker wishing to list all of the domains in a zone could have gone through all of these NSEC records in order.

However, there are mitigations that make DNS-signed zones less enumerable. In response to the issues with NSEC, IETF developed an alternative record type, NSEC3, designed to mitigate the possibility of zone enumeration.[30] In 2014, researchers found that they were able find 64% of all DNSSEC-signed .com domains with just a few days of computing, indicating that the NSEC3 mitigations are not always effective.[31] However, the enumerability of a domain is related to how "guessable" it is as a string, which means that domains that are enumerable could have been identified anyway. Additionally, there exist other mitigations, such as "DNSSEC white lies," for avoiding enumeration attacks.[32]

[29]IETF, "RFC 4034," https://www.ietf.org/rfc/rfc4034.txt.
[30] IETF, "RFC 5155," https://tools.ietf.org/html/rfc5155.
[31] Wander et al., "GPU-Based NSEC3 Hash Breaking."
[32] https://blog.cloudflare.com/dnssec-complexities-and-considerations/

2 STAKEHOLDERS



Full implementation of DNSSEC requires the active involvement of the following key stakeholders: The Internet Corporation for Assigned Names and Numbers (ICANN), domain name registries, domain name registrars, DNS zone operators, recursive resolver operators (typically ISPs and public DNS resolvers), and domain name registrants (i.e. website administrators). These key stakeholders all have different incentives, implementation costs and potential benefits from DNSSEC implementation. More importantly, there exists a collective action problem which is slowing down the rate of DNS adoption because although these stakeholders all need to take action, the recursive resolver operators (a service mostly provided by ISPs to home Internet users) have the least incentive to play their part, hence the need for regulatory action.

Before delving deeper into each of these key stakeholders and the need for regulatory action to motivate the operators of recursive resolvers, it is worth mentioning that web browser

developers were deliberately excluded from this list of key stakeholders because they do not play an active role in DNSSEC deployment. Although web browser manufacturers could decide to implement DNSSEC validation in their browsers, this would simply serve as a notification to end users because most users do not perform recursive DNS lookups on their computers. Most internet users tend to rely on their ISPs for recursive DNS lookups [33] while a small fraction of users rely on public DNS services such as Google Public DNS[34] or OpenDNS[35].

2.1 ICANN

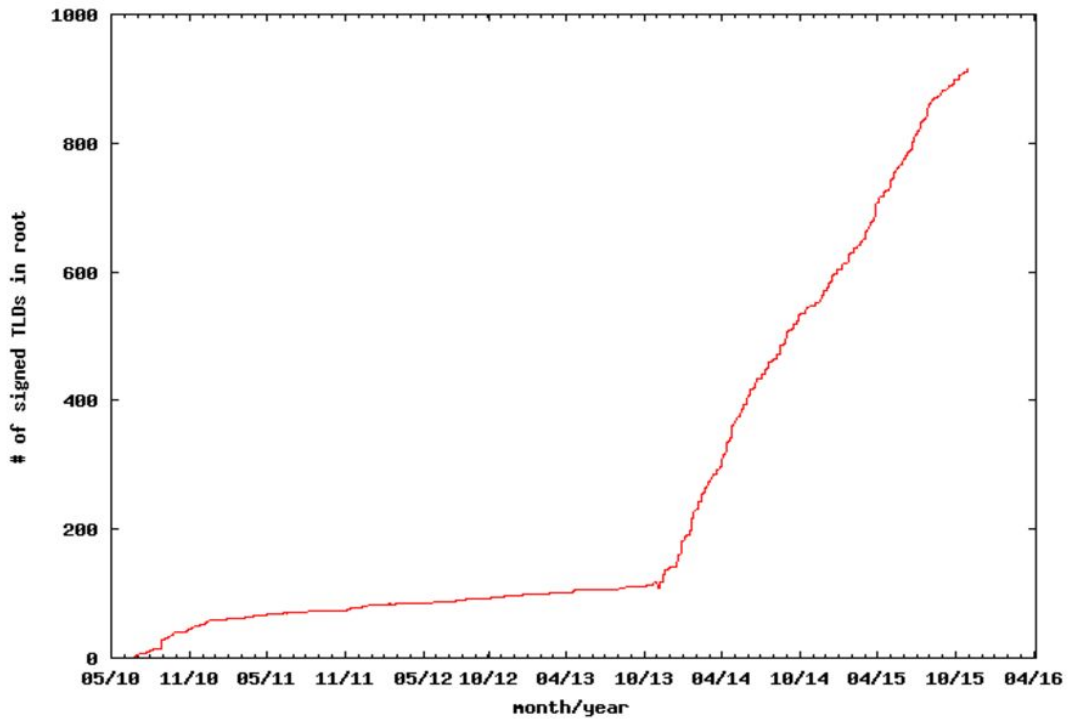
ICANN is an advocate of DNSSEC and they view it as a technology that complements some other current technologies such as SSL in order to prevent DNS attacks[36]. ICANN completed deployment of DNSSEC in the root zone in July 2010[37]. DNSSEC for the root zone was a joint effort between ICANN and VeriSign, with support from the U.S. Department of Commerce. This paved the way for the TLD registries and other stakeholders to implement DNSSEC.

2.2 Domain name registries

The top level domain registries play a pivotal role because these TLDs must be signed in order to achieve full DNSSEC deployment. There would be no benefit in deploying DNSSEC in the second-level domains and other lower levels of the domain name system unless the TLDs have already implemented DNSSEC. As indicated in the following graph, there has been rapid DNSSEC deployment in the TLDs in recent years. About 84% of the 1,106 TLDs have fully deployed DNSSEC.[38]

---

[33] https://labs.apnic.net/?p=555
[34] https://developers.google.com/speed/public-dns/docs/using
[35] https://www.opendns.com/
[36] https://www.icann.org/resources/pages/dnssec-qaa-2014-01-29-en
[37] http://www.root-dnssec.org/index.html
[38] TLD DNSSEC Report, 2015-11-16 - http://stats.research.icann.org/dns/tld_report/



DNSSEC adoption in the TLDs
Source: http://stats.research.icann.org/dns/tld_report/

One of the reasons for rapid adoption by the registries is that they need to protect their reputation and assure the internet community that their zone is properly protected. These registries consist of government departments and reputable organizations (e.g. Verisign) that feel they have a responsibility to lead by example when it comes to internet infrastructure security. In addition, most registries are non-profit organizations, so commercial targets and profitability are not so important to them[39].

2.3 Domain name registrars

Domain name registrars are organizations accredited by generic top-level domain (gTLD) registries or country code top-level domain (ccTLD) registries to manage the reservation of internet domain names. With DNSSEC, the domain name registrars play a critical role in

[39] Security Tools and Architectures Section of ENISA, and Deloitte Enterprise Risk Services. 2009. Study on the Costs of DNSSEC Deployment. https://www.enisa.europa.eu/publications/archive/dnsseccosts

linking signed domains to the higher level domains in order to form a "chain of trust"[40]. The top domain name registrars such as GoDaddy[41], eNom[42] and Tucows[43] have all implemented DNSSEC. Besides, most of the other top domain name registrars have either implemented DNSSEC or provided information on how their clients can add DNSSEC for their domain through third-party DNS providers.

Registrars have various incentives to implement DNSSEC because it can serve as a differentiator and competitive advantage. ICANN currently maintains a list of domain name registrars that have implemented DNSSEC[44]. Besides, DNSSEC implementation projects at registrars tend to be less costly and less time consuming than similar projects at registries or zone operators because the registries often guide registrars in their implementation. Some of the registrars also charge an additional fee (e.g. 2 €/ domain / year) to their customers (i.e. domain name registrants), so they have a means of recovering their financial expenses[45].

2.4 DNS Zone operators

Zone operators are incentivized to implement DNSSEC by both the registries that want to promote DNSSEC adoption and the registrants (i.e. domain name owners) that want to use DNSSEC. As a result, DNSSEC deployment can serve as a differentiator and competitive advantage for zone operators. Research conducted by the European Network and Information Security Agency (ENISA) shows that zone operators often charge registrants an average of 2 € per year per domain for DNSSEC. Although it is not clear whether this fee is enough to cover

[40] How To Secure And Sign Your Domain With DNSSEC Using Domain Registrars http://www.internetsociety.org/deploy360/resources/dnssec-registrars/
[41] https://uk.godaddy.com/help/dnssec-faq-6135
[42] http://www.enom.com/tlds/dot-pw.aspx
[43] https://opensrs.com/blog/2015/05/dnssec/
[44] https://www.icann.org/resources/pages/deployment-2012-02-25-en
[45] Security Tools and Architectures Section of ENISA, and Deloitte Enterprise Risk Services. 2009. Study on the Costs of DNSSEC Deployment. https://www.enisa.europa.eu/publications/archive/dnsseccosts

the cost of DNSSEC implementation, the research observed that the implementation cost gets significantly reduced over time due to the reliance on open source software that results in lower software development expenses. In addition, the big zone operators also offer registrar services, so they are able to transfer some of the implementation cost to their customers by charging registrants (i.e. domain owners) for signing their domains. This then makes it possible to spread the investment cost and increase total revenue obtained from the domain owners within each zone.[46] With such financial incentives, the zone operators would most likely support any regulatory effort that encourages greater adoption of DNSSEC by registrants.

2.5 Recursive Resolver Operators

Recursive lookup of DNS queries is a service that is provided by ISPs and public DNS resolvers such as Google Public DNS and OpenDNS. These DNS resolvers are the middlemen between a user's web browser and website content.

A 2015 study conducted in Europe indicated that over 90% of the observed internet users were using either Google open DNS or their ISP's local DNS resolvers. Of those 90%, between 72% and 93% used their local ISP's DNS resolvers on the days the tests were performed[47]. A different study performed by APNIC in 2014 also showed that most Internet users relied on their ISPs for DNS lookups. APNIC's study revealed that only 0.7% (1,889) of DNS resolver systems handled the query load for 90% of Internet users around the world. Furthermore, the 10 largest DNS visible resolver systems actually accounted for the DNS queries of about 30% of the Internet's user population. 8 out of these top 10 DNS resolver systems were ISP-provided resolvers (with Google Public DNS and ChinaNet being the other

[46] Security Tools and Architectures Section of ENISA, and Deloitte Enterprise Risk Services. 2009. Study on the Costs of DNSSEC Deployment. https://www.enisa.europa.eu/publications/archive/dnsseccosts
[47] Hadrien, H., Ernst, B., Patrick, L., Alessandro, F., & Marco, M. (2015). A Study of the Impact of DNS Resolvers on Performance Using a Casual Approach.

top two). The population of clients served by the ISP-provided resolvers largely matched the estimates of the size of the ISPs' client base,[48] thereby indicating that most Internet users rely on the default DNS servers of their ISPs for DNS lookups.This implies that the roles of ISPs cannot be ignored if we hope to ensure that most home and small office internet users are performing secure DNS lookups. Since some of the biggest DNS resolvers used by Americans (Google Public DNS and ComCast) have already implemented DNSSEC, we believe that DNSSEC implementation by ISPs is feasible, in spite of it being the last major hurdle that needs to be overcome in order to secure the DNS traffic of most Internet users in the US.

The business motivation for recursive resolver operators to implement DNSSEC is the increased security of DNS queries by their name servers. Although Google public DNS and Comcast have already implemented DNSSEC, interviews conducted by ENISA[49] revealed that recursive resolver operators are generally reluctant to implement DNSSEC because they claim that the financial benefits do not outweigh the implementation cost.[50]

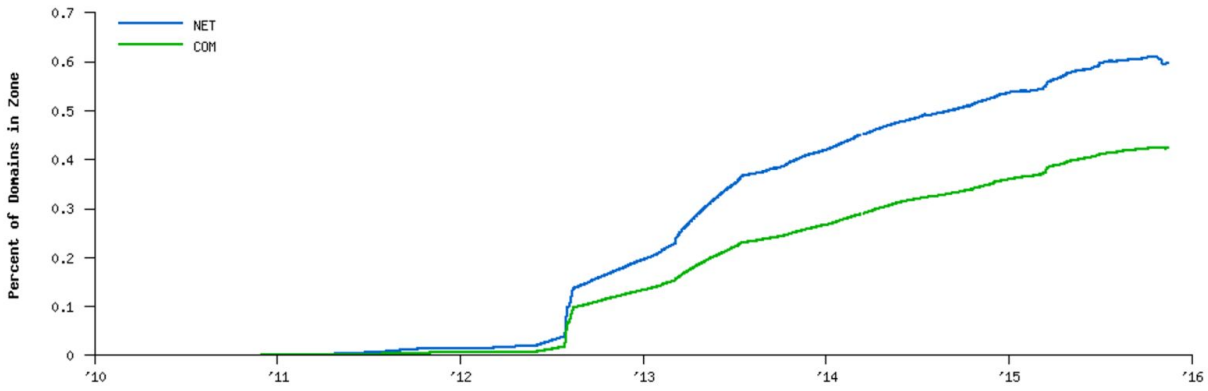
ISPs may not gain significant competitive advantage from implementing DNSSEC because the average home Internet user will not be able to recognize or appreciate the additional security that DNSSEC provides. The reason is because unlike HTTPS, web browsers currently do not distinguish between signed and unsigned domain names, so the end users have no obvious means of distinguishing between secure and insecure DNS lookups. If customers cannot appreciate the additional benefit obtained from DNSSEC, it would be difficult for ISPs to transfer the implementation cost to the end users, hence the economic disincentive for ISPs to invest in DNSSEC implementation. For these reasons, we believe that regulatory

[48] https://labs.apnic.net/?p=555
[49] Security Tools and Architectures Section of ENISA, and Deloitte Enterprise Risk Services. 2009. Study on the Costs of DNSSEC Deployment. https://www.enisa.europa.eu/publications/archive/dnsseccosts
[50] Security Tools and Architectures Section of ENISA, and Deloitte Enterprise Risk Services. 2009. Study on the Costs of DNSSEC Deployment. https://www.enisa.europa.eu/publications/archive/dnsseccosts

action (or the threat of regulation) by the FCC would accelerate DNS implementation by requiring all ISPs to implement DNSSEC. Pressure or regulatory requirements for all ISPs to implement DNSSEC would ensure a level playing field since they will all be bearing similar implementation costs.

2.5 Domain name registrants

The domain name registrants are the website administrators and businesses that need a secure environment for online business transactions. This class of stakeholders is well incentivized to adopt DNSSEC because of the need to protect their business reputation and they can often find ways to transfer the cost to their customers. Domain name registrants typically rely on their registrars to enable DNSSEC on their domains so they do not need to be tech savvy. Some of the top domain name registrars such as GoDaddy[51] provide detailed information to facilitate DNSSEC adoption by their clients. So far, DNSSEC adoption by domain name owners has been slow. The figure below (obtained from Verisign) shows that less than 1% of .com and .net domains are currently secured with DNSSEC.



Percentage of .com and .net domains secured with DNSSEC
Source: Verisign Labs (http://scoreboard.verisignlabs.com/percent-trace.png)

[51] https://uk.godaddy.com/help/dnssec-faq-6135

In order to sign a domain with DNSSEC, the top-level domain must be signed, the domain registrar must support DNSSEC, and the DNS hosting provider must also support DNSSEC[52]. Even if all this is achieved, the ISPs and public DNS resolvers must also support DNSSEC in order for clients to reap the benefit of improved internet security. We believe that over time, DNSSEC adoption by domain name registrants would improve when more domain name registrars simplify the process involved in enabling DNSSEC on a domain. Besides, we believe the business and reputation risks to businesses will be enough motivation to get domain name owners to sign their domains once DNSSEC has been adopted by the other key stakeholders. This is a situation that could be monitored over time to see whether there is a need to develop stronger incentives for website administrators of certain types of firms e.g. financial services firms or medical institutions.

The following table contains a provides of the incentives and DNSSEC deployment status of the key stakeholders.

Stakeholder	**Incentives and deployment status**
ICANN	● Strong advocate for DNSSEC and plays a leading role in encouraging other stakeholders to adopt DNSSEC. ● DNSSEC has been fully deployed in the root zone.
Domain name registries	● Need to protect their reputation and assure the internet community that their zone is properly protected. ● Non-profit organizations, so commercial targets and profitability are not so important to them. ● Most registries have deployed DNSSEC.

[52] http://www.internetsociety.org/deploy360/resources/dnssec-registrars/

Domain name registrars	● DNSSEC implementation can serve as a differentiator and competitive advantage. ● ICANN currently maintains a public list of domain name registrars that have implemented DNSSEC. ● DNSSEC implementation projects at registrars tend to be less costly and less time consuming than similar projects at registries or zone operators because the registries often guide registrars in their implementation. ● Can charge an additional fee to their customers. ● Most top registrars have deployed DNSSEC.
DNS zone operators	● DNSSEC deployment can serve as a differentiator and competitive advantage. ● Big zone operators also offer registrar services, so they are able to transfer some of the implementation cost to their customers by charging registrants (i.e. domain owners) for signing their domains. ● DNS zones are often operated by registrars and registries, which are well incentivized as explained above, hence there is no need for regulatory action.
Recursive resolver operators (mostly ISPs and public DNS resolvers)	● May not gain significant competitive advantage from implementing DNSSEC because the average home Internet

	user will not be able to recognize or appreciate the additional security that DNSSEC provides. ● Most home internet users rely on their ISP's domain name servers for DNS lookups, hence ISPs are key stakeholders that should implement DNSSEC.
Registrants (i.e. website operators)	● They need to protect their business reputation and they can often find other ways to transfer the cost to their customers. ● Rely on their registrars for implementation, so they do not need to be tech savvy. ● May not be aware of DNSSEC, hence they may not request it from their registrars. ● Although most second-level domains have not deployed DNSSEC, registrars have a financial incentive to advertise it to registrants.

3 FCC JURISDICTION

We believe the FCC is well-placed to positively impact Internet infrastructure security by pressuring ISPs to adopt Best Current Practices and standards developed through CSRIC Working Groups. Below we develop an argument for the adoption of DNSSEC, as

recommended by WG5[53], and also note that other working groups lay the groundwork for the adoption of other Internet protocol improvements, such as BGPsec, or other best practices, such as the 20 Critical Security Controls[54]. While it is uncertain whether or not the FCC can mandate that ISPs adopt DNSSEC, there are no acts of Congress we are aware of that prohibit them from making such rules, and ISPs appear willing to adopt similar rules and codes of conduct voluntarily. We aim to show that ISPs cannot know whether they would prevail in court or not, and that they may, consequently, favor adopting voluntary measures over costly litigation.

We begin with an overview of the creation of the FCC and CSRIC, then describe the current status of the FCC bully pulpit through two examples of non-legislative policy statements which we have based our proposal on: the Anti-Botnet Code of Conduct and the Internet Policy Statement. ISPs have voluntarily signed on to the Anti-Botnet Code of Conduct, and have agreed to abide by the principles of the Internet Policy Statement as part of merger agreements overseen by the FCC. Lastly we discuss some of the legal interpretations of previous court decisions, in anticipation of possible ISP resistance to our DNSSEC proposal,.

3.1 The FCC and CSRIC

The FCC, which Congress established under the Communications Act of 1934, regulates interstate and international communications by radio, television, wire, satellite and cable in the United States, leveraging its competencies in, among other things, “Providing leadership in strengthening the defense of the nation's communications infrastructure”[55]. Later, the Telecommunications Act of 1996 attempted to restructure the rapidly changing

[53] “Final Report on Measurement of DNSSEC Deployment” Federal Communications Commission, CSRIC III Working Group 5, Feb. 22, 2013.
[54] CSRIC III Working Groups 4 and 11, respectively.
[55] What We Do. (n.d.). Retrieved from https://www.fcc.gov/what-we-do

telecommunications market to improve competition[56]. The purpose of the FCC, per 47 U.S. Code § 151, is to make available "rapid, efficient, Nation-wide, and world-wide wire and radio communication service with adequate facilities at reasonable charges, for the purpose of the national defense, for the purpose of promoting safety of life and property through the use of wire and radio communications". Internet security improvements like DNSSEC offer an opportunity to further the purpose of the FCC by improving national defense[57], and safety of property by preventing DNS spoofing attacks.

Further, the FCC is directed in 47 U.S.C. § 254 (b) to "base policies for the preservation and advancement of universal service on the following principles: (1) …Quality services should be available." and, "(2)...Access to advanced telecommunications and information services should be provided in all regions of the Nation."[58] While quality is often considered synonymous with availability of network service, it seems reasonable to include integrity and security in the definition. For example, the International Telecommunication Union - Telecommunication Standarization Sector (ITU-T) defined both integrity and security as primary components of quality of service[59], and the Internet Engineering Task Force (IETF) considers security a standard requirement for Quality of Service[60].

In keeping with the Federal Advanced Committee Act (FACA)[61] passed in 1972, the FCC establishes advisory committees to research specific areas and provide recommendations to the FCC. One such committee, CSRIC's mission is "to provide recommendations to the FCC to

[56] Telecommunications Act of 1996. (n.d.). Retrieved from https://transition.fcc.gov/telecom.html
[57] CSD-DNSSEC. (n.d.). Retrieved from http://www.dhs.gov/csd-dnssec
[58] Telecommunications Act of 1996, Title 47, Chapter 5 § 254 (b) (1) and (2)
[59] See Figure 1/E.800 of *Terms and Definitions Related To Quality of Service and Network Performance Including Dependability*. (1994). (No. E.800). ITU-T. Retrieved from http://www.itu.int/rec/T-REC-E.800/en
[60] Chaskar, H. (2003, September). Requirements of a Quality of Service (QoS) Solution for Mobile IP. Nokia Research Center. Retrieved from https://tools.ietf.org/html/rfc3583
[61] Federal Advisory Committee Act, Pub.L. 92–463 (1972). Retrieved from https://www.epic.org/open_gov/faca.html

ensure, among other things, optimal security and reliability of communications systems"[62]. CSRICs, like all advisory committees, may be further split into Working Groups, which each focus on specific topics, such as best practices for Internet protocols, security extensions for Internet protocols, or botnet remediation. These working groups, in turn, seek input from government agencies and private industry, often drawing heavily from ISPs, to ensure they include key stakeholders and experts, and report their findings back to the FCC.

CSRIC III Working Group 5, as an example, was chaired by Steve Crocker[63], the chair of the board at the Internet Corporation for Assigned Names and Numbers (ICANN), with representatives from other technology companies like Google, ISPs like AT&T, Cox, Sprint, and Verizon, root nameserver operators like Verisign, and government agencies like NIST. Having employees of ISPs participate in Working Group 5 lends credence and a sense of fairness to the group's findings: when it recommends that ISPs should immediately make their DNS recursive nameservers DNSSEC-aware, if not full validators, this carries weight because the ISPs had input in the process. After CSRIC released recommendations in 2012, several large ISPs agreed to adopt DNSSEC to some degree. They also signed the Anti-Bot Code of Conduct, which requires substantive action towards mitigating botnets and information sharing with other participants[64]. These adoptions were voluntary, a strong sign that ISPs are willing to work with the FCC.

---

[62] The Communications Security, Reliability and Interoperability Council. (n.d.). Retrieved from https://transition.fcc.gov/pshs/advisory/csric/

[63] See Stephen Crocker's Wikipedia entry for general background information: https://en.wikipedia.org/wiki/Steve_Crocker

[64] Paragraph 3 of Rashid, F. Y. (2012, March 22). ISPs Agree to FCC Rules on Anti-Botnet, DNSSEC, Internet Routing. Retrieved from http://securitywatch.pcmag.com/security/295722-isps-agree-to-fcc-rules-on-anti-botnet-dnssec-internet-routing

3.2 Non-legislative Policy Statements

The Anti-Botnet Code and the Internet Policy Statement of 2005 provide two examples of the bully pulpit approach we recommend. In both examples, the FCC releases a statement and ISPs publicly agree to adhere to the principles in this statement, without the FCC enacting legislation. The Anti-Botnet Code came out of the final report of Working Group 7 for CSRIC III. Published March 22, 2012, this Code outlined objectives and developed a voluntary code of conduct for ISPs to participate in. Participants in the Code agreed to take meaningful action in educating end-users about botnets, detecting botnets on their networks, notifying customers of suspected infections, assist end-users in remediation of infections, and collaborating with other ISPs in all of the above. Several ISPs immediately agreed to participate, including AT&T, CenturyLink, Comcast, Cox Communications, and Time Warner Cable[65]. The Code, similar to our proposal, draws steps for action from a multi-stakeholder Working Group. Working Group 7, which drafted the Code, had members representing all five initial participants. It also discussed some of the barriers to combating botnets, similar to how we consider barriers to implementation of DNSSEC.

Another example of FCC persuasion is the Internet Policy Statement of 2005. In this statement, the FCC adopts four principles for encouraging broadband deployment and protecting what it considers key features of the Internet. Specifically, it states that consumers are entitled to access lawful content, run applications of their choice, connect their choice of devices, and to competition among network providers. These four principles form the basis of future FCC policymaking, but by themselves do not constitute any rulemaking. Our proposal calls for more specific measures than the Internet Policy Statement, but we recommend that the FCC exert pressure on ISPs to adopt our proposal similarly, namely by leveraging situations in

[65] ABCs for ISPs. (n.d.). Retrieved from https://www.m3aawg.org/abcs-for-ISP-code

which ISPs required FCC approval, such as during mergers. “Before a company may assign an FCC license to another company or acquire a company holding an FCC license, it must receive the Commission’s approval”[66], so when an ISP wants to merge with or acquire another FCC license-holding company, as during the SBC/AT&T merger or the Verizon/MCI merger[67], they are, to a certain extent, at the FCC’s mercy.

We recommend that the FCC use the CSRIC Working Group on DNSSEC’s findings as a template for a policy statement, as we do below in the Appendix. This statement would set up clear goals for ISPs to meet regarding DNSSEC adoption. After publishing this statement, the FCC can leverage its authority to regulate ISPs to find situations where they can request that ISPs adopt some or part of the proposal. Further, once adoption of this proposal gains steam, it joins a body of policy statements, like the Anti-Botnet Code, which exert authority over ISPs. Future CSRIC Working Groups will provide the material for more policy statements which the FCC will promote via its growing bully pulpit, driving a cycle of ever-improving Internet security.

3.3 Court Cases and FCC Regulations

Should the FCC try, even through non-legislative means, to force ISP action, there is a chance that ISPs will fight back. The FCC’s legal authority to regulate ISPs has been challenged on multiple fronts, most recently from ISPs regarding their reclassification as common carriers. As a check to FCC authority, the Administrative Procedure Act (APA) sets standards for judicial review of agency actions. Acceptable challenges include that a rule was enacted contrary to the Constitution or a statute or that it is arbitrary and capricious.[68]

---

[66] Mergers and Acquisitions. (n.d.). Retrieved from https://www.fcc.gov/mergers
[67] See FCC APPROVES SBC/AT&T AND VERIZON/MCI MERGERS. (2005, October 31) and FCC APPROVES MERGER OF AT&T INC. AND BELLSOUTH CORPORATION. (2006, December 29).
[68] See Q.13 at https://www.fcc.gov/encyclopedia/rulemaking-process-fcc. and 5 U.S.C. Section 706 - Scope of Review

If asserting that the FCC acted contrary to the Constitution or a statute, petitioners must overcome a level of deference to agency authority set in Chevron v. NRDC[69]. This test asks two questions: first, whether Congress has directly addressed the matter on agency authority over this space. Barring this immediate disqualification, the Chevron decision "requires a federal court to defer to an agency's construction, even if it differs from what the court believes to be the best interpretation, if the particular statute is within the agency's jurisdiction to administer, the statute is ambiguous on the point at issue, and the agency's construction is reasonable". The court should then, under Chevron, only decide whether the agency's interpretation is "arbitrary, capricious, or manifestly contrary to the statute", rather than substituting their own judgement. For example, in Direct Communications Cedar Valley[70], the court applied both the Chevron standard and the "arbitrary and capricious" standard[71] to revisions the FCC made to how universal service funds were to be allocated and used by ISPs.

We also find the Chevron test used in Verizon v. FCC. The FCC launched a public request for input about what needed to be done to ensure the Internet remained, "an open platform for innovation, investment, job creation, economic growth, competition, and free expression"[72], and in response to a year's worth of comments from over 100,000 commenters from industry, academia, and consumer advocacy groups, the FCC released their Open Internet Order in December 2010[73]. In particular, the Order calls to attention the importance of a robust, well-functioning Internet[74], and the need for descriptions of congestion management and security practices derived from the transparency rule[75], grounding the FCC's authority to adopt

[69] Chevron U.S.A., Inc. v. Natural Resources Defense Council, Inc.
[70] Direct Communications Cedar Valley LLC v. FCC, No. 11-9900 (US 10th Circuit Court of Appeals May 23, 2014). Retrieved from https://apps.fcc.gov/edocs_public/attachmatch/DOC-327257A1.pdf
[71] The court also considered the matter *de novo*.
[72] Para. 2 of the Open Internet Order, released Dec. 23, 2010
[73] Para. 2 of the Open Internet Order, released Dec. 23, 2010
[74] Para. 6 of the Open Internet Order, 2010.
[75] Para. 56 of the Open Internet Order, 2010.

these rules in 47 USC § 1302. Internet Service Providers disagreed with the FCC's findings, and filed suit against them. In Verizon, the US Court of Appeals for the DC Circuit vacated the "No Blocking" and "No Unreasonable Discrimination" rules, holding that since the FCC had not classified ISPs as common carriers, it could not regulate them under its Title II authority. However, the transparency rule, which requires disclosure of security practices used to protect both the end user and the network itself, was upheld. This suggests the FCC can require that ISPs provide details about their DNSSEC adoption, and may advertise to consumer if any ISPs refuse to implement DNSSEC.

ISPs have also taken issue with how they are classified by the FCC. After the Verizon case the FCC sought comment on its authority under Section 706 and Title II in a Notice of Proposed Rulemaking[76], specifically questioning whether the FCC should reclassify ISPs as common carrier services, and what constituted an "advanced telecommunications capability". A year later, the FCC released a Report and Order, which reiterated and strengthened their transparency rule, and, in response to comments, invoked multiple sources of authority for future rules: including Section 706 of the Telecommunications Act, and Title II and Title III of the Communications Act[77]. The FCC took pains to adopt clear, bright-line rules: no blocking, no throttling, and no paid prioritization, and, in asserting its Title II authority, also endeavored to establish "light-touch" Title II regulation by exercising broad forbearance from 30 statutory provisions under Title II. ISPs took issue with this and filed suit again, consolidating cases and filing for a motion of partial stay of the FCC's broadband reclassification, which the DC Circuit Court of Appeals denied[78]. The trial is scheduled for December 4, 2015[79].

---

[76] *Notice of Proposed Rulemaking* (GN Docket No. 14-28 No. FCC 14-61) May 15, 2014.
[77] Para. 274 and Footnotes 701, 702 of the Report and Order, 2015, detailing comments by the CFA and AOL about the complementary nature of Section 706 and Title II.
[78] Court history of US Telecom Assn v. FCC available at https://www.fcc.gov/encyclopedia/major-court-cases-fcc#15-1063

Courts have held against some FCC assertions of authority, as when in Comcast Corp v. FCC[80] the court held that the FCC did not have ancillary authority to bar Comcast from interfering with peer-to-peer traffic on its network under 47 U.S.C. § 154(i). However, as mentioned above, the transparency rule, and with it security and network management practices, was upheld in the Verizon case by merit of the FCC's Section 706 authority.

Unless the courts overturn the FCC's assertion of Title II authority, additional legal precedents involving the duties of common carriers are also relevant, such as the holding in Rotheli v. Chicago Transit Authorities that "carrier owes a duty to exercise the highest degree of care consistent with the practical operation of its conveyances to protect the safety of the passenger and such duty is continuous throughout this relationship and extends to passengers who are given a transfer"[81]. Later, Tortes v. King County[82] held that, "a common carrier is not required to take measures to protect its passengers from the unforeseen intentional misconduct or criminal acts of third persons", suggesting that carriers may have to protect against the easily foreseeable criminal acts that DNSSEC prevents.

Regardless of future precedent regarding the classification of ISPs as common carriers, however, we believe the FCC possesses enough authority to make ISPs think twice about litigation. The Chevron test, in particular, although it has been used against the FCC, should show deference when it comes to any proposals that aim to improve the quality of Internet

[79] 15-1063 United States Telecom Assoc. v. FCC, to be heard by Judges Tatel, Srinivasan, Williams.
[80] *Comcast Corporation v. FCC*. 2010. (US Court of Appeals for the District of Columbia Circuit).
[81] Rotheli v. Chicago Transit Authority, No. No. 33606 (Supreme Court of Illinois November 23, 1955). Retrieved from https://scholar.google.com/scholar_case?case=7360554567166694650&hl=en&as_sdt=6&as_vis=1&oi=scholarr
[82] Tortes v. King County, No. No. 49576-3-I (Court of Appeals of Washington, Division 1 June 2, 2003).

services, since the FCC was established for the purpose of promoting quality communications services.

4 PROPOSAL

We now outline our recommendations to the FCC and provide a general proposal on DNSSEC, available in the Appendix. The FCC should draw from the body of work of its various councils and committees, because these groups tend to include experts from a cross section of stakeholders. The FCC should issue a broad statement, similar to the adoption of CSRIC recommendations for combatting major cybersecurity threats[83], which included the Anti-Bot Code[84], or the Internet Policy Statement of 2005, which the FCC has held ISPs to in recent merger agreements[85]. The FCC can applaud ISPs that have adopted the recommendation of at least making nameservers DNSSEC-aware, even pointing to ISP's which have already made their nameservers full DNSSEC validators. The FCC can leverage situations in which ISPs require its approval to pressure ISPs to agree to adopt our proposal, similarly to how the Internet Policy Statement was included in merger agreements approved by the FCC.

The statement should:

- frame the situation by identifying key stakeholders and potential harm to consumers,
- propose a solution which ISPs may adopt,
- provide a system for measuring compliance with their solution,

[83] CSRIC Adopts Recs. to Minimize Three Major Cyber Threats. (2012, March 22). Retrieved from https://www.fcc.gov/document/csric-adopts-recs-minimize-three-major-cyber-threats

[84] Rashid, F. Y. (2012, March 22). ISPs Agree to FCC Rules on Anti-Botnet, DNSSEC, Internet Routing. Retrieved from http://securitywatch.pcmag.com/security/295722-isps-agree-to-fcc-rules-on-anti-botnet-dnssec-internet-routing

[85] See FCC APPROVES SBC/AT&T AND VERIZON/MCI MERGERS. (2005, October 31) and FCC APPROVES MERGER OF AT&T INC. AND BELLSOUTH CORPORATION. (2006, December 29).

- issue a timeline for compliance,
- request comments from all interested parties, and
- provide examples of previous successes.

We do not suggest to attempt binding legislation, such as an Notice of Proposed Rulemaking (NPRM) or Report and Order (R&O), but instead recommend the FCC make use of non-legislative policy statements and signal their intention to enact future regulations if the desired results are not achieved[86]. This puts pressure on ISPs without binding the FCC to the release and comment cycle required by the APA. This broad statement should include a voluntary pledge for ISPs to sign, similar to the Anti-Bot Code. ISPs should pledge that they:

1. Consider network security and reliability to be top priorities
2. Consider DNSSEC an integral part of network security and reliability, and will make substantive progress towards full adoption

To make substantive progress, Working Group 5 recommends that ISPs at least upgrade their DNS recursive nameservers to be DNSSEC aware, and we think this is a fine start. But a more comprehensive plan from the FCC should see this only as a first step. The FCC should further pressure ISPs to make their nameservers validate DNSSEC requests, sign the DNS records for the zones they are authoritative for, and assist customers wherever possible. It is also important to strike a balance between requesting specifics so that it is easier to verify whether or not ISPs are complying, and keeping the process open enough to allow room for new and innovative solutions.

In order to facilitate this process, the FCC should advise future working groups to contract specialists to develop tools for testing compliance, make them widely available and

[86] Rulemaking Process at the FCC. (n.d.). Retrieved from https://www.fcc.gov/encyclopedia/rulemaking-process-fcc

easy to use, and plainly state that these tools will be used to measure compliance on an ongoing basis. As an example, Working Group 5 contracted work from Shinkuro and SamKnows to develop a tool, DNSSEC Resolver Check. DNSSEC Resolver Check is available online[87], and while Shinkuro. Inc owns the copyright to the software. It is licensed under a permissive license, merely requesting that the LICENSE file is always distributed with the software. The FCC should not only make this tool available, but also use the tool at regular intervals, on either a random subset of, or, preferably, all Internet Service Providers' networks. Further, they should publish the results of their tool to the public on an ongoing basis, so that consumers can see when and how ISPs are dragging their feet. In order to promote dialogue, if ISPs think the tool is unreasonable, they should be able to suggest a different tool, or recommend changes to the existing tool, which the FCC can choose to incorporate.

The FCC should also issue a timeline for compliance, taking into consideration how complicated the proposed changes are, and what headstart ISPs have already. ISPs that have already fully or partially implemented DNSSEC serve the dual purpose of advocates for DNSSEC adoption and measuring sticks for time involved, costs associated, expertise required, and obstacles encountered. To start, we recommend the FCC give ISPs one month to analyze their networks and decide for themselves what they can do and how long it will take, since "Legislative rules generally become effective at least 30 days after they are published in the *Federal Register*"[88]. This encourages a two-way relationship between ISPs and the FCC. After ISP's provide a general statement of intent, the FCC will review their progress on an ongoing basis, holding their pledge to implement DNSSEC over their heads if necessary.

[87] Public code repository is hosted at: https://github.com/ogud/DNSSEC-resolver-check
[88] See Q6, Effective Date of Rulemaking Process at the FCC. (n.d.). Retrieved from https://www.fcc.gov/encyclopedia/rulemaking-process-fcc

The FCC should provide a mechanism where comments may be submitted and reviewed. In the past, the FCC has made these comments available in an easily machine-parsable XML format[89], and Working Group 5 went so far as to make its tool's code available on Github. The FCC could then address specific comments and adapt its strategy over time, which could in turn be commented upon, creating a continuing multi-stakeholder dialogue.

Lastly, the FCC should provide concrete examples of past successes, where applicable, and the current state of adoption over time. Here again we may draw from Working Group 5's final report, which collected data using the DNSSEC Resolver Check tool, finding just over 10% of ISPs nameservers to be proper DNSSEC validators, with over ⅓ of nameservers being DNSSEC aware[90]. Working Group 4's final report on BGPsec, in contrast, delivers an excellent overview of the situation and cites resources to consult for specific remedies, but conducts no experiments itself and releases no tools which could be used to establish an objective standard of measurement for ISP's progress. In addition, the FCC should encourage ISPs that have already adopted DNSSEC to vocally advertise their implementation and provide details about the process, stopping short of providing specific advantages to competitors. Google's public advocacy for DNSSEC is one example[91].

5 CONCLUSION

This paper recommends that the FCC take advantage of its authority to advocate for improved Internet security, starting with DNSSEC, because it addresses specific technological deficiencies in the Domain Name System that result in harm to consumers. DNSSEC is also

[89] Comments are available at https://www.fcc.gov/files/ecfs/14-28/14-28-RAW-Solr.zip. The XML file accessed on 15 November 2015 contains nearly 4 million submissions, with a compressed size of 168MB
[90] See Figure 2 of Working Group 5's Final Report on Measurement of DNSSEC Deployment
[91] See https://developers.google.com/speed/public-dns/docs/security?hl=en

partially adopted already, making the transition easier as software and procedures have previously been developed and powerful stakeholders have sunk costs.

We addressed the technical, stakeholder market, and legal issues in turn, and then drafted a proposal for the FCC to follow which draws on CSRIC Working Group findings, similarly to the Anti-Botnet Code. DNSSEC represents an incremental increase in Internet infrastructure security. By cryptographically signing query results, these security extensions allow DNSSEC-validating nameservers to verify whether a DNS record is genuine or not. This closes out an entire class of attacks, DNS spoofing, which has been used in campaigns costing billions of dollars in damages over the years[92]. DNSSEC is also deployed in part, and many ISPs have, in whole or in part, agreed to move forward towards wide deployments. While DNSSEC imposes economic costs in the form of signing and re-signing authoritative zones and non-trivial transitions of network configurations, many stakeholders stand to win from increased security, especially consumers, whom the FCC is supposed to protect. Further, the FCC has some authority in this area. Although the exact contours of their jurisdiction appear murky at the moment, ISPs have heeded the FCC's recommendations in the past, and may do so in the future as an alternative to costly and time-consuming litigation.

We recommended that the FCC draw from its venerable Communications Security, Reliability and Interoperability Councils and Working Groups, outlining a possible proposal for DNSSEC using CSRIC III Working Group 5. Our proposal specified the harms caused to users, suggested a solution, provided clear measurements and tools to assess progress over a timeline, opened a channel for comments from stakeholders, and provided examples of previous successes. We drafted such a proposal, which is available in the Appendix.

---

[92] See Kovacs, E. (2015, February 10). Cybercriminals Use DNS Poisoning in Brazilian Boleto Fraud Scheme and slides 4, 5, and 6 of Lamb, R. (2012, April). *DNSSEC Deployment: Where We Are (and where we need to be)*. PowerPoint presented at the MENOG 10, Dubai. Retrieved from https://www.icann.org/en/system/files/files/menog-dnssec-deployment-30apr12-en.pdf

6 APPENDIX

DNSSEC Adoption Code of Conduct for Internet Service Providers

1. Introduction:
    a. The FCC is committed to ensuring the virtuous cycle of the Open Internet. Internet security and reliability are key components of this virtuous cycle.
    b. The inability to verify the integrity of the responses to DNS queries represents a meaningful threat to end-users of the Internet. Attacks like DNS spoofing, whereby an attacker forces a DNS resolver to return an incorrect IP address for a given hostname, can redirect user traffic to malicious web pages, resulting in users disclosing personal data or being exploited in other ways.
    c. This document sets forth specific voluntary measures which ISPs may adopt to improve Internet security for end-users. These measures draw on the findings of CSRIC III Working Group 5.
    d. The core requirements for participation in this Code are set forth in Section 4.
2. Objectives and Principles
    a. The objectives of this Code are to:
        i. Provide specific, actionable steps for ISPs to take to improve Internet quality of service by implementing DNSSEC.
        ii. Provide a timeline for adoption.
        iii. Provide specific tools which will be used to measure compliance with DNSSEC adoption.
        iv. Seek comments about the effectiveness of this Code and how to improve it.

b. Implementation of this Code will be guided by the following principles:
    i. Voluntary -- participation is voluntary and ISPs may end their participation at any time.
    ii. Specific -- this Code endeavors to present specific implementation details, in order to make appropriate actions as clear as possible.
    iii. Best discretion -- the FCC does, however, recognize that technologies change, and allows ISPs to provide justification for using different techniques and technologies than those specified, provided they justify how their choice is consistent with the spirit of this Code.
    iv. Shared responsibility -- The FCC recognizes that DNSSEC adoption requires a multi-stakeholder approach, and is committed to providing assistance and listening to comments.
    v. Legal, effective, and appropriate -- All activities must comply with applicable law. If an ISP believes that part of this code would be ineffective, they should suggest an alternative. Activities should be cost effective for ISPs, provide clear benefits to end-users, and take into account the tenets of the Open Internet.
c. The FCC considers continuous, ongoing improvements to Internet security and reliability to be essential to preserving the Open Internet. It pledges to support ISPs that adopt this Code by providing technical guidance and tools for measuring compliance. ISPs are encouraged to work with the FCC to suggest improvements and amendments to this Code.

3. Scope and Rules

a. Definition of success: Success of this Code will be assessed in terms of implementation of timeline goals, defined in Section 4, by ISPs and by their participation in a conversation about how to improve the Code, and Internet security and reliability at large.

b. Benefits of participation in the Code

    i. Increased protection of consumer data.

    ii. Increased awareness of security threats by end-users.

    iii. Mitigation of some attacks, such as DNS spoofing.

    iv. Increased multi-stakeholder dialogue about how to improve the quality of Internet service via security and reliability.

    v. ISP's may advertise that they comply with the Code.

4. Parameters for Participation

    a. To take part in the pledge, an ISP will:

        i. agree that network security and reliability are top priorities

        ii. agree that DNSSEC is an integral part of network security and reliability

        iii. pledge to make substantive progress towards full adoption, in the form of:

            1. Implementing DNSSEC-specific functionality in compliance with the timeline below.

            2. Suggesting improvements to the Code.

            3. Publicly reporting on their progress in adopting DNSSEC.

    b. ISPs participating in the pledge agree to abide by the following timeline:

        i. Within 30 days of the publishing of this Code, agree to adopt the Code or provide clear reasons why the Code is unreasonable and suggest how it may be improved.

ii. Within 30 days of adopting the Code, provide an overview of the state of their network with regard to DNSSEC adoption. Identify obstacles to DNSSEC adoption and request assistance from the FCC and other stakeholders.

iii. Within 60 days of adopting the Code, make their DNS recursive nameservers DNSSEC-aware, as measured by the DNSSEC Resolver Check tool.

iv. Within 180 days of adopting the Code, make their DNS recursive nameservers full validators, as measured by the DNSSEC Resolver Check tool.

v. Within 1 year of adopting the Code, provide support for authenticated denial of existence, large packets, DNAME, and other functionality measured by the DNSSEC Resolver Check tool. Begin to suggest future improvements and additions to the Code as deemed appropriate by the community.

c. ISPs agree to publish specific updates about their compliance at regular intervals. ISPs do not have to publish information that would result in a competitive disadvantage.

d. ISPs participating in the pledge understand that their compliance will be measured by public tools provided by the FCC. Scans will be conducted at random intervals, and reports on ISP compliance will be regularly published in a format that is easily accessible.

e. If an ISP feels a tool is unreasonable or unfairly biased, they may submit reasons why they think the tool should be changed or not used. We encourage ISPs that do this to provide an alternative tool, so that they may be compared side-by-side.

5. Resources
    a. The DNSSEC Resolver Check tool, and accompanying usage instructions, can be found at: https://github.com/ogud/DNSSEC-resolver-check. Appendix 3 of Shinkuro's DNSSEC Roadmap for DHS also lists available tools, implementations, hardware and software (http://www.shinkuro.com/FA8750-10-C-0020/Publications/roadmap-021313-v21.pdf)
    b. A deployment guide written by the Internet society is available at: www.internetsociety.org/deploy360/resources/deployment-guide-dnssec-for-isps/
    c. NIST has published a Secure Domain Name System Deployment Guide (NIST 800-81), available online at: http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-81-2.pdf
    d. Several major ISPs, such as AT&T, Comcast, and Sprint, have implemented DNSSEC, as have newer ISP market entrants like Google Fiber. This Code draws on the findings of CSRIC III Working Group 5, which included members from several ISPs.
6. Comments: The FCC is committed to a dialogue with all stakeholders about how to ensure the Open Internet and protect end-users, and will make available methods for sending comments. The FCC pledges to review, publish, and respond to comments on an ongoing basis.

7 BIBLIOGRAPHY

ABCs for ISPs. (n.d.). Retrieved from https://www.m3aawg.org/abcs-for-ISP-code

American Recovery and Reinvestment Act of 2009, Pub. L. No. Public Law 111–5 (2013). Retrieved from http://www.gpo.gov/fdsys/pkg/BILLS-111hr1enr/pdf/BILLS-111hr1enr.pdf

Amir, H., & Haya, S. (n.d.). Towards Adoption of DNSSEC: Availability and Security Challenges. Retrieved from http://eprint.iacr.org/2013/254.pdf

Arends, R., Austein, R., Larson, M., Massey, D., & Rose, S. (March). DNS Security Introduction and Requirements. The Internet Society. Retrieved from https://www.ietf.org/rfc/rfc4033.txt

Assolini, F. (2011, November 7). Massive DNS poisoning attacks in Brazil.

Beaumont, C. (2009, December 18). Twitter hacked by “Iranian Cyber Army.” Retrieved from http://www.telegraph.co.uk/technology/twitter/6838993/Twitter-hacked-by-Iranian-Cyber-Army.html

Biggest Cybercriminal Takedown in History. (2011, November 9). Retrieved from http://krebsonsecurity.com/2011/11/malware-click-fraud-kingpins-arrested-in-estonia/

Brent, R., Dallas, W., Douglas, R., & Fern, B. (2011, June). The Role of Internet Service Providers in Cyber Security. Institute for Homeland Security Solutions. Retrieved from http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.473.2323&rep=rep1&type=pdf

Brent, R., & Michael, G. (2006). Private Sector Cyber Security Investment Strategies: An Empirical Analysis. Retrieved from http://www.econinfosec.org/archive/weis2006/docs/18.pdf

Chaskar, H. (2003, September). Requirements of a Quality of Service (QoS) Solution for Mobile IP. Nokia Research Center. Retrieved from https://tools.ietf.org/html/rfc3583

Chen, Jeremy. (2012, February 14). Google Public DNS: 70 Billion Requests a Day and Counting. Retrieved from https://googleblog.blogspot.com/2012/02/google-public-dns-70-billion-requests.html

Chevron U.S.A., Inc. v. Natural Resources Defense Council, Inc., No. 467 U.S. 837 (Supreme Court of the United States June 25, 1984). Retrieved from https://www.law.cornell.edu/supremecourt/text/467/837

Comcast Corporation v. FCC (US Court of Appeals for the District of Columbia Circuit April 6, 2010).

Communications Act of 1934, 47 USC § Title II--Common Carriers (1934). Retrieved from https://transition.fcc.gov/Reports/1934new.pdf

CSD-DNSSEC. (n.d.). Retrieved from http://www.dhs.gov/csd-dnssec

CSRIC Adopts Recs. to Minimize Three Major Cyber Threats. (2012, March 22). Retrieved from https://www.fcc.gov/document/csric-adopts-recs-minimize-three-major-cyber-threats

CSRIC III Working Group 4. (2012). *DNS Best Practices*. Retrieved from https://transition.fcc.gov/bureaus/pshs/advisory/csric3/CSRICIII_9-12-12_WG4-FINAL-Report-DNS-Best-Practices.pdf

CSRIC III Working Group 5. (2012). *DNS Implementation Practices for ISPs*. Retrieved from https://transition.fcc.gov/bureaus/pshs/advisory/csric3/CSRIC-III-WG5-Final-Report.pdf

CSRIC III Working Group 5. (2013). *Final Report on Measurement of DNSSEC Deployment*. Retrieved from https://transition.fcc.gov/bureaus/pshs/advisory/csric3/CSRIC_III_WG5_Report_March_%202013.pdf

Devdatta, A., & Adrienne Porter, F. (2013). *Alice in Warningland: A Large-Scale Field Study of Browser Security Warning Effectiveness*. Retrieved from http://research.google.com/pubs/pub41323.html

Direct Communications Cedar Valley LLC v. FCC, No. 11-9900 (US 10th Circuit Court of Appeals May 23, 2014). Retrieved from https://apps.fcc.gov/edocs_public/attachmatch/DOC-327257A1.pdf

DNSSEC FAQ | Domains - GoDaddy Help. (n.d.). Retrieved October 11, 2015, from https://uk.godaddy.com/help/dnssec-faq-6135

DNSSEC in 6 minutes - Deploying DNSSEC. (n.d.). Retrieved from https://kb.isc.org/article/AA-00820/0/DNSSEC-in-6-minutes.html

DNSSEC Scoreboard. (n.d.). Retrieved October 11, 2015, from http://scoreboard.verisignlabs.com/

DNSSEC stats. (n.d.). Retrieved from http://www.internetsociety.org/deploy360/dnssec/statistics/

ECONOMIC ANALYSIS OF CYBER SECURITY. (n.d.). Retrieved from www.dtic.mil/cgi-bin/GetTRDoc?AD=ADA455398

epic.org | Electronic Privacy Information Center. (2015). Retrieved from https://epic.org/privacy/dnssec/

FCC APPROVES MERGER OF AT&T INC. AND BELLSOUTH CORPORATION. (2006, December 29). FCC. Retrieved from https://apps.fcc.gov/edocs_public/attachmatch/DOC-269275A1.pdf

FCC APPROVES SBC/AT&T AND VERIZON/MCI MERGERS. (2005, October 31). FCC. Retrieved from https://apps.fcc.gov/edocs_public/attachmatch/DOC-261936A1.pdf

Federal Advisory Committee Act, Pub.L. 92–463 (1972). Retrieved from https://www.epic.org/open_gov/faca.html

Federal Communications Commission. (2010a). *Open Internet Order* (No. GN Docket No. 09 - 191). Retrieved from https://apps.fcc.gov/edocs_public/attachmatch/FCC-10-201A1.pdf

Federal Communications Commission. (2010b). *The National Broadband Plan*. Retrieved from https://transition.fcc.gov/national-broadband-plan/national-broadband-plan.pdf

Federal Communications Commission. (2013a). *BGP Security Best Practices*. CSRIC III Working Group 4. Retrieved from https://transition.fcc.gov/bureaus/pshs/advisory/csric3/CSRIC_III_WG4_Report_March_%20201 3.pdf

Federal Communications Commission. (2013b). *Consensus Cyber Security Controls* (Final Report). CSRIC III Working Group 11. Retrieved from https://transition.fcc.gov/bureaus/pshs/advisory/csric3/CSRIC_III_WG11_Report_March_%2020 13Final.pdf

Federal Communications Commission. (2013c). *Measurement of DNSSEC Deployment*. CSRIC III Working Group 5. Retrieved from https://transition.fcc.gov/bureaus/pshs/advisory/csric3/CSRIC_III_WG5_Report_March_%20201 3.pdf

Federal Communications Commission. (2013d). *U.S. Anti-Bot Code of Conduct (ABC) for Internet Services Providers (ISPs)* (Final Report). CSRIC III Working Group 7. Retrieved from https://transition.fcc.gov/bureaus/pshs/advisory/csric3/CSRIC_III_WG7_Report_March_%20201 3.pdf

Federal Communications Commission. (2014). *Notice of Proposed Rulemaking* (GN Docket No. 14-28 No. FCC 14-61). Retrieved from https://apps.fcc.gov/edocs_public/attachmatch/FCC-14-61A1.pdf

Federal Communications Commission. (2015). *Report and Order on Remand, Declaratory Ruling, and Order* (GN Docket No. 14-28 No. FCC 15-24). Retrieved from https://apps.fcc.gov/edocs_public/attachmatch/FCC-15-24A1.pdf

Fernando Paolieri Neto. (2015, February 9). DNS Poisoning Used In Boleto Fraud. Retrieved from https://blogs.rsa.com/dns-poisoning-used-boleto-fraud/

GoDaddy DNSSEC FAQ. (n.d.). Retrieved from https://uk.godaddy.com/help/dnssec-faq-6135

Google Developers | Security Benefits - Introduction: DNS security threats and mitigations. (2015, June 25). Retrieved from https://developers.google.com/speed/public-dns/docs/security#dnssec

Hadrien, H., Ernst, B., Patrick, L., Alessandro, F., & Marco, M. (2015). *A Study of the Impact of DNS Resolvers on Performance Using a Casual Approach*.

Infoblox Inc. (2013). *Top Five DNS Security Attack Risks and How to Avoid Them*. Retrieved from https://www.infoblox.com/sites/infobloxcom/files/resources/infoblox-whitepaper-top5-dns-security-attack-risks-how-to-avoid-them.pdf

Jason, L. (2012, January 10). Comcast completes DNSSEC deployment. Retrieved from http://corporate.comcast.com/comcast-voices/comcast-completes-dnssec-deployment

Lamb, R. (2012, April). *DNSSEC Deployment: Where We Are (and where we need to be)*. PowerPoint presented at the MENOG 10, Dubai. Retrieved from https://www.icann.org/en/system/files/files/menog-dnssec-deployment-30apr12-en.pdf

List of Major DNSSEC Outages and Validation Failures. (n.d.). Retrieved from http://ianix.com/pub/dnssec-outages.html

Marquis-Boire, M. (n.d.). A Brief History of DNS Hijackings. Retrieved from http://costarica43.icann.org/meetings/sanjose2012/presentation-dns-hijackings-marquis-boire-12mar12-en.pdf

Mergers and Acquisitions. (n.d.). Retrieved from https://www.fcc.gov/mergers

National Association of Broadcasters v. FCC (US Court of Appeals for the District of Columbia Circuit July 24, 1984).

Neto, F. P. (2015, February 9). DNS Poisoning Used In Boleto Fraud. Retrieved from https://blogs.rsa.com/dns-poisoning-used-boleto-fraud/

Prince, M. (2014, February 13). Technical Details Behind a 400Gbps NTP Amplification DDoS Attack. Retrieved from https://blog.cloudflare.com/technical-details-behind-a-400gbps-ntp-amplification-ddos-attack/

Rashid, F. Y. (2012, March 22). ISPs Agree to FCC Rules on Anti-Botnet, DNSSEC, Internet Routing. Retrieved from http://securitywatch.pcmag.com/security/295722-isps-agree-to-fcc-rules-on-anti-botnet-dnssec-internet-routing

Rotheli v. Chicago Transit Authority, No. No. 33606 (Supreme Court of Illinois November 23, 1955). Retrieved from https://scholar.google.com/scholar_case?case=7360554567166694650&hl=en&as_sdt=6&as_vis=1&oi=scholarr

Rulemaking Process at the FCC. (n.d.-a). Retrieved from https://www.fcc.gov/encyclopedia/rulemaking-process-fcc

Rulemaking Process at the FCC. (n.d.-b). Retrieved from https://www.fcc.gov/encyclopedia/rulemaking-process-fcc

Security Tools and Architectures Section of ENISA, & Deloitte Enterprise Risk Services. (2009). *Study on the Costs of DNSSEC Deployment*. Retrieved from https://www.enisa.europa.eu/publications/archive/dnsseccosts

Security Vulnerabilities in DNS and DNSSEC. (n.d.). Retrieved from https://dl.acm.org/citation.cfm?id=1250514

Sherling, M. (2014). The Likely Regulators? An Analysis of FCC Jurisdiction over Cybersecurity. *Federal Communications Law Journal*, *567*. Retrieved from http://www.fclj.org/wp-content/uploads/2014/12/66.3.7-Sherling-FINAL.pdf

Telecommunications Act of 1996, Title 47, Chapter 5 § 254.

Terms and Definitions Related To Quality of Service and Network Performance Including Dependability. (1994). (No. E.800). ITU-T. Retrieved from http://www.itu.int/rec/T-REC-E.800/en

The Communications Security, Reliability and Interoperability Council. (n.d.). Retrieved from https://transition.fcc.gov/pshs/advisory/csric/

The Domain Name System (DNS): Security challenges and improvements. (n.d.). Retrieved from http://www.ma.rhul.ac.uk/static/techrep/2010/RHUL-MA-2010-03.pdf

The Internet of Everything: 2015. (n.d.). Retrieved from http://www.businessinsider.com/internet-of-everything-2015-bi-2014-12

Tortes v. King County, No. No. 49576-3-I (Court of Appeals of Washington, Division 1 June 2, 2003).

Ullrich, J. B. (n.d.). SNMP: The next big thing in DDoS Attacks? Retrieved from https://isc.sans.edu/forums/diary/SNMP+The+next+big+thing+in+DDoS+Attacks/18089/

United States Telecom Association v. FCC (US Court of Appeals for the District of Columbia Circuit December 4, 2015).

Verizon Communications Inc. v. FCC (D.C. Circuit January 14, 2014).

What We Do. (n.d.). Retrieved from https://www.fcc.gov/what-we-do

Why you need to deploy DNSSEC now. (n.d.). Retrieved from http://www.infoworld.com/article/2608759/security/security-why-you-need-to-deploy-dnssec-now.html

Workshop on the economics of information security. (n.d.). Retrieved from http://www.econinfosec.org/archive/weis2015/

8 AUTHOR CONTRIBUTIONS

- At the earlier stages, we all researched the benefits and criticisms of DNSSEC, and we looked into various DNS and cyber security alternatives

- Clark wrote the abstract, first section of the introduction, the FCC jurisdiction, proposal, conclusion, and appendix Code of Conduct sections. He also proofread and edited the paper.
- Eric wrote the technical analysis of DNSSEC, flaws in DNS, and attacks on DNS.
- Kesiena wrote the stakeholder analysis, some of the economic analysis and implementation cost.