CSRIC

Communications Security, Reliability and Interoperability Council

March 2019

Final Report – Report on Best Practices and Recommendations to Mitigate Security Risks to Current IP-based Protocols

Table of Contents

1 Executive Summary

The charter of this working group included a deliverable to report on the Best Practices and Recommendations to Mitigate Security Risks to Current IP-based Protocols. This is an extremely broad topic, and could include many different technologies; too many to give any justice in a single report. The Session Initiation Protocol (SIP) was also considered, although this study would require much more time given the many vulnerabilities in SIP.

It was the working group's decision to focus on the Domain Name System (DNS) and the Border Gateway Protocol (BGP) protocol used in routing for DNS messages. This decision was partly based on a recommendation from the FCC, given the current issues facing the DNS ecosystem.

There has been a lot of work in previous CSRICs on DNS and BGP; however, we continue to face the same issues (as well as some new ones) that have plagued DNS for many years. In recent years, there have been marked increases in traffic redirection, spoofed originating addresses, and Denial of Service (DoS) attacks.

When the DNS was first implemented, there were different protocols used to route packets through the Internet. BGP was introduced as an improvement to these earlier routing protocols, but the Internet was still young and security was not a major consideration.

Over time, the Internet has grown exponentially, and the Internet domains have grown along with it. As with any network technology, over time vulnerabilities begin to be exploited, and security becomes a priority. This is certainly the case with the DNS.

CSRIC VI, WG 3 examined the findings of the previous CSRICs to understand how those findings aligned with today's current DNS, and whether there were new issues that should be addressed. Additionally, this CSRIC examined changes to the DNS ecosystem, and identified new threats based on incidents over the last several years.

There are new best practices being developed to address many issues remaining in DNS and BGP (not to mention other Internet protocols and applications), but CSRIC VI, WG 3 ran out of time to finish studying these new recommendations. Some (such as NIST) have not even been published as of this date, and therefore could not be reviewed by this CSRIC. There will certainly need to be future studies of the DNS and its routing protocol BGP, to ensure that the system is made secure without impacting performance.

Working Group 3 wishes it could have completed its studies in both previous recommendations and new best practices, but time was cut short by a government shutdown, preventing access to many resources the WG was considering. We were able to provide a good summary of what was recommended previously, what has changed since previous CSRIC studies of DNS, and what we see coming in the future.

2 Introduction

2.1 *CSRIC Structure*

Communications Security, Reliability and Interoperability Council VI		
Working Group 1: Transition Path to NG911	**Working Group 2: Comprehensive Re-imagining of Emergency Alerting**	**Working Group 3: Network Reliability and Security Risk Reduction**
Chair: Mary Boyd, West Safety Services	***Chair***: Farrokh Khatibi, Qualcomm	***Chair***: Travis Russell, Oracle
FCC Liaisons: Tim May, John Healy	***FCC Liaisons***: Steven Carpenter, Austin Randazzo	***FCC Liaisons***: Suzon Cameron

Table 2-1: CSRIC VI Structure

2.2 *Working Group 3 Team Members*

Working Group 3 consists of the members listed below.

Name	Company
Chair Travis Russell, Director, Cyber Security	Oracle Communications
Shirley Bloomfield, CEO	NTCA–The Rural Broadband Association
Don Brittingham, VP, Public Safety Policy	Verizon Communications
Charlotte Field, SVP, Application Platform Operations	Charter Communications
Bob Gessner, Chairman	American Cable Association
Michael Iwanoff, SVP and CISO	iconectiv
Mohammad Khaled, Senior Security Specialist	Nokia Bell Labs
Jason Livingood, VP, Technology Policy & Standards	Comcast Cable
Jennifer A. Manner, SVP of Regulatory Affairs	EchoStar/Hughes
Robert Mayer, VP – Industry and State Affairs	USTelecom
Susan Miller, President & CEO	Alliance for Telecom Industry Solutions (ATIS)
Drew Morin, Director, Federal Cyber Security Technology and Engineering Programs	T-Mobile
Sara Mosley, Acting CTO, OCC/NPP*	Department of Homeland Security
Greg Schumacher, Technology Development Strategist	Sprint Corporation
Lee Thibaudeau, CTO & VP of Engineering	Nsight
Tim Walden, SVP of Engineering and Construction	CenturyLink

Name	Company
Jeremy Larson, Network Manager	USConnect
Martin Dolly, Lead Member of Technical Staff	AT&T Services Inc.
John A. Marinho, VP Technology & Cybersecurity	CTIA

Table 2-2 : List of Working Group Members

SMEs, Acknowledgements:

- **Doug Montgomery, NIST**
- **Tale Lawrence – Oracle Dyn**

In addition to these SMEs, several WG members provided their expertise in the area of DNS and BGP.

3 Introduction to DNS and BGP

The BGP and the DNS are two fundamental technologies for the Internet. DNS provides, among other things, addressing information for computers connected to the network, and BGP guides how data is routed between systems. At the time, there were very few networks, and therefore security was not of concern. Both facilities were originally defined without strong security guarantees but they have evolved to address that shortcoming through a combination of heuristics, best current practices, and cryptographic extensions.

At a high level, the DNS is a widely distributed database that maps names (such as fcc.gov) to various types of data, most commonly the numeric addresses of devices connected to the Internet (such as an IP address). It is a directory, distributed globally to support millions of Internet domain names.

When someone types in the URL of a website for example, a query is sent to the DNS server supporting the consumers Internet connection to be resolved to an IP address. The first server it reaches is a recursive resolver. The mobile operator or the ISP providing Internet services usually operate the recursive resolver.

Before the recursive resolver can provide an answer, it first must find out about the top-level domain (TLD) (.com for example). There are root servers located all over the world that provide this information. The root servers provide the address of the TLD servers that contain the addressing information for the domain name servers in their jurisdiction. The domain name servers contain the specific addressing for the requested URL (i.e., fcc.gov).

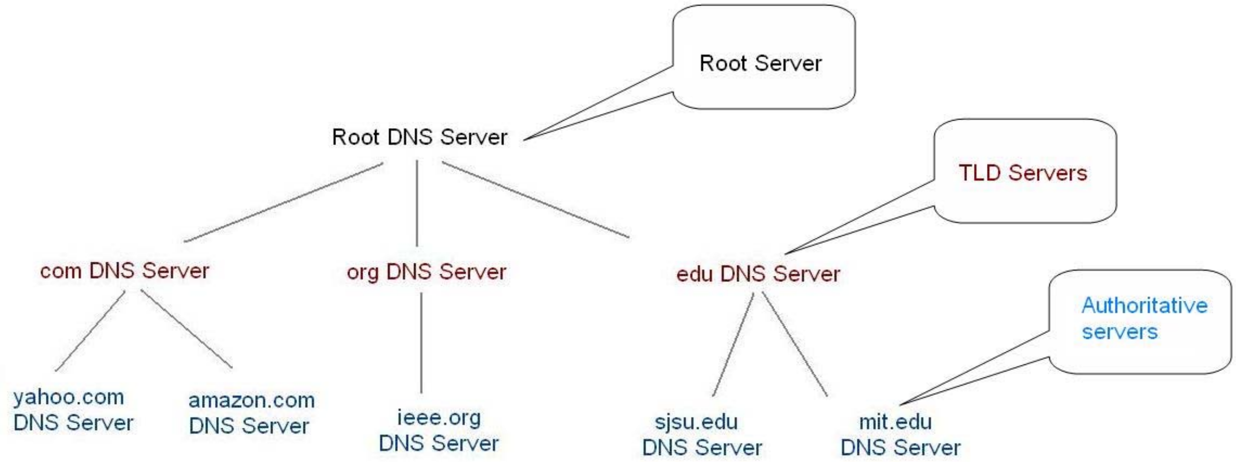

Figure 3-1: The DNS hierarchy. SOURCE: Richard.bhuleskar at English Wikibooks

The DNS protocol is defined in roughly 150 Request for Comments (RFC) documents published by the Internet Engineering Task Force (IETF), dating back to 1983. Significant backwards compatibility has been maintained in the DNS since its creation, such that a DNS request formatted per the original definition can still be processed today.

BGP controls the flow of data by describing how the various sub-networks that comprise the Internet are connected to each other. In essence, it works pairwise by one router telling a peer router that a particular network can be reached through it. This updates the state of the peer router’s internal table for directing packets, feeding the adjacency information into an algorithm that resolves how to move data packets through the network mesh. The earliest BGP definition by IETF RFC was in 1989, though there have been significant version updates in the core protocol since its inception.

IP addresses are grouped into prefixes, into an Autonomous System (AS). A corporation owning those IP addresses is considered an AS. The BGP than maintains the routing between these autonomous systems. Each AS will advertise its routes to its peer AS autonomously.

Given the legacy of both BGP and DNS, coming from a time before the pre-commercial Internet when network membership was very restricted[1], they each have many design aspects that decades of experience have shown to impact security and resiliency.

Namely, the concept of peer discovery has been found in other technologies to be subject to vulnerabilities. The automated fashion by which network elements learn of new routes, and automatically adjust their own routing based on discovery of routes from a new network element (or modifications made to an existing router) is at the very essence of most of the vulnerabilities in BGP.

[1] This era featured a relatively limited number of connected networks, run mostly by university and government organizations, with assumed or implied trust and security in the underlying protocols and networks. This is obviously no longer the case and so subsequent protocols have been developed with a need for security and resiliency to attack as key design requirements.

4 Previous CSRIC Findings

The CSRIC III, WG 4 and WG 6 published reports on DNS and BGP vulnerabilities. They focused on a number of vulnerabilities with the DNS network, supported by the BGP protocol, and made several recommendations.

This section outlines the vulnerabilities cited by the previous CSRICs.

4.1 *Challenges cited in previous reports*

4.1.1 BGP Session-Level Vulnerability

When two routers are connected and properly configured, they form a BGP peering session. Routing information is exchanged over this peering session, allowing the two peers to build a local routing table, which is then used to forward actual packets of information. The first BGP attack surface is the peering session between two individual routers, along with the routers themselves. Two classes of attacks are included here, session hijacking and denial of service.

4.1.2 Session Hijacking[2]

Session hijacking is the interception of IP addresses through the corruption of BGP routing tables. This results in Internet packets being routed away from their intended destinations. Hijacking can occur using a variety of techniques:

- An AS can advertise that it originates an IP prefix that it does not actually originate
- An AS can advertise a more specific IP prefix than what may be announced by the true originating AS
- An AS can advertise that it can route traffic to the hijacked AS through a shorter route than is already available, regardless of whether or not the route actually exists. Denial of Service (DoS) Vulnerability

Because routers are specialized hosts, they are subject to the same sorts of Denial of Service (DoS) attacks as any other networked host or server. These attacks fall into three types:

1) Attacks that seek to consume all available interface bandwidth making it difficult for enough legitimate traffic to get through such as UDP floods and reflective attacks
2) Attacks that seek to exhaust resources by consuming all available CPU cycles, memory, or ports so that the system is too busy to respond such as TCP SYN attacks
3) Attacks utilizing specially crafted packets in an attempt to cause the system to crash or operate in an unexpected way such as buffer overflow attacks, or malformed packet attacks that create an exception that is not properly handled

4.1.3 Source-address filtering

Many Internet security exploits hinge on the ability of an attacker to send packets with spoofed source IP addresses. Masquerading in this way can give the attacker unauthorized access at the device or application level. Some BGP vulnerabilities are also in this category of exploit. The

[2] https://en.wikipedia.org/wiki/BGP_hijacking

problem of source-spoofing has long been recognized and countermeasures are available for filtering at the interface level[3].

4.1.4 Internet Routing Registry (IRR)

The Internet Routing Registry (IRR) is a globally distributed routing information database. Established in 1995, the purpose of the IRR is to ensure the stability and consistency of Internet-wide routing by sharing information between network operators. The IRR actually consists of several databases where network operators publish their routing policies and routing announcements so that other network operators can use this data.

4.2 *Previous CSRIC Recommendations*

Many of the recommendations from the previous CSRIC work efforts are still applicable to current day DNS and BGP implementations. The CSRIC VI WG3 supports consideration of these recommendations, in addition to the specific recommendations cited at the end of this report in Section 6, which represent the current state of industry evolution

1) ISPs should refer to and implement the practices found in CSRIC II, WG 2A – Cyber Security Best Practices that apply to securing servers and ensure that routing infrastructure is protected.
2) ISPs should adopt applicable Best Current Practices (BCPs) found in network security industry approved/adopted publications. Three documents were identified that currently apply to protecting ISP networks: IETF BCP 38, BCP 46, and RFC 4778
3) ISPs should ensure that methods exist within the ISP's operations to respond to detected or reported successful route injection and propagation attacks, so that such entries can be rapidly remediated.
4) ISPs should consider implementing routing-specific monitoring regimes to assess the integrity of data being reported by the ISP's routers that meet the particular operational and infrastructure environments of the ISP.

4.3 *What Has Changed Since CSRIC III*

Industry has addressed some of the issues in the BGP protocol by introducing a new specification for encryption. "BGPsec Protocol Specification", RFC 8205[4], was introduced in September 2017. BGPsec is an extension to the BGP that provides security for the path of ASs through which a BGP UPDATE message passes.

BGPsec has limited deployment due to a number of factors, including its relative newness, its complexity, and new risks that it introduces. When being implemented, configurations that are currently working can be broken due to the stricter security policy. A good portion of the routers currently used to transport traffic on the Internet would need to be upgraded with more processing power and memory to handle BGPSec that makes BGPSec an expensive option.

[3] Such as from the Internet Corporation for Assigned Names and Numbers (ICANN), which maintains the Security & Stability Advisory Committee (SSAC). https://www.icann.org/groups/ssac. The ICANN SSAC released a document with observations and recommendations on source-address filtering, SAC004, available at https://www.icann.org/en/system/files/files/sac-004-en.pdf. Another authoritative source is the IETF and their Best Current Practice (BCP) document series, with BCP 38 applicable here, entitled "Network Ingress Filtering: Defeating Denial of Service Attacks which employ IP Source Address Spoofing", available at https://tools.ietf.org/html/bcp38.

[4] https://tools.ietf.org/pdf/rfc8205.pdf

In addition to technical solutions, the IETF has introduced best practices for BGP. "BGP Operations and Security", RFC 7454,[5] was released in February 2015 updating best practices for BGP security.

The IETF released "BGP Prefix Origin Validation", RFC 6811[6], in January 2013 (a few months before the release of the CSRIC III document). While BGP Prefix Origin Validation has been released, it has not been widely deployed.

NIST released a draft of the Special Publication 1800-14C[7] practice guide in August of 2018. NIST is proposing Route Origin Validation (ROV) and provides examples on how to implement the BGP ROV protocol on commercially available hardware and software.

The Internet Society (ISOC) launched an initiative in 2014 to address the need for clearly defined best operational practices for routing. The Mutually Agreed Norms for Routing Security (MANRS)[8] was initially targeted to core transit providers and the Internet exchange points where many ASs are connected. The effort has grown to encompass more than 100 different network operators and recently expanded its scope to include the slightly different needs of content delivery networks and cloud service providers.

During CSRIC III, several working groups touched on the DNS. CSRIC Working Group 4 studied DNS security as well as other aspects of network security generally, while Working Group 5 focused more specifically on DNS Security Extensions (DNSSEC) implementation practices for ISPs. In addition, Working Group 7 focused on botnet remediation and established the U.S. Anti-Botnet Code of Conduct. DNS operations, standards, and threats have evolved since this time, and these changes touch on the work of each of those prior working groups.

4.4 *Developments Since CSRIC III, Working Group 4's Report:*

WG4's assessment of threats remains accurate today, as do their associated recommendations[9]. However, Section 4.3.1 "Recursive DNS server operator for customer base" may in the future change, based on the implementation of the new DNS over HTTPS (DoH) or DNS over TLS (DoT) standards, as explored further below in "Coming Years: How Will New Standards be Implemented?" In essence, it seems possible that a large fraction of DNS traffic could shift from ISPs to a small number of third parties[10], with undetermined implications for the security and stability of the Internet.

4.5 *Developments Since CSRIC III, Working Group 5's Report:*

WG5's assessment of issues and their recommendations[11] and deployment measurement[12] remain largely accurate today. Since the time of the report, ISPs such as Comcast and centralized DNS providers such as Google Public DNS have implemented DNSSEC validation, leading to increasing numbers of users that are protected by DNSSEC-based resolvers.[13,14]

[5] https://tools.ietf.org/pdf/rfc7454.pdf

[6] https://tools.ietf.org/pdf/rfc6811.pdf

[7] Protecting the Integrity of Internet Routing: Border Gateway Protocol (BGP) Route Origin Validation; https://csrc.nist.gov/publications/detail/sp/1800-14/draft

[8] https://www.internetsociety.org/issues/manrs/

[9] https://transition.fcc.gov/bureaus/pshs/advisory/csric3/CSRICIII_9-12-12_WG4-FINAL-Report-DNS-Best-Practices.pdf

[10] Such as Google and Cloudfare

[11] https://transition.fcc.gov/bureaus/pshs/advisory/csric3/CSRIC-III-WG5-Final-Report.pdf

[12] https://transition.fcc.gov/bureaus/pshs/advisory/csric3/CSRIC_III_WG5_Report_March_%202013.pdf

[13] https://www.internetsociety.org/resources/doc/2016/state-of-dnssec-deployment-2016/

[14] https://stats.labs.apnic.net/dnssec

According to APNIC's statistics[15] for the US as of January 2019, 25% of Internet users leveraged DNSSEC-validating resolvers.

Domain signing, especially automated key rollover, continues to be an area of developing operational maturity for authoritative domain name owners, especially those with high DNSSEC adoptions rates in the United States .gov[16] TLD. However, as expected and noted in the report, Negative Trust Anchors[17] (NTAs) can and have been used to reduce the impact of such DNS failures as necessary.[18]

Finally, a related protocol that leverages DNSSEC is called DNS-based Authentication of Named Entities (DANE).[19,20,21] As a result of a foundation of DNSSEC deployment, the DANE protocol is being adopted at an increasing rate.[22,23]

Though many major DNS providers frequently interact through organizations like the IETF, DNS-OARC, and an informal industry group known as "DNS Inside Baseball", there is currently no equivalent to the MANRS effort in the DNS space. People in the industry have noted this void and there are some initial seeds being planted to grow such an organization.

4.6 *Developments Since CSRIC III, Working Group 7's Report:*

In general, WG7's assessment of barriers and metrics, as well as their Anti-Botnet Code of Conduct, remain valid.

The report is neutral on the manner of technical implementation, though in practice some ISPs performed this function by monitoring recursive DNS traffic from end users and devices for matches against well-known malware command and control fully qualified domain names (FQDNs).

However, new technical barriers may emerge in the future as a result of the implementation of the new DoH or DoT standards, as explored further below in "Coming Years: How Will New Standards be Implemented?" To the extent that ISPs play a significantly reduced role in end-user DNS recursion, those ISPs may be less able to serve in a meaningful role to combat the myriad threats related to botnets and malware.

4.7 *DNS Amplification Attacks*

Distributed Denial-Of-Service (DDoS) attacks using DNS amplification have been dramatically increasing over the last few years. Reflection is achieved by eliciting a response from DNS resolvers to a spoofed IP address. Attackers can send DNS queries to these servers by specifying the target's IP address as the request's source address. This causes the server to direct its response to the victim instead of the real source of the DNS query.

DNS amplification is a type of reflection attack that manipulates publicly-accessible DNS open resolvers, making them flood a target with large quantities of UDP packets. Through various

[15] https://stats.labs.apnic.net/dnssec/US
[16] https://itif.org/publications/2017/03/31/closer-look-dnssec-us-government-websites
[17] https://tools.ietf.org/html/rfc7646
[18] https://indico.dns-oarc.net/event/28/contributions/519/attachments/496/808/Crowe-NTA-Comcast.pptx
[19] https://tools.ietf.org/html/rfc6698
[20] https://www.ietfjournal.org/dane-taking-tls-authentication-to-the-next-level-using-dnssec/
[21] https://www.internetsociety.org/resources/deploy360/dane/
[22] https://twitter.com/internet_nl/status/1092357261169737728
[23] https://mail.sys4.de/pipermail/dane-users/2019-February/000517.html

methods, a DNS request message of 60 bytes can be configured to elicit a response message of over 4000 bytes to the target server – resulting in a 70:1 amplification factor.

Common ways to prevent or mitigate the impact of DNS amplification attacks include tightening DNS server security, blocking specific DNS servers or open recursive relay servers and response rate and response size limiting. Attack detection rules (such as seeing many queries from the same source IP address) can be created to identify signs of an attack. These methods do not eliminate attack sources nor do they reduce the load on networks and switches between name servers and open recursive servers. Blocking traffic from open recursive servers can potentially interfere with legitimate DNS communication attempts.

In the report from CSRIC III, WG 5, the report noted in Section 5.1.2.6 a potential concern that more severe DNS amplification attacks could result with the widespread deployment of DNSSEC. However the significant DNS-related security threats appear to be due to more typical DNS amplification attacks,[24] domain name hijacking,[25,26,27] DNS-changing malware,[28] and—in particular—DDoS attacks against authoritative DNS infrastructure.[29] A primary risk for fraudulent data appearing in the DNS is not even an attack on the DNS protocol itself, but rather compromised credentials at DNS hosting services that can then be used to update the authoritative data that is published in the DNS.

4.8 *DNS over TLS and HTTPS*

There have been ongoing concerns over protecting DNS queries from different types of confidentiality, integrity and availability attacks. Two security mechanisms have been proposed that have different characteristics and operate very differently.

4.8.1 New IETF Standard: DNS over TLS (DoT)

The first is using TLS encryption and authentication for protecting the DNS queries (RFC 7858, 8310).[30][31]

In 2016, the Internet Engineering Task Force (IETF) approved a new standard for encrypting DNS traffic using the new DNS over Transport Layer Security (TLS) standard, referred to as DoT, in RFC 7858.[32] In short, DoT enables encryption of DNS traffic over the wire, from the source client (stub) to the recursive DNS server.

The key aspects of this approach are the following:

- TLS is a well know secure tunneling protocol that is widely used to protect sensitive traffic
- DNS queries are encrypted until they reach the resolver to avoid sniffing and integrity attacks
- TLS sessions can be reused for multiple queries
- The next hop ISP can no longer intercept DNS queries

[24] https://krebsonsecurity.com/2018/12/feds-charge-three-in-mass-seizure-of-attack-for-hire-services/

[25] https://arstechnica.com/information-technology/2019/01/godaddy-weakness-let-bomb-threat-scammers-hijack-thousands-of-big-name-domains/

[26] https://cyber.dhs.gov/assets/report/ed-19-01.pdf

[27] https://www.zdnet.com/article/iranian-hackers-suspected-in-worldwide-dns-hijacking-campaign/

[28] https://www.scmagazine.com/home/security-news/ghostdns-hijacking-campaign-steps-up-attacks-on-brazilians-100k-devices-compromised/

[29] https://dyn.com/blog/dyn-statement-on-10212016-DDoS-attack/

[30] https://tools.ietf.org/html/rfc7858

[31] https://tools.ietf.org/html/rfc8310

[32] https://tools.ietf.org/html/rfc7858

- TLS requests use a distinct port (853) where anyone at the network level can easily see them and potentially block them. However, they would not see the content or response.
- With this approach DNS continues to be a network service provided by ISPs where monitoring, traffic inspection, blocking botnets and malware with localized DNS filters and network management can continue to operate

While DoT implementation is in the very early stages, this capability is being added to existing DNS server software.[33] It seems reasonable to expect that many or even most large-scale recursive DNS operators will test and/or implement DoT in the next several years.

4.8.2 New IETF Standard: DNS over HTTPS (DoH)

In 2018, the IETF approved an alternative standard to DoT for encrypting DNS traffic using the new DNS over HTTPS (DoH) standard in RFC 8484 to protect queries but creates a different service model.[34]

The key aspects of this approach are the following:

- This transmits DNS queries to the resolver over an encrypted HTTPS connection via a browser
- It can be used by any HTTPS-speaking app, bypassing the Operating System and its configuration
- The device-to-resolver connection is encrypted and hidden inside Web traffic thus making it harder to block without impacting good traffic
- Each application can use a different resolver (DNS becomes an application level service, not a network one). Your queries go wherever the app wants.

Due in part to how recent this standard is, the future for its implementation is less clear. But software developers, such as Mozilla and Google, appear to be considering a model[35,36] where the mobile operating system, mobile application, and/or web browser will ignore or bypass the ISP DNS IP addresses that have been assigned[37] to users and instead leverage DoH to direct DNS queries to a centralized DNS provider.

4.9 *Coming Years: How Will New Standards be Implemented?*

The recent DoT and DoH standards can be beneficial to users because they encrypt the communications from a client to a recursive DNS server. That protects them from potential surveillance or modification, such as by a hostile government or malicious actor.

However, if standards such as DoH bypass local DNS resolvers inside the networks of ISPs[38], government offices, enterprises, schools, libraries, and others, then these networks will be unable to provide DNS-based security and content controls, such as those being used to meet the US Anti-botnet Code of Conduct.

[33] Such as BIND, PowerDNS, and Unbound.
[34] https://tools.ietf.org/html/rfc8484
[35] https://hacks.mozilla.org/2018/05/a-cartoon-intro-to-dns-over-https/
[36] https://blog.powerdns.com/2018/09/04/on-firefox-moving-dns-to-a-third-party/
[37] Typically assigned via DHCP.
[38] Descriptions of this deployment mode are still developing. It has sometimes been called “DoH over Cloud” – DoC – or “Centralized DoH” -- CDoH.

This could reduce the end-user security and national security benefits of the recommendations made by CSRIC III's Working Groups 4, 5, and 7. In addition, it could move DNS query traffic to a small number of centralized providers that are not currently regulated by the FCC and do not participate in CSRIC, reducing the positive impact that ISPs have today in monitoring and securing their networks.

These standards are likely to be tested and, in some cases, deployed, perhaps even quite broadly if an individual company such as Google did so for Android devices, mobile applications, and Chrome/Chromium-based browsers.

Such a shift could represent a speedy and dramatic centralization of what is today a highly distributed protocol, with potential impacts on end user performance, Content Delivery Network (CDN) localization/performance, and the security and stability of the Internet as a whole. As a result, any such changes should be tested and measured thoroughly, and the pros and cons, costs, benefits, and risks weighed carefully by the broader Internet community,[39] regulators, and others.

4.10 *Mutually Agreed Norms for Routing Security (MANRS)*

There is a global initiative called MANRS comprising over 100 network operators, IXP operators and enterprises with the common goal of preventing route hijacking and certain types of DoS attacks via tools, standards and best practices developed by the IETF and the larger operational community. These operators represent thousands of autonomous system numbers (ASNs).

MANRS reports that there were close to 14,000 total routing incidents recorded in 2017. The major types of routing incidents were route/prefix hijacking, route leaks and IP spoofing. They have also identified existing best practices to address these threats through stronger filtering policies, and IP source validation. MANRS recognizes ongoing efforts to develop more effective tools like Route Origin Validation (ROV) and strengthening existing ones like further defining a feasible path in uRPF.

MANRS has four main focus areas to improve routing security:

4.10.1 Filtering

This is to ensure correctness of BGP route announcements and of those from customers to adjacent networks with prefix and AS-path granularity. This is to secure inbound routing advertisements particularly from customer networks through the use of explicit prefix-level filters or equivalent mechanisms. AS-path filters may be used to require that the customer network be explicit about which ASs are downstream of that customer.

[39] Not any single commercial entity. For example, Android has a 75% global market share according to http://gs.statcounter.com/os-market-share/mobile/worldwide. As a result, turning on DoH and sending traffic to a centralized DoH resolver could in one step redirect 75% of mobile device DNS lookups from ISP DNS servers to a centralized DoH resolver.

4.10.2 Anti-spoofing

This enables source IP address validation for at least single-homed stub customer networks, their end users and supporting infrastructure. It is designed to decrease spoof attacks by preventing hosts from sending packets with spoofed source IP addresses. There are different approaches identified such as Source Address Validation (SAV) or strict uRPF validation on router networks that could be used.

4.10.3 Coordination

This area covers maintaining accessible accurate and current contact information (e.g., NOC contact) in Regional Internet Registries (RIRs). Additional information should be captured to make it easy to obtain and use. Another aspect is authenticating and authorizing the maintainers of the information so that information cannot be corrupted.

4.10.4 Global Validation

This entails network operators publishing their data so others may validate routing information on a global scale. This includes the publicly documented routing policy, ASNs and prefixes that are intended to be advertised to external parties. This information can be stored in a RIRs mirrored by Routing Assets Database (RADb). Certificate-based technique can be also used to provide an extra layer of security.

MANRS has published an Implementation Guide[40] to provide specific guidance in implementing the various standards, tools and best practices. For publishing information, a checklist identifies all of the information elements (e.g., NOC contacts, peering locations) that should be stored in the different RIRs. Another checklist captures different mechanisms like ACLs, and filtering routes from your neighbors.

4.11 *NIST Technical Guidance and Recommendations*

There is a draft NIST Special Publication[41] currently out for review that provides initial technical guidance and recommendations to improve the security and robustness of inter-domain traffic exchange. The focus is on securing the inter-domain routing control traffic between enterprise networks or hosted service providers and the public Internet, preventing IP address spoofing and certain aspects of DoS/DDoS detection and mitigation. This covers both “stub” networks that only provide connectivity to their end systems and transit networks that interconnect and pass traffic between stub networks and other transit networks.

The recommendations attempt to reduce the risk of misconfigurations and malicious attacks in the routing control plane (i.e., border BGP router) and they help detect and prevent IP address spoofing and resulting DoS/DDoS attacks. The coverage also extends to other systems that support reachability in the Internet including DNS and RPKI repositories. The document does not address transport layer security that is key to message integrity during BGP communication sessions. It also does not address the entire server hardening issues that may be exploited for reflection and amplification attacks.

To address typical BGP vulnerabilities like prefix hijacking, AS path modification and route leaks, NIST provides a series of recommendations to address these issues. The completeness, correctness, freshness and consistency of the data derived from various sources like Regional

[40] MANRS Implementation Guide, Version 1.0, BCOP Series, January 25, 2017.

[41] Secure Interdomain Traffic Exchange – *BGP Robustness and DDoS Mitigation,* Draft NIST Special Publication 800-189, December 2018.

Internet Registries (RIRs) and Internet Routing Registries (IRRs) varies widely and requires proper registration and maintenance.

The RPKI is a standards-based approach for providing cryptographically secure registries of Internet resources and routing authorizations. Another key area discussed is verifying that an AS is authorized to announce BGP prefixes by providing a digital signature (i.e., Route Origin Authorization) with the prefixes.

There are other standards that are noted to further address the operational and security risks. BGP path validation (BGP-PV) or BGPsec has been standardized to secure the AS path in BGP announcements. BGP origin validation (BGP-OV) is necessary but by itself is insufficient for fully securing the prefix and AS announcement path.

While there has been work done on identifying operational considerations there are no commercially available vendor implementations. Recommendations for route leakage prevention solutions in terms of AS operators having ingress and egress policies are documented. The last area covered is recommended use by edge routers of the BGP flow specification (Flowspec) to facilitate DoS/DDoS mitigation in coordination between upstream and downstream ASs.

5 Current BGP Threats

5.1 *Denial of Service (DoS)/Distributed DoS (DDoS)*

Denial of Service is a general class of attack against a device connected to a network that attempts to use up a resource on that device. The resource is anything on the device itself; memory, CPU, and storage media and it can affect network resources as well.

The vast majority of these DoS attacks are DDoS attacks because it is much easier to send traffic from potentially millions of routable IPv4 addresses that do not belong to the attacker, thus drawing attention away from where the attacks originate. DoS attacks generally come from one or limited sources and are much easier to mitigate with Access Control Lists (ACLs) on a router or with a simple update to a firewall rule.

Bandwidth or Open Systems Interconnect (OSI) layer 3 network attacks will send traffic that is larger than the circuit belonging to the victim.

OSI layer 4 or transport attacks generally are protocol type attacks such as TCP SYN floods that try to use up TCP connection tables in a device.

OSI layer 7 or presentation attacks will cause the application on the device to become overwhelmed with responding to the application request that it will make the device too busy to respond to valid requests.

Not all attacks are inbound either, there are some that will try to request media from the device and fill up the outbound circuit of the victim with traffic that not only ties up the circuit but also could make the whole system non-responsive due to high disk usage needed to respond to the attack.

5.2 *Spoofed Source Address*

Spoofed IP source address abuse is a major cause of current Reflective Amplification (RA) DDoS attacks. RA attacks are a type of DDoS attack that uses services and protocols that respond to small requests for information with data that is many more times the size of the request.

Without any anti-spoofing controls, this allows the service (DNS, NTP, Chargen) to act as a reflector and amplify the amount of data towards the victim. It takes a minute amount of effort to change the source IP address in an IP packet and have Internet routing send the packet to the victim, making it highly improbable to identify the attacker. Recent attacks against a customer of a U.S. based service provider[42] and Github[43] in March of 2018 show spoofing is alive and well.

5.2.1 Previous CSRIC Recommendations:

In Section 5 of the report from CSRIC III, WG4, a number of recommendations raise various mitigation techniques to combat spoofed source addresses[44]. Since 2013 industry continued to evolve methods and techniques to address the threat, and while many recommendation from

[42] https://asert.arbornetworks.com/netscout-arbor-confirms-1-7-tbps-DDoS-attack-terabit-attack-era-upon-us/

[43] https://www.wired.com/story/github-DDoS-memcached/

[44] https://transition.fcc.gov/bureaus/pshs/advisory/csric3/CSRICIII_9-12-12_WG4-FINAL-Report-DNS-Best-Practices.pdf

2013 remain relevant, the recommendations contained herein represent the current industry status.

5.3 *Incorrect Routing Injections*

One of the recommendations made in previous CSRICs was for all AS operators to use the Resource Public Key Infrastructure (RPKI) to certify their numbered resources. In the case of North America, ARIN (American Registry for Internet Numbers) currently offers a hosted RPKI service, and intends to offer a fully delegated RPKI service at a later date.

Researchers from the University of Pennsylvania Law School recently published a paper exploring legal barriers that may be hindering RPKI adoption in North America. Such potential barriers include the North American RIR's (Regional Internet Registry) requirement for RPKI users to enter a Relying Party Agreement and certain terms in that agreement. The paper recommends certain steps that the RIR and other community members might take to spur RPKI adoption.[45]

5.3.1 Previous CSRIC Recommendations:

To mitigate routing injections, the previous CSRICs recommended implementation of a number of measures, including:

- Filtering received routing information
- Limiting the number of prefixes
- Monitoring announcements
- Autonomous System (AS) operators should ensure their Internet Routing Registry (IRR) records are public, complete, and up-to-date: Having a common, public notion of "ground truth" for identifying bogus routing information is a prerequisite for all BGP security solutions.

[45] Public Law and Legal Theory Research Paper Series Research Paper No. 19-02; Lowering Legal Barriers to RPKI Adoption, Christopher S. Yoo, David A. Wishnick, UNIVERSITY OF PENNSYLVANIA

6 CSRIC VI Recommendations

6.1 *Further CSRIC studies*

The DNS and BGP continue to evolve as the Internet continues to grow. Likewise, best practices continue to evolve. There are new best practices being developed, and implementation of existing measures (such as RPKI) continues. Therefore, this CSRIC recommends that there be future studies to ensure the most current best practices and mitigation techniques are understood and promoted through industry collaboration.

6.2 *Network Providers should implement the recommendations from the NSA Cyber Security Report*[46]

Network operators should implement the measures from the NSA Cyber security Report, "A Guide to Border Gateway Protocol (BGP) Best Practices, Document PP-18-0645, 10 Sept 2018", namely:

- Implementation of Access Control Lists Implementation of Control Plane Policing (COPP) Enabling the Maximum BGP Prefix Enabling BGP Prefix Filtering Enabling BGP Prefix Filtering with Autonomous System (AS) path Access Lists Enabling BGP Neighbors Authentication Enabling TTL Security Check

6.3 *Route Origin Validation*

NIST 1800-14A is still in its infancy, and needs more work. CSRIC VI recommends operators work closely with NIST on finalizing 1800-14A to ensure Route Origin Validation (ROV) can be implemented by operators.

6.4 *MANRS Recommendation*

MANRS is an important organization addressing routing security globally that is endorsed by CSRIC VI WG 3. It promotes global collective action to address routing security threats. It also provides the technical, operational and business framework to tackle this infrastructure problem. Tools, standards, industry efforts and best practices are identified and MANRS provides guidance in how to effectively implement these controls.

CSRIC recommends network operators participate and contribute to MANRS.

6.5 *NIST Recommendation*

NIST continues to evolve recommendations relating to secure inter-domain traffic exchange. Draft NIST Special Publication 800-189 is out for public review and responses are due March 15, 2019. The document references current standards and best practices from standards forums, industry groups and vendors. CSRIC VI, WG 3 recommends stakeholders provide comments to the draft so it can be finalized and provide specific technical guidance to federal and commercial

[46] https://www.nsa.gov/Portals/70/documents/what-we-do/cybersecurity/professional-resources/ctr-guide-to-border-gateway-protocol-best-practices.pdf?v=1

enterprises and service providers. These recommendations should be reviewed by future CSRICs for inclusion in future DNS/BGP reports.

Future CSRIC WGs may also consider studying the effects on the security, stability, and fragility of the Internet due to centralization of core protocols such as DNS.

6.6 *DNSSEC Development*

The historical use of RA attacks using open reflector devices indicates that the attack method is not going away and that attackers will seek more efficient ways to launch larger attacks in shorter periods of time, taking advantage of DNSSEC and exploiting weaknesses that exist. CSRIC VI recommends that no further work be done at this time on DNSSEC in favor of driving efforts showing more promise such as DNS over TLS and HTTPS as described below.

6.7 *DNS over TLS/HTTPS Recommendation*

6.8 *These two approaches are considered promising but they vary widely in terms of how they operate and potentially impact the current network-based service model. Considerable debate continues about the merits and negative aspects of each approach. CSRIC VI recommends that further work be done to evolve network and application security best practices to address these various types of endpoints, applications, network systems, encrypted connections, and traffic flows. In addition, given the potential negative performance concern with these new protocols and a lack of associated measurements, the FCC and industry should consider leveraging the Measuring Broadband America (MBA) platform to conduct a MBA Assisted Research Study (MARS)[47] to measure the performance differences between the current network-based DNS service model, centralized DoH, and DoT. Internet Routing Registry (IRR)*

ISPs that assign portions of their address space to customers should register and maintain accuracy of these address assignments in IRRs as appropriate.

6.9 *Number resource certification*

Operators of an Autonomous System (AS) should certify their number resources with your regional Internet registry.

[47] https://www.fcc.gov/general/mba-assisted-research-studies

Appendix A

ACL	Access Control List
APNIC	Asia-Pacific Network Information Centre
ARP	Address Resolution Protocol
AS	Autonomous System
ASN	Autonomous System Number
BCP	Best Current Practice
BGP	Border Gateway Protocol
BGP-OV	Border Gateway Protocol – Origin Validation
BGP-PV	Border Gateway Protocol – Path Validation
BGPsec	Border Gateway Protocol Security
CDN	Content Delivery Network
COPP	Implementation of Control Plane Policing
DANE	DNS-based Authentication of Named Entities
DNS-OARC	DNS Operations, Analysis, and Research Center
DNSSEC	Domain Name System Security extensions
DoT	DNS over TLS
DoH	DNS over HTTPs
CPU	Central Processing Unit
CSRIC	Communications Security, Reliability, Interoperability Council
DDoS	Distributed Denial of Service
DNS	Domain Name System
DoS	Denial of Service
FQDN	Fully Qualified Domain Name

HTTPS	Hyper Text Transfer Protocol Secure
ICANN	Internet Corporation for Assigned Names and Numbers
IETF	Internet Engineering Task Force
IP	Internet Protocol
IRR	Internet Routing Registry
ISOC	Internet Society
ISP	Internet Service Provider
MANRS	Mutually Agreed Norms for Routing Security
MARS	MBA Assisted Research Study
MBA	Measuring Broadband America
NIST	National Institute of Science and Technology
NOC	Network Operations Center
NSA	National Security Agency
NTA	Negative Trust Anchors
NTP	Network Time Protocol
OSI	Open Systems Interconnection model
RA	Reflective Amplification
RADb	Routing Asset Database
RIR	Regional Internet Registry
ROV	Route Origin Validation
RPKI	Resource Public Key Infrastructure
SAV	Source Address Validation
SSAC	Security & Stability Advisory Committee
TCP	Transmission Control Protocol
TLD	Top Level Domain
TLS	Transport Layer Security

UDP	User Datagram Protocol
URL	Universal Resource Locator
uRPF	Unicast Reverse Path Forwarding
WG	Working Group