SIDN Labs

https://sidnlabs.nl

July 3, 2020

Peer-reviewed Publication

Title: The DNS in IoT: Opportunities, Risks, and Challenges

Authors: Cristian Hesselman, Merike Kaeo, Lyman Chapin, kc claffy, Mark Seiden, Danny McPherson , Dave Piscitello, Andrew McConachie, Tim April, Jacques Latour, and Rod Rasmussen

Journal: IEEE Internet Computing 2020 (*to appear*)

DOI: 10.1109/MIC.2020.3005388

Citation:

- Citation: C. Hesselman, M. Kaeo, L. Chapin, kc claffy, M. Seiden, D. McPherson, D. Piscitello, A. McConachie, T. April, J. Latour, and R. Rasmussen, "The DNS in IoT: Opportunities, Risks, and Challenges", IEEE Internet Computing (*to appear*), 2020. DOI: 10.1109/MIC.2020.3005388
- Bibtex:

```
@article{Hesselman20a,
  author =  {Hesselman, C.  and Kaeo, M. and Chapin, L and kc claffy and
  Seiden, M.  and McPherson, D. and  Piscitello, D. and McConachie, A.
  and April, T.  and Latour, J. and Rasmussen, R. },
  title = {The DNS in IoT: Opportunities, Risks, and Challenges.},
  journal =  "IEEE Internet Computing (to appear)",
  year = {2020},
 number =TBD,
 doi = "10.1109/MIC.2020.3005388"
}
```

Citation: C. Hesselman, M. Kaeo, L. Chapin, kc claffy, M. Seiden, D. McPherson, D. Piscitello, A. McConachie, T. April, J. Latour, and R. Rasmussen, "The DNS in IoT: Opportunities, Risks, and Challenges", IEEE Internet Computing, to appear, 2020
DOI: 10.1109/MIC.2020.3005388
THIS IS THE AUTHORS' VERSION OF THE WORK

The DNS in IoT: Opportunities, Risks, and Challenges

Cristian Hesselman[1,2], Merike Kaeo[3], Lyman Chapin[4], kc claffy[5], Mark Seiden[6], Danny McPherson[7], Dave Piscitello[4], Andrew McConachie[8], Tim April[9], Jacques Latour[10], and Rod Rasmussen[11]

[1]SIDN Labs, cristian.hesselman@sidn.nl
[2]University of Twente
[3]Double Shot Security
[4]Interisle Consulting Group
[5]CAIDA/UC San Diego
[6]Internet Archive
[7]Verisign
[8]ICANN
[9]Akamai Technologies
[10]CIRA
[11]R2 Cyber

Abstract. *The Internet of Things (IoT) is widely expected to make our society safer, smarter, and more sustainable. However, a key challenge remains, which is how to protect users and Internet infrastructure operators from attacks on or launched through vast numbers of autonomously operating sensors and actuators. In this paper, we discuss how the security extensions of the Domain Name System (DNS) offer an opportunity to help tackle that challenge, while also outlining the risks that the IoT poses to the DNS in terms of complex and quickly growing IoT-powered Distributed Denial of Service (DDoS) attacks. We identify three challenges for the DNS and IoT industries to seize these opportunities and address the risks, for example by making DNS security functions (e.g., response verification and encryption) available on popular IoT operating systems.*

Keywords: DNS security, IoT security

Introduction

The Internet of Things (IoT) promises to further ease our daily lives through tens of billions of connected devices that passively and autonomously sense and act upon our physical environment. While this makes the IoT vastly different from traditional interactive Internet applications like email and web browsing, many IoT devices will

use the Domain Name System (DNS) to look up the IP addresses of the remote services they need, for instance to offload the analysis of sensor data. The DNS is a globally distributed, hierarchical, multi-operator infrastructure, in which we are involved as operators and researchers.

We discuss the interplay between the DNS and the IoT, arguing that the IoT represents both an opportunity for and a risk to the DNS [1]. It is an opportunity because the DNS provides functions and data that can help make the IoT more secure, stable, and transparent, which is critical given the IoT's seamless interaction with the physical world. It is a risk because various measurement studies suggest that IoT devices may stress the DNS due to complex DDoS attacks carried out by botnets that can grow to hundreds of thousands or perhaps even millions of infected IoT devices within hours.

These opportunities and risks present new challenges for the DNS and IoT industries [1] (e.g., for DNS and IoT operators and software developers) including, but not limited to: making the DNS's security functions (e.g., response verification and encryption) available on popular IoT operating systems and developing and operating shared systems that allow DNS operators to automatically share data on IoT botnet activity.

Our contribution is the analysis of the opportunities and the risks and the challenges we put forward, which to the best of our knowledge is unique work. Our aim is to trigger and facilitate dialogue on IoT security practices among stakeholders like IoT firmware developers and device manufacturers, DNS operators, and policy makers, as well as to provide guidance for new research directions. We do not detail a specific system or solution.

Overview of opportunities, risks, and challenges

Table 1 provides an overview of the opportunities, risks, and challenges we identify and discuss in detail in [1]. We discuss the ones in grey in this paper, after we briefly survey the IoT landscape and how the DNS serves the IoT in the next two sections.

Table 1: Overview of opportunities, risks, and challenges [1].

Opportunities
Using DoH/DoT to encrypt DNS queries
Using DNSSEC to detect malicious redirects of IoT devices
DNS protocols to double-check the authenticity of IoT services
Protecting IoT devices against domain registration hijacks
Using DNS datasets to increase IoT transparency

Risks
DNS unfriendly programming at IoT scale
Increased size and complexity of IoT botnets targeting the DNS
Increased DDoS amplification through open DNS resolvers

Challenges

Developing a DNS security and transparency library for IoT devices
Training IoT and DNS professionals
Developing a system to share information on IoT botnets
Proactive and flexible mitigation of IoT-powered DDoS traffic
Developing a system to measure how the IoT uses the DNS

The IoT landscape

The IoT is a term used to describe a range of Internet applications that extend "network connectivity and computing capability to objects, devices, sensors, and items not ordinarily considered to be computers" [2]. IoT applications are expected to connect tens of billions of such objects to the Internet [2] and affect almost all sectors of society, including "smart homes" with connected kitchen appliances, toys, and lighting, "smart cities" with connected streetlights and environmental sensors, and self-organizing dynamic networks of drones and robots.

The IoT is different because it exists "in the background" as an integral and invisible part of people's lives [2]. This is unlike traditional Internet applications, which focus on enabling humans to interact deliberately with content and services (e.g., through web browsers). For example, a smart home may be able to automatically unlock its front door based on the location of someone's phone and various biometric signals from their smart wristwatch (e.g., movement or heart rate patterns).

Another important difference is that IoT applications are typically control programs that run on wildly heterogeneous devices, while today's (web-based) Internet applications typically run on relatively homogenous laptops and mobile phones. For example, a smoke detector is typically small, battery-operated, does not have a user interface, and communicates via low-powered radios (e.g., Bluetooth Low Energy or Zigbee). On the opposite end of the spectrum, a connected refrigerator will often have a touch screen user interface, powerful processing and storage capabilities, and a WiFi connection to services on the Internet (e.g., goods suppliers or maintenance facilities).

DNS and the IoT

IoT devices typically exchange data with one or more remote services hosted on the Internet (e.g., to analyze sensor data) and often locate these services using the DNS protocol [3]. As a result, IoT deployments operate across two co-evolving and interacting ecosystems: (1) the DNS with its resolver operators, authoritative name server operators, and domain registration providers, and (2) the IoT with its device manufacturers, IoT device operators (e.g., drone operators), and providers of the remote services with which these devices interact.

Figure 1 shows two examples of IoT deployments, DP1 and DP2. The first scenario (on top) shows a smart home in which the devices first interact with the DNS in order to locate specific services. A smart wristwatch (device D1) queries the DNS for the address of a remote service (S1) named `s1.home1234.net`. The DNS returns S1's

IP address to D1 (see *DNS Lookups*, below), which D1 uses to send sensor readings to S1 (e.g., the user's movement and heart rate) across the Internet. S1 runs in data center DC1, analyzes the measurements, and automatically sends instructions to other devices in the house. For example, it could use biometric information from D1's sensors to identify the user (e.g., by analyzing the person's body movements) and automatically instruct the lock on the front door (device D3) to unlock when the smart watch (D1) is near it. At the same time, S1 could send instructions to turn on the lights in the house (device D2) and interact with other devices in the home (e.g., to turn on the heating).

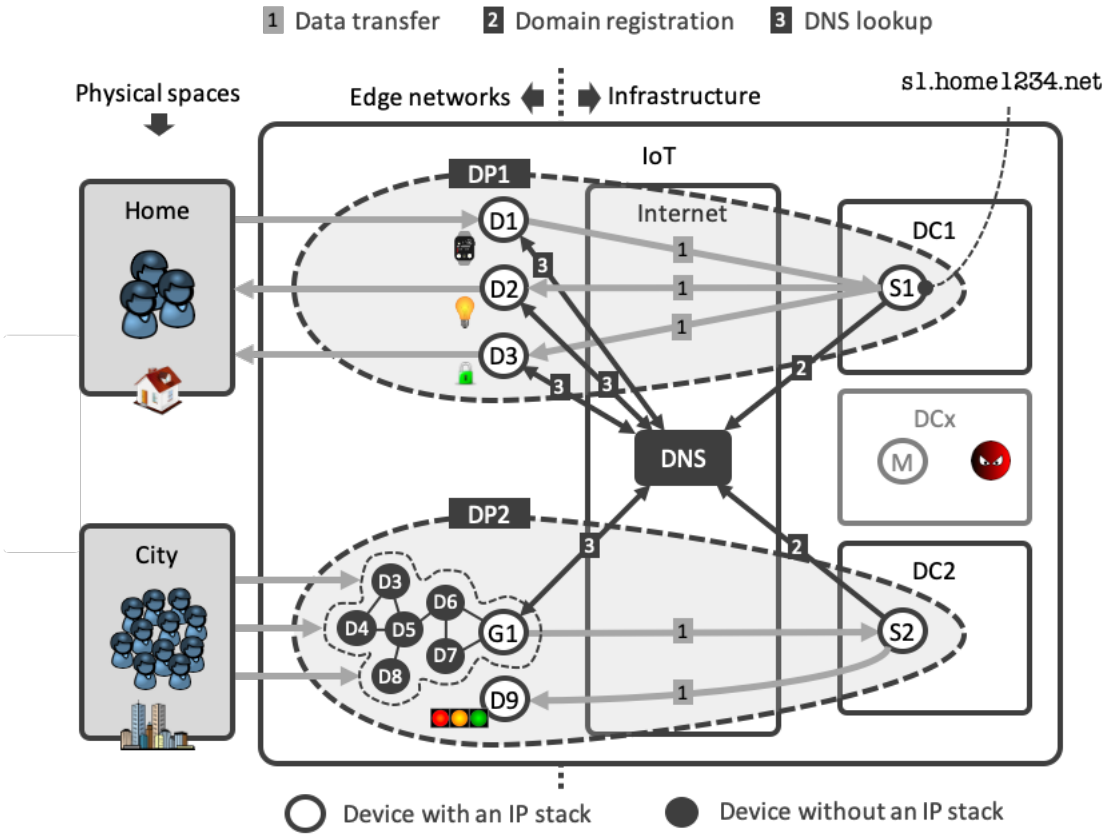

Figure 1: IoT deployment and the DNS.

The second scenario (bottom of Figure 1) shows a deployment DP2 with air pollution sensors (D3 through D9) spread across a city. They do not have an IP stack and therefore interact with their remote service S2 (running in DC2) through an intermediate gateway G1, which performs the DNS functions on behalf of the IoT devices. One advanced future scenario could be that S2 uses the air pollution readings to dynamically adjust traffic lights to guide traffic to parts of the city that are less polluted.

The services of an IoT deployment (e.g., S1 and S2) have their domain names registered in the DNS like any discoverable service on the Internet. The difference is that services in the IoT help IoT devices with sensing and acting upon a user's

physical world, whereas traditional Internet applications help users interact with content or services. In addition, services in an IoT deployment are usually invisible to end-users because the IoT device manufacturer configures them and users typically cannot easily change them.

DNS lookups

IoT devices and gateways resolve the domain name of a service by sending a DNS lookup request to a resolver, the DNS component that traverses the DNS to map the host name to an IP address. *Figure 2* shows a simplified view this process using device D1 (See *Figure 1*). For simplicity, we depict a single name server at each of the root (.), the top level (.net), and the second level (home1234.net).

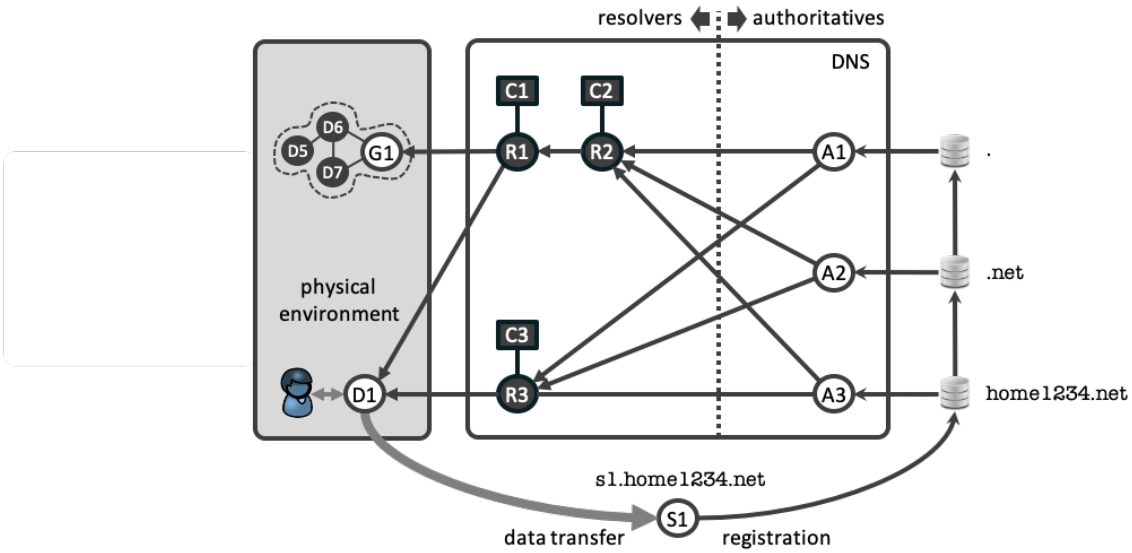

Figure 2: Simplified DNS resolution for IoT devices.

D1 sends a DNS query for s1.home1234.net to resolver R3, which passes the query to a root name server (A1). A1 returns the IP address of the authoritative name server for the .net "top level domain" (TLD), which R3 contacts next using the same query. The .net TLD's server (A2) returns the IP address of the name server for home1234.net (A3), to which R3 sends the query once more. A3 returns the IP address of s1.home1234.net, which R3 sends to D1 so it can use that IP address to connect to S1.

Resolver R3 is typically operated in edge networks by the user or by the user's ISP, but may also be a central public resolver (e.g., Google Public DNS) or one that the device manufacturer provides. Domain name lookups may involve multiple layers of resolvers; for instance, R1 might be a resolver on the user's home router and R2 a resolver at the user's ISP.

Resolver R3 typically has a cache (C3) in which it temporarily stores DNS responses, such as that of D1's query for s1.home1234.net. Caches are a crucial part of the DNS

architecture because they reduce the load on authoritative name servers (e.g., on A1 though A3), which enables the system to scale and reduces lookup latencies.

Opportunities for the DNS

IoT deployments introduce new security, availability, and transparency requirements because they interact with physical space [2], often without explicit human involvement or awareness. This is an opportunity for the DNS because it is a globally pervasive infrastructure with security extensions that can help in fulfilling these requirements. We discuss three extensions here and refer to [1] for a more elaborate overview.

DoH and DoT

DNS-over-HTTPS (DoH) and DNS-over-TLS (DoT) [4] are two new protocols that encrypt DNS messages between a DNS client and its resolver, thus hiding domain lookups and responses from on-path inspection and/or alteration.

One advantage of DoH and DoT for IoT devices is that third parties with access to links along the path the DNS query travels (e.g., an ISP or public hotspot operator), cannot observe the contents of the queries. For example, the sleep monitor studied in [3] uses six pre-configured domain names for its operation, such as hello-audio.s3.amazonaws.com and sense-in.hello.is. DoH or DoT hide these names from on-path observers, making it more difficult to learn the type of device and any vulnerabilities it may have. This is particularly important in the IoT because IoT devices often do not have a user interface, which means that compromises are more likely to go undetected.

For any potential DoH and DoT deployments, the risks and issues in centralized settings (e.g., when R3 in Figure 2 is a central public resolver) must be carefully considered, such as that it becomes more difficult for operators of access networks to detect malware with encrypted DNS traffic [5].

Using DNSSEC to detect malicious redirects of IoT devices

The purpose of the DNSSEC protocol is to verify that the response to a DNS query comes from an authoritative server and was not altered in transit. DNSSEC works by adding cryptographic signatures to DNS records, which resolvers validate using DNSSEC's chain of trust [6]. Validation errors indicate that the response to a DNSSEC-enabled query may have come from a non-authoritative source or has been tampered with in transit.

DNSSEC is important in the IoT because manipulated DNS messages can redirect IoT devices to a malicious service, jeopardizing user privacy, safety, and well-being. A relevant attack that DNSSEC helps to detect occurs when an adversary uses a Border Gateway Protocol (BGP) hijack to impersonate an authoritative DNS server. In *Figure 1,* an attacker could carry out such a hijack by injecting malicious announcements into the Internet's routing system claiming that it owns the IP

address range of S1's network, and then setting up a malicious authoritative DNS server utilizing the hijacked IP address of the actual server [7]. As a result, DNS queries for D1 services would receive answers from the malicious but now authoritative DNS server, which could direct D1 to a malicious site (M). All of D1's DNS queries (and all of D1's sensor data) would be sent to the attacker's network, possibly without user awareness. D1's resolver would detect such an attack if it were DNSSEC-enabled, because it would fail to validate the data from the malicious DNS server through DNSSEC's chain of trust.

DNSSEC also offers IoT devices additional means to check the authenticity of remote services after DNS resolution. For example, if D1 uses HTTPS to connect to S1, it can use DNS Authentication of Named Entities (DANE) [8] to look up the certificate associated with S1 and confirm that the certificate it received through the HTTPS connection is valid and bound to S1. DANE builds on DNSSEC and requires DNSSEC validation to work.

Using DNS datasets to increase IoT transparency

A third opportunity is to use DNS queries as a data source to visualize and control what services IoT devices use that potentially process personal data. This would enable users to understand which resolvers their IoT device use (e.g., a public resolver or the resolver of the user's ISP) and if interactions between their devices take place directly or via remote services on the Internet (e.g., a light switch that receives on/off instructions from an app on a mobile phone via a remote service on the Internet [3]).

While today most users are unaware of the internal workings of IoT deployments and mostly cannot influence them, future regulation of the IoT may give users greater control over how their information is used, which would make support for IoT transparency a stronger requirement.

Risks to the DNS

IoT devices can serve as a platform for large-scale Distributed Denial of Service (DDoS) attacks [9][10]. While DDoS attacks are not new, some of the IoT's most important characteristics—billions of wildly heterogeneous deployed devices and autonomous device operation—make DDoS attacks both easier to launch and harder to contain. We consider two sources of DDoS attack risk in the IoT and refer to [1] for more details.

DNS-unfriendly programming at IoT scale

One cause of additional load on the DNS is IoT device engineers using the DNS naively. For example, after an update to iOS 6.0 in November 2012 [9], the TuneIn music app (a traditional Internet application) started transmitting one DNS query per second for domains of the form www.<random-string>.com, perhaps to regularly check for network connectivity. The mobile network operator that observed the event reported about 1,000 of these queries per second from about 700 iPhones.

The result was that the operator's DNS resolver cache grew to about 5 million entries (normally around 400K) and its memory consumption increased to around 10 GB (normally around 4 GB), leading the operator to classify the event as a DDoS attack on its resolver. The network operator was unable to block the traffic because the devices were also making normal DNS queries, and instead had to wait until a new version of the app was released, about three weeks later. In the IoT, such incidents can have adverse global effects on DNS (resolver) operations.

A contributing factor is that IoT device engineers rely on open source libraries that hide the details of networking functions from them. As a result, they are less familiar with how the DNS works and may be unaware that DNS-unfriendly programming can have Internet-scale effects.

Increased size and complexity of IoT botnets targeting the DNS

Another risk is IoT botnets, which are created when IoT devices (e.g., IP cameras and DVRs) are infected with malware which then hits the DNS (and other types of Internet infrastructure) with large coordinated DDoS attacks [10].

With the growth of the IoT, botnets are likely to grow to millions of devices and serve as launch pads for ever-larger DDoS attacks. Currently observed IoT botnets contain hundreds of thousands of bots (e.g., the Mirai botnet [10] with 400K-600K infected devices and the Hajime botnet [11] with around 400K infected devices), which can launch DDoS attacks that cripple services of large operators such as the name service provider Dyn and hosting provider OVH. Compounding the security threat are the 3 million open DNS resolvers reported by Shadowserver (Dec 2018) [12], which enable amplification of Mirai-sized DDoS attacks on the DNS by factors between 29 and 64 [13].

The complexity of DDoS attacks is also likely to increase. For example, the Hajime botnet has a churn (bots recruited into and leaving the botnet) of around 2K bots per 20-minute interval [11], which makes it very challenging to filter out botnet traffic based on IP addresses. Similarly, we expect that the propagation rate of botnets will increase. For example, the operators of the Hajime botnet rolled out a software update to exploit and infect Gigabyte Passive Optical Network (GPON) routers through a vulnerability that was published only 10 days earlier [11]. As a result, the number of Hajime infections jumped from around 60K to 93K in 31 hours [11].

An IoT botnet is more difficult to eradicate because it can be assembled from a much wider range of devices (e.g., different CPU architectures, hardware, and operating systems [11]). This makes it more difficult to reduce its size quickly and at scale, especially when IoT devices interact with people's physical environment and therefore require more painstaking repair for safety reasons. Another difference is that infections of IoT devices often stay undetected longer because IoT devices typically operate "in the background" and may not be evident to end-users (e.g., pressure sensors in floor tiles).

Challenges for the DNS and IoT ecosystems

Based on the risks and opportunities we discussed above, we identify 5 challenges for the DNS and IoT ecosystems (see Table 1), 3 of which we discuss here.

Developing a DNS security and transparency library for IoT devices

The first challenge is developing and maintaining an open source library that implements functions of DNS security for IoT devices (e.g., DNSSEC validation, DANE, and DoH/DoT); transparency and control of remote services with which their IoT devices interact; and other functions such as traffic obfuscation to hide the typical patterns of IoT devices with highly specific functions (e.g., the traffic pattern of light switches [3]) and automatic resolver failover.

Such a library would have to work with the most popular IoT operating systems (e.g., OpenWRT and RIOT) and CPU architectures (e.g., arm and mips [11]), and with the more limited resources of typical IoT devices (e.g., limited battery power, CPU power, or capacity to perform cryptographic operations). It would also have to offer an API that enables IoT device engineers to easily include and use the library.

Potential starting points for development of such a library are Danish [14], which makes HTTPS DANE available on OpenWRT and the SPIN real-time visualizer for DNS query patterns of IoT devices [15].

Developing a system to share information on IoT botnets

Another challenge is to develop a system that enables DNS operators to automatically share the characteristics of the DDoS attacks they handle and how they handled them. This helps the operations teams of other DNS operators to more quickly write filtering rules or set up other measures in case the attack targets them, which is particularly important in the IoT because IoT botnets can grow quickly in size and can quickly vary the types of DDoS traffic they generate.

The system we envision contains entries for IoT botnets that have generated a significant amount of DDoS traffic (e.g., 500Gbps or more), with each entry describing the fingerprint of the DDoS traffic the botnet generates and configuration information that DNS operators have used to filter the botnet's traffic (e.g., filtering rules for different router platforms). The system could also combine measurements from different vantage points (e.g., different DNS operators) to track statistics such as concentrations of bots across autonomous systems and booter sites that sell attacks that use the botnet.

Potential starting points for implementing such a system are 3DCoP (DDoS Defense for a Community of Peers) [16] and the Dutch national DDoS clearing house [17]. The system should preferably be implemented in a fully distributed way (like 3DCoP) because it may become a target for DDoS attacks itself.

Proactive and flexible mitigation of IoT-powered DDoS traffic

A final challenge is to link the various DDoS mitigation systems that protect DNS operators and other Internet infrastructure operators in a flexible and synergistic way so they can quickly share DDoS mitigation capacity through a DDoS mitigation broker. This capability would help an individual operator who can no longer handle a DDoS attack on their own and must quickly scale up its mitigation capacity through third parties (e.g., its upstream transit providers). Such scenarios become possible with the DDoS Open Threat Signaling (DOTS) protocol [18], which enables a network to signal to another organization that it needs additional DDoS mitigation capacity. We envision such collaborative DDOS mitigation systems will be important because IoT botnets enable complex and amplified DDoS attacks that can grow to several hundred thousands—and in the future perhaps millions—of infected devices within hours, and are difficult to eradicate.

In parallel, we envision security systems in edge networks (e.g., on home gateways) that automatically block traffic from local devices that appear to have now become part of a botnet based on a specified traffic profile learned of a priori (e.g., using DDoS fingerprints). This would proactively stop IoT-powered DDoS attacks close to the source, reducing the volume of DDoS traffic that DNS operators would have to handle. Traffic blocking requires functions like distributed traffic measurements in edge networks, anomaly detection, and interactions with users when a security system has temporarily blocked one of their devices.

Implementations can use Manufacturer Usage Descriptions (MUDs) for IoT devices [19], which enable edge security systems to whitelist a device's normal behavior and block all other traffic, such as outbound DDoS traffic. Examples of emerging security systems for edge networks are SPIN [15] and the Secure Home Gateway project [20].

Conclusions

The expectations that IoT technology will produce a smarter, safer, and more sustainable society are extraordinarily high. While they may come true, we recommend complementing such optimism with a recognition of the reality of the also extraordinary safety and privacy risks to society that this technology brings. The opportunity for the DNS is that it is a globally pervasive infrastructure that can help addressing these risks, although the IoT also poses a risk for the DNS itself. Several challenges lie ahead to seize these opportunities and to address the risks, which will at the very least require cooperation across the IoT and DNS communities, both in terms of research as well as operations.

Acknowledgements

SIDN and the University of Twente were partly funded by the European Union's Horizon 2020 Research and Innovation program under Grant Agreement No. 830927. Project website: https://www.concordia-h2020.eu/

References

[1] T. April, L. Chapin, kc claffy, C. Hesselman, M. Kaeo, J. Latour, D. McPherson, D. Piscitello, R. Rasmussen, and M. Seiden, "The DNS and the Internet of Things: Opportunities, Risks, and Challenges", SSAC report SAC105, June 2019, https://www.icann.org/en/system/files/files/sac-105-en.pdf

[2] K. Rose, S. Eldridge, and L. Chapin, "The Internet of Things: an Overview", ISOC, Oct. 2015, http://www.internetsociety.org/sites/default/files/ISOC-IoT-Overview-20151221-en.pdf

[3] N. Apthorpe, D. Reisman, N. Feamster, "A Smart Home is No Castle: Privacy Vulnerabilities of Encrypted IoT Traffic", Workshop on Data and Algorithmic Transparency (DAT '16), New York University Law School, November 2016, https://arxiv.org/abs/1705.06805

[4] T. Böttger, F. Cuadrado, G. Antichi, E. Leão Fernandes, G. Tyson, I. Castro, and S. Uhlig, "An Empirical Study of the Cost of DNS-over-HTTPS", IMC'19, Oct. 2019, Amsterdam, the Netherlands

[5] J. Livingood, M. Antonakakis, B. Sleigh, and A. Winfield, "Centralized DNS over HTTPS (DoH) Implementation Issues and Risks", Internet Draft, March 2019, https://www.ietf.org/id/draft-livingood-doh-implementation-risks-issues-03.txt

[6] E. Osterweil, M. Ryan, D. Massey, and L. Zhang, "Quantifying the Operational Status of the DNSSEC Deployment", Internet Measurement Conference (IMC'08), Vouliagmeni, Greece, Oct. 2008, https://irl.cs.ucla.edu/papers/imc71-osterweil.pdf

[7] "BGP Leaks and Crypto Currencies", Blog, April 2018, https://blog.cloudflare.com/bgp-leaks-and-crypto-currencies/

[8] P. Hoffman, J. Schlyter, "The DNS-Based Authentication of Named Entities (DANE) Transport Layer Security (TLS) Protocol: TLSA", RFC6698, Aug 2012, https://tools.ietf.org/html/rfc6698

[9] G. Choules, "Cache Attacks", DNS-OARC Spring Workshop, Dublin, May 2013, https://indico.dns-oarc.net/event/0/contributions/3/

[10] M. Antonakakis, T. April, M. Bailey, M. Bernhard, E. Bursztein, J. Cochran, Z., Durumeric, J. A. Halderman, L. Invernizzi, M. Kallitsis, D. Kumar, C. Lever, Z. Ma, J. Mason, D. Menscher, C. Seaman, N. Sullivan, K. Thomas, and Y. Zhou, "Understanding the Mirai Botnet", 26th USENIX Security Symposium, 2017, https://www.usenix.org/system/files/conference/usenixsecurity17/sec17-antonakakis.pdf

[11] S. Herwig, K. Harvey, G. Hughey, R. Roberts, and D. Levin, "Measurement and Analysis of Hajime, a Peer-to-peer IoT Botnet", Network and Distributed Systems Security (NDSS) Symposium 2019, San Diego, CA, USA, February 2019

[12] Open Resolver Scanning Project, https://dnsscan.shadowserver.org/

[13] C. Rossow, "Amplification Hell: Revisiting Network Protocols for DDoS Abuse", Network and Distributed System Security Symposium, NDSS 2014, San Diego, USA,https://www.ndss-symposium.org/ndss2014/programme/amplification-hell-revisiting-network-protocols-ddos-abuse/

[14] DANISH homepage, https://github.com/smutt/danish

[15] SPIN homepage, https://spin.sidnlabs.nl/en/
[16] J. Berkes and A. Wick, "DDoS Defense for a Community of Peers", Presentation, FloCon 2017, San Diego, USA, January 2017, https://resources.sei.cmu.edu/library/asset-view.cfm?assetid=497970
[17] C. Hesselman, "Collaboratively increasing the resilience of critical services in the Netherlands through a national DDoS clearing house", Triple-I Security Day at APRICOT2019, Feb 2019, https://www.sidnlabs.nl/downloads/presentations/collaborative%20ddos%20mitigation.pdf
[18] Dobbins, D. Migault, S. Fouant, R. Moskowitz, N. Teague, L. Xia, and K. Nishizuka, "Use cases for DDoS Open Threat Signaling", Internet Draft, draft-ietf-dots-use-cases-16, July 2018, https://www.ietf.org/id/draft-ietf-dots-use-cases-16.txt
[19] E. Lear, R. Droms, and D. Romascanu, "Manufacturer Usage Description Specification", RFC8520, March 2019, https://www.rfc-editor.org/rfc/rfc8520.txt
[20] CIRA Secure Home Gateway Homepage, https://cira.ca/cira-secure-home-gateway

Author bios

Cristian Hesselman directs SIDN Labs, the research team of the operator of the Netherlands' national top-level domain, .nl. His research focuses on increasing the trustworthiness of the Internet, for instance through large-scale infrastructure measurements and the design of transparent and secure future networks. Cristian is a member of SIDN's leadership team, member of the Security and Stability Advisory Committee (SSAC) at ICANN, part-time associate professor at the University of Twente, and chair of the board of directors at NLnet Labs. He holds a Ph.D. (2005) and an M.Sc. (1996) in Computer Science from the University of Twente, the Netherlands. He can be reached at cristian.hesselman@sidn.nl.

Merike Kaeo is the CEO and Chief Security Strategist of Double Shot Security. Her professional interests include cyber defense from a policy, legal and technical perspective, including a focus on international cyber norms. She has an MSEE from the George Washington University and is a member of the IEEE. She is a member of ICANN's Security and Stability Advisory Committee (SSAC) and has been appointed to serves on the ICANN Board of Directors as the SSAC liaison. Contact email: merike@doubleshotsecurity.com.

Lyman Chapin is a co-founder of Interisle Consulting Group, LLC, where he advises companies, non-profit organizations, and government agencies on Internet technology, policy, and governance, network security and resilience, and critical infrastructure protection. Before starting Interisle in 2003 he was a Chief Scientist at BBN Technologies. Mr. Chapin is a Life Fellow of the IEEE, and was a founding trustee of the Internet Society. He has served as a Director of the Internet Corporation for Assigned Names and Numbers (ICANN), where he currently serves as a member of the Security and Stability Advisory Committee (SSAC), and as

chairman of the Internet Architecture Board (IAB) and the ACM Special Interest Group on Data Communication (SIGCOMM). Email: lyman@interisle.net.

Kimberly Claffy ("kc claffy") is founder and director of the Center for Applied Internet Data Analysis (CAIDA), a resident research scientist of the San Diego Supercomputer Center at UC, San Diego, and an Adjunct Professor in the Computer Science and Engineering Department at UC, San Diego. Her research interests span Internet topology, routing, security, economics, future Internet architectures, and policy. She leads CAIDA research and infrastructure efforts in Internet cartography, aimed at characterizing the changing nature of the Internet's topology, routing and traffic dynamics, economics, and investigating the implications of these changes on network science, architecture, infrastructure security and stability, and public policy. kc has been a member of the Security and Stability Advisory Committee (SSAC) since 2003. She has been at SDSC since 1991 and holds a Ph.D. in Computer Science from UC San Diego. Email: kc@caida.org

Mark Seiden has been a programmer since the '60s, has worked with diverse companies and research organizations in network and OS security and software engineering. He is Security Advisor to the Internet Archive, and frequent expert in computer crime cases, a participant in multiple (US) National Academy of Sciences studies, and a member of ICANN SSAC. His Erdos number is 3. Contact email: mis@seiden.com.

Danny McPherson is Executive Vice President and Chief Security Office at Verisign, where he is responsible Verisign's information systems, services, and security. Prior to joining Verisign, McPherson has held technical leadership positions with Arbor Networks, Qwest Communications, MCI Communications, and the U.S. Army Signal Corps. McPherson is an active contributor in the network, security, operations, and research communities and has authored several books, numerous Internet protocol standards, network and security research papers, and other publications. He is currently a member of ICANN's SSAC and the FCC's CSRIC, and has served on the IAB and IRSG, and chaired an array of IETF and other working groups and committees in these and related forums.

Dave Piscitello is a partner at Interisle Consulting Group, LLC, where he investigates cyber threats generally and cybercrime with a DNS nexus particularly. Dave holds a BS in mathematics from Villanova University. Dave is a member of the Boards of Directors of the AntiPhishing Working Group and the Coalition Against Unsolicited Commercial Email. He was awarded the Mary Litinski Lifetime Achievement Award by the Messaging, Malware, and Mobile Anti-Abuse Working Group. Dave has served on the IETF IESG and ICANN SSAC and remains involved in secure and transparent Internet policy and legislation activities. Email: dave@interisle.net

Andrew McConachie supports the Security and Stability Advisory Committee (SSAC) and the Root Server System Advisory Committee (RSSAC) as a member of ICANN's policy support staff. His professional interest is in socioeconomic and policy aspects

of Internet infrastructure. He has a Bachelor of Computer Science from James Madison University and a Master of Information Management and Systems from UC Berkeley. His contact email is andrew.mcconachie@icann.org.

Tim April works for Akamai Technologies as a Principal Architect in its Information Security department. In his time there, Tim has served as a consulting security architect for the groups responsible for Akamai's DNS Services and Infrastructure, the company's Networking team and various other groups throughout the organization. He holds a Masters of Science in Electrical Engineering from the University of New Hampshire. Tim is also a member of the ICANN Security and Stability Advisory Committee (SSAC). Email: tim@tapril.net.

Jacques Latour is chief technology and security officer for the Canadian Internet Registration Authority (CIRA). His professional interests include innovation on cybersecurity, DNS and new IoT security technologies. He is a member of the Internet Corporation for Assigned Names and Numbers (ICANN) Security and Stability Advisory Committee (SSAC) and is actively engaged in a number of multi stakeholder cybersecurity initiatives. Contact email: Jacques.latour@cira.ca.

Rod Rasmussen is a retired cybersecurity executive, who is now investing in and advising start-ups but spends the bulk of his work time volunteering for cybersecurity related organizations. This includes chairing ICANN's Security and Stability Advisory Committee (SSAC), serving as a member of the leadership of the Anti-Phishing Working Group (APWG) and participation in other industry organizations including M3AAWG, FIRST, and DNS-OARC. Contact email: rod@r2cyber.com