
Security in the Spotlight: A Recap of IDS 2019

OCTO-001

12 July 2019

The third annual ICANN DNS Symposium (IDS), a two-day event focused on all aspects of the Domain Name System (DNS) operations, was held 10-11 May in Bangkok, Thailand. Organized by ICANN's Office of the Chief Technology Officer (OCTO), this year's theme was **"Understanding the Security, Stability, and Resiliency of the DNS"**.

Opening Keynote Speeches

Internet Hall of Fame inductee Professor Kanchana Kanchanasut kicked off IDS 2019 with a keynote reviewing the 30-year history of the DNS in Thailand. Dr. Kanchana chronicled the successful implementation and growth of both the .th top-level domain and its local language Internationalized Domain Name (IDN) variant .ไทย. She described the challenges Thailand now faces with scaling and security. Next, Professor David Dagon of the Georgia Institute of Technology's School of Electrical and Computer Engineering gave a keynote on how the DNS is being used not just to map semantic names to IP addresses, but to map DNS queries to individuals through protocols such as EDNS Client Subnet (ECS). The ECS protocol was intended to allow content providers to determine roughly where topologically the DNS question originates in order to provide an answer pointing to the content server closest to the end user. Instead, DNS operators are using data from misconfigured (or badly implemented) ECS to pinpoint individual end user IP addresses.

IDS 2019: Day One

The first day of IDS 2019 featured presentations on Domain Name System Security Extensions (DNSSEC): Fernando Lopez from *Universidad Nacional de La Plata* in Argentina talked about his work implementing DNSSEC on very small UNIX devices such as a Raspberry Pi, while Phil Roberts from Diamond Key Security explained his multi-year effort to develop an open platform Hardware Security Module (HSM) to store DNSSEC keys.

Continuing the security theme of IDS 2019, Jacques Latour gave an update on CIRA's project intended to create a security framework for home Internet of Things (IoT) devices, in hopes of preventing "the light bulbs in our homes from taking down the Internet". Jim Reid provided an update on the potential impact of the United Kingdom's "Security of Network & Information Systems" (NIS) Directive on the DNS, which is intended to improve cybersecurity across the European Union. Jim addressed the difficulty of formally defining the parts of the DNS that are critical to national security interests as outlined in the directive.

Alexander Mayrhofer of nic.at detailed his ongoing efforts to measure the impact that individual domains have through his DNS Magnitude platform. Petr Špaček from CZ.NIC introduced a new open-source tool which automates basic debugging and helps to quickly uncover DNS-related problems in client networks. And taking a step back and looking at the bigger picture, João Damas from APNIC gave a presentation on the increasing centrality of recursive resolvers, showing that Google Public DNS was responding to about 33% of queries, with other very large public DNS operators also capturing noticeable percentages of DNS traffic.

Day one ended with a group discussion about when and how IANA Root Zone Management should perform the next rollover of the root zone key signing key (KSK). As is usual for this topic, discussion was lively with many differing opinions on the value of rolling the KSK, the frequency with which the KSK should be rolled, and the need for a potential standby key. The audience also touched on the possibility of changing the cryptographic algorithm used to generate a new key.

IDS 2019: Day Two

Day two of IDS 2019 kicked off with a series of presentations on combating cybercrime that exploits the DNS. The day began with a keynote speech by Stewart Garrick from Shadow Server, who described the tremendous efforts his team made in helping coordinate the takedown of the Avalanche botnets.

Joe Wein from SURBL detailed how to use reputation data from spam traps, zone file analysis, query mining, and other data sources to compile domain reputation lists to aid filtering malicious domains. A different way of combating malicious behavior uses Response Policy Zones (RPZs) developed by and discussed at IDS by Paul Vixie of Farsight Security. RPZs allow DNS operators to stop bad actors from using their DNS infrastructure as a weapon.

ICANN's Samaneh Tajalizadehkhoob talked about the current status of the Domain Abuse Activity Reporting (DAAR) project, a monthly report compiled by ICANN classifying the different types of abuse originating from gTLDs, while Ralf Weber from Akamai presented his team's measurements of abuse from different TLDs. Carel Bitter from Spamhaus presented three case studies that show how cyber criminals are using very large portfolios of domain names to wreak havoc on end users. Bitter also presented how weaknesses in DNS infrastructure contribute to phishing abuse. Bill Woodcock from Packet Clearing House gave a post mortem on the "DNSpionage" attacks from late 2018.

DNS over HTTPS (DoH) was also a topic at IDS 2019. Vittorio Bertola from Open-Xchange highlighted the pros and cons of DoH's possible implementations, while Andrew Fidler from BT detailed his company's challenges in providing end user support for DoH. Paul Vixie returned to the stage and presented his thoughts on applications doing DNS. Paul Hoffman from ICANN then moderated a panel discussion on DoH.

Wrap-up

A full house of 164 attendees from all over the world enjoyed IDS 2019. After the event, we surveyed the attendees, and found that over 90% were satisfied or very satisfied with the meeting. They expressed a high level of satisfaction with the quality of the agenda and valued the excellent opportunity to spend a few days networking and problem solving with DNS experts and operators. The topic of greatest interest was the panel on DoH deployment, and many respondents indicated that want to hear more about security in future IDS events.

If you missed this year's event, you can still read more about all the topics above: the presentation materials are available at <https://www.icann.org/ids>. See you at IDS 2020!

