Technical Study Group: DNS Security Facilitation Initiative

Purpose

The DNS Security Facilitation Initiative Technical Study Group (DSFI-TSG) is responsible for providing technical expertise and guidance on the technical work ICANN can initiate to investigate possible DNS security facilitation functions that ICANN can initiate. The DSFI-TSG is charged with providing recommendations to the ICANN CEO on ways to establish and promote best practices, facilitate communication between ecosystem participants, and implement processes to help stakeholders handle threats.

These recommendations will involve discussion and consultation with relevant stakeholders. Policy-related issues and technical areas not related to DNS security are out of scope.

Background

Attacks on the Domain Name System (DNS) rarely impact only one actor in the Internet ecosystem. With significant recent attacks such as the Sea Turtle hijacking and the DNSpionage, along with other attacks such as protocol-level attacks and common implementation vulnerabilities to the background (e.g., NSNX Attack), we see an urgent need to collaborate and respond. The solution, or solutions, that would best improve the security and stability of the DNS ecosystem are not yet clear; however, it is clear that a new level of collaboration and understanding is required.

In line with the FY21-FY25 Strategic Plan, ICANN org committed to work with the community to investigate mechanisms to strengthen collaboration and communication on security and stability issues through a technical study group (TSG). This TSG will explore ideas around what ICANN can and should be doing to improve the level of collaboration and engagement with DNS ecosystem stakeholders to improve the security profile for the DNS.

Assumptions

This section documents the context of the DSFI-TSG, which establishes where specific considerations drive the decisions of what is in and out of scope.

- Theoretical attacks are unlikely to result in concrete recommendations. However, any recommendations that the DSFI-TSG makes will have to take into account the evolving landscape and must be able to adjust over time.
- The recommendations will be based on the mechanics of broad security issues.

- Any recommendations made to ICANN will attempt to avoid conflicting with ICANN bylaws.
- Although the DSFI-TSG's recommendations are to the ICANN CEO, they may require work/implementation from the broader set of stakeholders.
- Recommendations will span multiple areas and may include, but are not limited to, best practice, information sharing, and incident response considerations.
- This group will not make policy, but it may make recommendations that policy changes may need to be considered.
- There are other dependencies to the DNS (e.g., routing) that may impact our recommendations.
- This group will not focus on the content of the attacks but will focus on the mechanism by which the attack is carried out.

If future changes to this charter are necessary as a result of discovering unknown-unknowns, the charter will be revised and versioned as needed.

Key Questions

The DSFI-TSG will explore, analyze, and make recommendations that address gaps in the current DNS security landscape:

1. What are the mechanisms or functions currently available that address DNS security?
2. Can we identify the most critical gaps in the current DNS security landscape?
    a. What are the technical requirements needed to address the gaps?
    b. What operational best practices need to be developed, modified, promoted, or implemented to address the gaps?
    c. What are hindrances to deployments of best practices and other technical measures?
3. Who is best suited to fill those gaps?
    a. Is there a role for ICANN org here? Where can ICANN org facilitate improvements to the DNS security landscape?
    b. What strategic partnerships should ICANN org make to enhance DNS security?
4. What are the risks associated with these gaps that may not be well understood?
    a. What are the risk considerations?
    b. Where are there gaps in knowledge of the threat models to the DNS ecosystem?
    c. What externalities do people need to be aware of?
5. Does the DNS have unique characteristics that attract security problems, which other Internet services don't have?
    a. What can we learn from other protocols or industries that face similar issues (e.g., critical infrastructure industries)?
    b. How can we improve on any existing practices?

Scope

The Technical Study Group will focus on providing recommendations that may have a positive effect on managing the following areas:

Identity Management
Threats that rely on an entity asserting its identity through some means. Topics will include credential management lifecycle processes, identity management, and social engineering factors.

Availability
All threats that have an impact on the ability to provide reliable responses to DNS queries will fall under this category. It may include route hijacking as well as DDoS either against or leveraging (reflection or forwarding) DNS infrastructure (where infrastructure encompassed DNS authoritative servers, recursive DNS servers, DNS forwarders, and provisioning systems).

Infrastructure Impersonation
Threats that impersonate DNS Infrastructure (DNS authoritative servers, recursive DNS servers, DNS forwarders).

Vulnerabilities
This area includes threats / flaws of software and hardware implementations, deployment configurations, protocol design as well as side-channel attacks that can cause information leakage or put software into a state of exposing vulnerabilities.

Fate Sharing
Threats that create areas of weakness due to the homogeneity of the overall architecture, deployment, or system.

Security Threats That Utilize the DNS
Many threats actively utilize the DNS infrastructure or DNS data. These include various forms of malware that redirect queries, falsify queries, and create means of utilizing the DNS for the exfiltration of private and confidential data. Also includes threats where DNS is used as a DDoS amplification tool.

Verifying/Validating trust in the DNS Infrastructure and Data
Some threats are realizable due to a lack of focus on validating deployment architectures and configurations. This encompasses root zone and registration system operations as well as validation of the integrity and reliability of all DNS infrastructure components.

Cryptography

With the increased dependency on cryptographic solutions to preserve the integrity, confidentiality, and non-repudiation of DNS data and operations, threats related to DNSSEC key compromise and other cryptographic nuances will be discussed.

Team Composition

The DNS Facilitation Function Steering Committee is made up of ICANN executives and members of the ICANN Board. The committee will advise on strategic direction, oversee the development of a clear charter, and provide guidance on appropriate protocol and approval to facilitate project progress.

Role	Name
Coordinator	Merike Käo
Steering Committee	Board: Harald Alvestrand Danko Jevtovic Merike Käo ICANN org: Göran Marby, President and CEO David Conrad, SVP & Chief Technology Officer Ashwin Rangan, SVP, Engineering & Chief Information Officer
Team Members	Tim April Gavin Brown John Crain Rod Rasmussen Marc Rogers Katrina Sataki Robert Schischka Duane Wessels
ICANN Org Support Team	Sally Newell Cohen (communications) Steven Kim (project management) Heather Flanagan (technical writer) Wendy Profit (project management support)

Deliverables

The group aims to recommend next steps for the ICANN community and ICANN org by May 2021.

Deliverable

Seat the DSFI-TSG
Finalize Charter and Scope
Draft DSFI-TSG Recommendations
Final DSFI-TSG Recommendations