DNS Security Facilitation Initiative Technical Study Group (DSFI-TSG) Panel Discussion

Merike Käo (Coordinator)
Tim April
Gavin Brown
John Crain
Robert Schischka
Duane Wessels

25 May 2021

ICANN

Agenda

- Introduction
- The Work
- Attack Vectors
- Mitigation Techniques
- Next Steps
- Q&A

Introducing the DSFI-TSG

DSFI - TSG

In line with the FY21-FY25 Strategic Plan, ICANN org committed to work with the community to strengthen collaboration and communication on security and stability issues through a technical study group (TSG). In May 2020, the ICANN CEO established the Domain Name System Security Facilitation Initiative – Technical Study Group to:

Provide technical expertise and guidance on the technical work ICANN can initiate to investigate possible DNS security facilitation functions ICANN can initiate.

Provide recommendations on ways to:

- Establish and promote best practices
- Facilitate communication between ecosystem participants
- Implement processes to help stakeholders handle threats

The recommendations will involve discussion and consultation with relevant stakeholders to address the important questions:

- What can and should ICANN be doing to improve DNS security profile?
- What should ICANN NOT be doing?

The Team (Technical Study Group)

The Team

TECHNICAL STUDY GROUP

Merike Käo – Coordinator

- Chief Information Security Officer (CISO) of Uniphore
- Security and Stability Advisory Committee (SSAC) Liaison to the ICANN Board of Directors

Tim April

- Principal Architect, Akamai Technologies

Gavin Brown

- Head of Registry Services and Chief Innovation Officer, CentralNic

John Crain

- Chief Security, Stability and Resilience Officer, ICANN Org

Rod Ramussen

- Chair of ICANN SSAC, and retired Security Executive

Mark Rogers

- Vice President of Cybersecurity, Okta

Katrina Sataki

- Chief Executive, NIC.LV (Latvia) and Council member of the country code Names Supporting Organization (ccNSO)

Robert Schischka

- Chief Executive Officer, NIC.AT (Austria) and Director of the Computer Emergency Response Team (CERT.at)

Duane Wessels

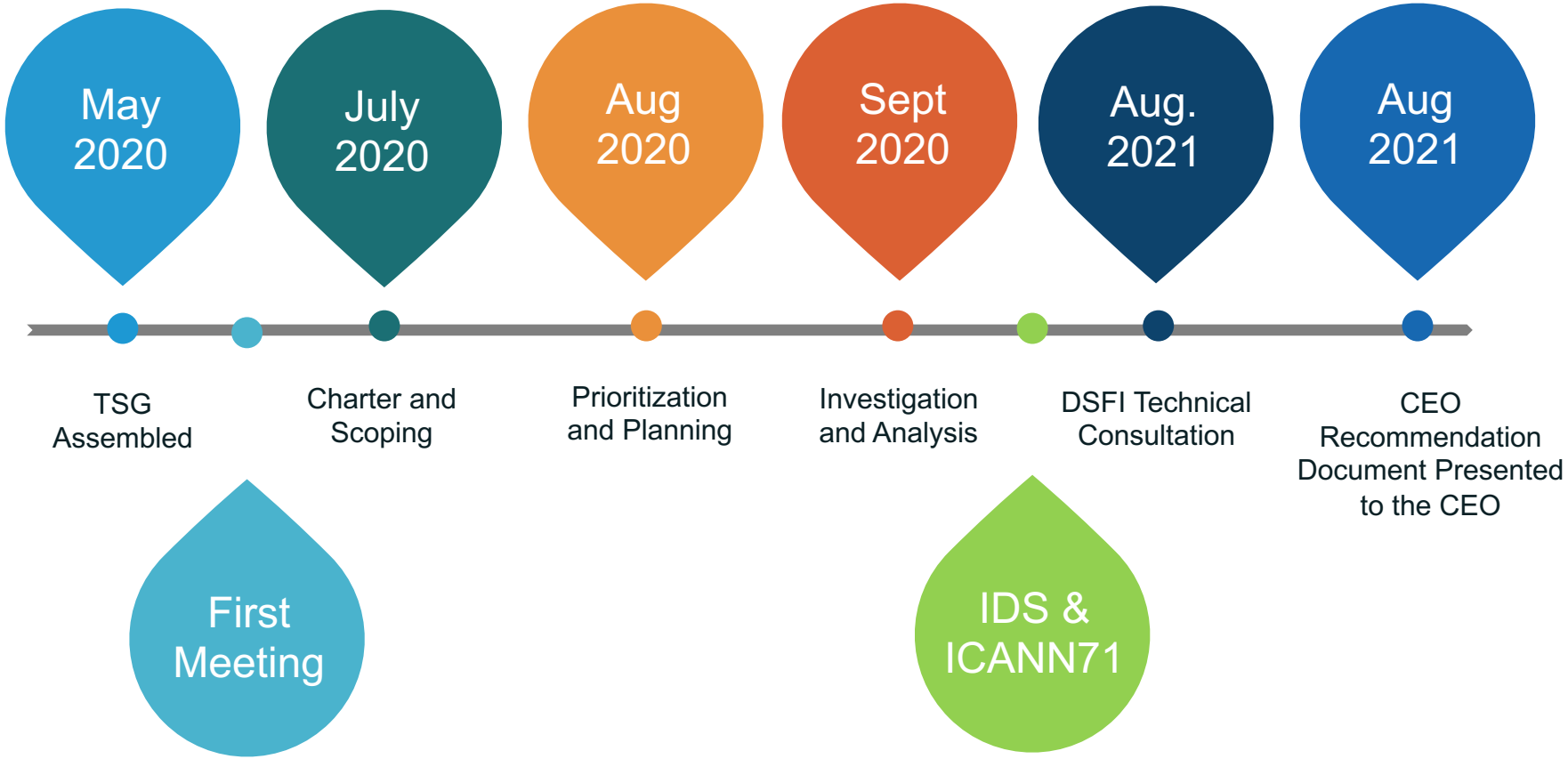
- Distinguished Engineer, Verisign

The Team

DSFI ICANN SUPPORT

ICANN BOARD	ICANN Org	ICANN Staff Support	Technical Writer (Consultant)
• Harald Alvestrand • Göran Marby • Danko Jevtovic • Merike Käo	• David Conrad • Ashwin Rangan	• Steven Kim • Sally Newell Cohen • Wendy Profit • Samaneh Tajalizadehkhoob	• Heather Flanagan

Timeline


May 2020
July 2020
Aug 2020
Sept 2020
Aug. 2021
Aug 2021
TSG Assembled
Charter and Scoping
Prioritization and Planning
Investigation and Analysis
DSFI Technical Consultation
CEO Recommendation Document Presented to the CEO
First Meeting
IDS & ICANN71

The Why

- There have been alarming attacks on the Domain Name System
  - The Sea Turtle hijacking
  - DNSpionage
  - DNS Changer
- These attacks rarely impact only one actor in the Internet ecosystem, and we need to come together and respond.
- The solution, or solutions, that would best improve the security and stability of the DNS ecosystem are not yet clear.
- A new level of collaboration and understanding is required

ATTACK VECTORS

Attack Vectors – Some Relevant Examples

DNSSec = Secure DNS?

- DNS is a complex ecosystem which involves many parties in different roles
- A lot of work has been done to make DNS protocol more resilient against spoofing or manipulation of DNS answers in general

But:

- DNSSec deployment still leaves a lot to be desired
- Also, the level of protection provided by signing data is often not fully understood
- Real world attacks show that sometimes proper DNSSec deployment might have helped to easier detect anomalies ...
- …. but also, that DNSSec is not the silver bullet to make DNS a system invulnerable to attacks
- Importance of DNS is not always clear to people outside the industry

Attack Vectors – Some Relevant Examples

Credential Compromise

Attacking the authentication layer is a common pattern in all sorts of real world cybercrime scenarios. Phishing or brute-forcing of password, social engineering, key-logger etc.

- All authentication systems which are not protected by MFA are subject to this kind of attacks and even attacks against MFA protected accounts are growing.
- The complex relations between
  - Registry - Registrar - Reseller(s) - Domain holder
  - and other involved parties: DNS Service Provider, Webhoster, makes this even more hard to solve

Attack Vectors – Some Relevant Examples

Fraudulent Certificates

- Certificates are among the most important sources of trust for websites and other services. Also, because they are to some degree displayed to the end user and are more or less well understood - better than a lot of other security measures.
- Therefore, it is no surprise that a lot of attacks use fraudulent certificates obtained in various ways.
- Manipulation of the DNS is one way to successful attack the certificate issuing process - so DNS is not always the main goal but very often a necessary step for the ultimate target
- Esp. true for supply chain attacks

Attack Vectors – Some Relevant Examples

Route Hijacking - BGP Based Attacks

- BGP - has not been designed with a security focus in mind (sounds familiar?)
- A high level of implicit trust between peers leads to design which makes it easy to inject false routing announcements - either per accident and also on purpose.
- Some examples of different attacks
  - Man in the middle, credential harvesting,
  - Server impersonation, etc) especially if there is a lack of appropriate authentication on applications relying on correct routing.
  - DNS traffic could be rerouted -> impersonate DNS Servers
  - Traffic for certificate request validation etc.
- Similar to the some “DNS attacks” this might be an intermediate goal to reach a final target

Attack Vectors – Some Relevant Examples

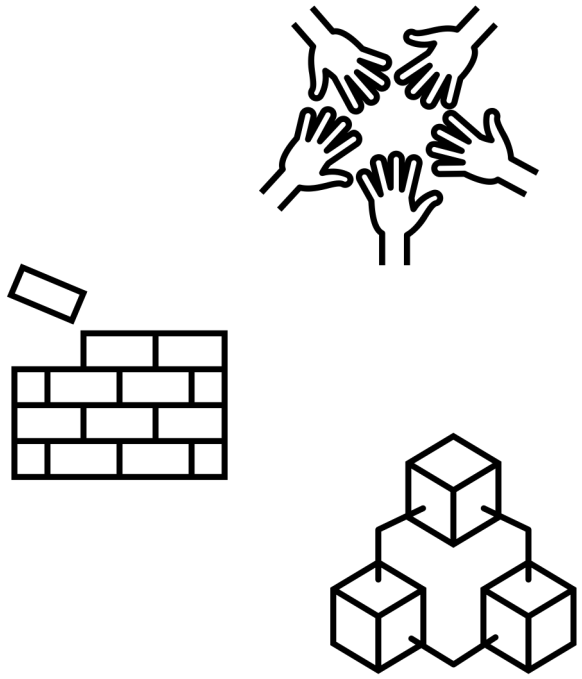
DNS as a Covert Channel

- DNS is usually considered a “legitimate protocol” in almost every network setup and use case
- Even in tightly managed environments it is common that DNS queries are allowed for all clients and answers are rarely parsed at the firewall other than for protocol correctness
- Therefore the DNS protocol is a “good choice” for usage as a cover channel - eg. for communication with command and control servers of a botnet, but also more sophisticated scenarios for data leakage has been observed in the real world
- Strictly spoken this not an attack ON the DNS, but again a pattern make use OF the ubiquity of DNS resolution and the central role it plays in today’s infrastructure

MITIGATIONS

MITIGATIONS

Mitigation Scope



- The TSG has considered many mitigations which could be used to counter the attacks described.
- Not all mitigations will make it into the final report.

MITIGATIONS

Authentication

- Complex Passwords
- One-time Use Credentials
- MFA
- Password Manager
- Risk Awareness (Credential)
- Use of Services that Prevent Weak Passwords
- Existence of Remedial Solutions in Case of Attack
- Domain & Registrant Verification & Validation

MITIGATIONS

Availability, Integrity, Privacy

- Availability
  - Avoid DNS Service Behind a Single Point of Failure
  - Secondary DNS Services with Different Platforms
- Integrity
  - DNSSEC
  - Registry Lock to prevent domain hijacking
  - Use of CDS/CDNSKEY/CSYNC
- Privacy
  - Use of Encrypted DNS Transport

MITIGATIONS

Monitoring & Trust, Software & System Safety

- Monitoring & Trust
  - Subscribing to Brand Protection Services
  - Monitor Certificate Transparency (CT)
  - Wider use of Certification Authority Authorization (CAA)
  - ROA Publication and Validation (RPKI)
  - Routers optimized for Packet Inspection, Frame Inspection
- Software and System Safety
  - Security Development Lifecycle (SDLC)
  - Patch Software Regularly

MITIGATIONS

Access Control

- Access Control
  - Behavior based access architectures (e.g., Zero-Trust)
  - Partition Critical Online Services (service segregation, e.g. email, website)
  - Consider alternate or more restrictive access controls for Sensitive Info/Accounts
  - Restrict access to DNS services to only DNS ports
  - Limit Resolver Use by 3rd Parties

MITIGATIONS

End Point & Network Controls

- End Point and Network Controls
  - Antivirus for End Users
  - Strict Control over DNS Resolver Selection
  - DNS Blocking/Redirecting via DNS Resolvers (DNS Firewall)
  - DNS Blocking/Redirecting via Perimeter Firewalls

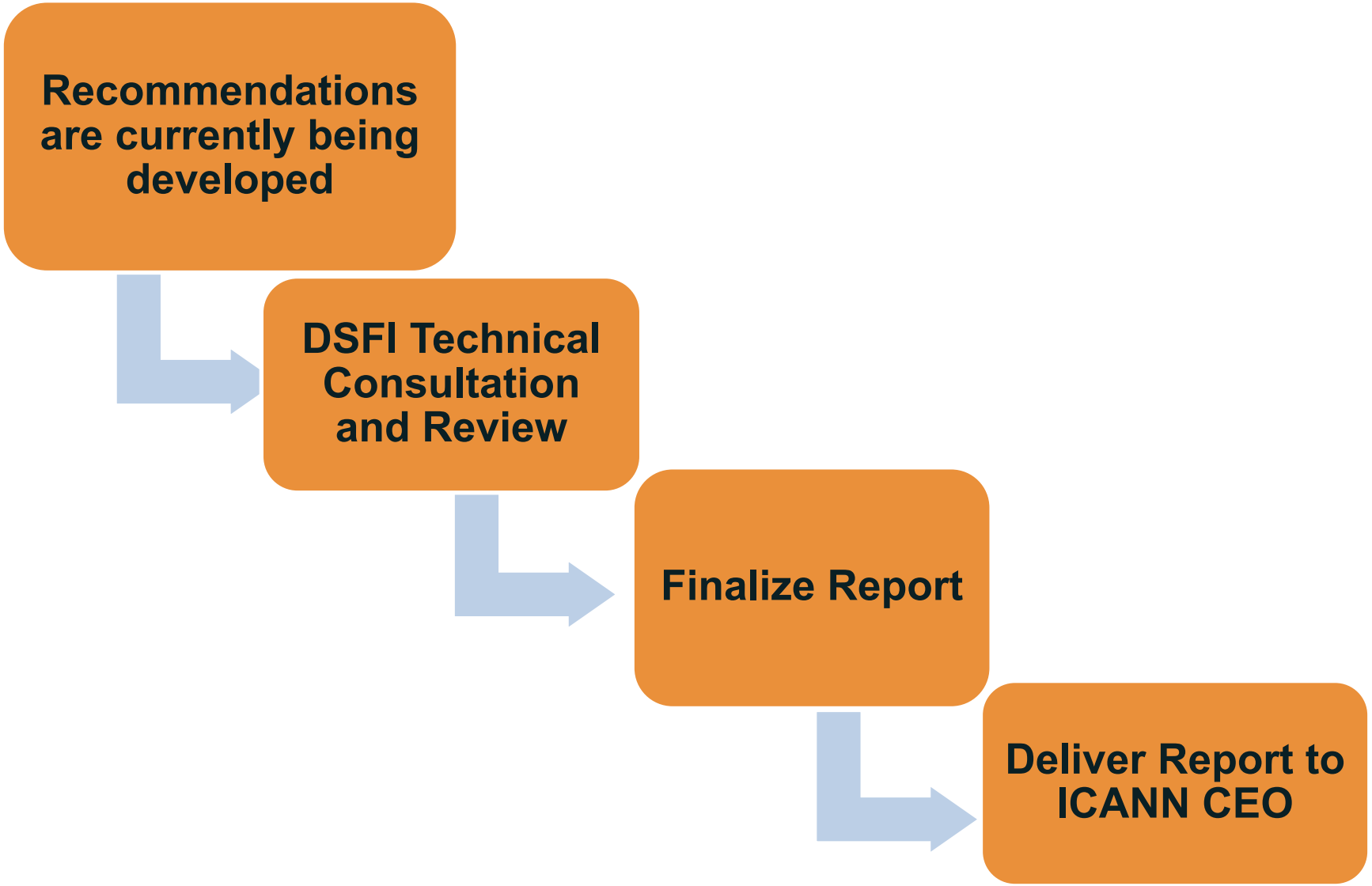
MITIGATIONS

Major Categories

- Credential Challenges
- Inadequate Access Control and Authorization Issues
- Resource Impersonation
- Code and Protocol Vulnerabilities
- Infrastructure Choices
- DNS as the Attack Vector
- Denial of Service
- Incident Response Mechanisms

NEXT STEPS

Next Steps


Recommendations are currently being developed
DSFI Technical Consultation and Review
Finalize Report
Deliver Report to ICANN CEO

For More Information

- Visit https://community.icann.org/display/DSFI

- DNS Security Facilitation Initiative Technical Study Group
  - Charter
  - Scoping document
  - Work plan and timelines
  - Meeting agendas and notes
  - Resources

Discussion