OECD publishing

SECURITY OF THE DOMAIN NAME SYSTEM (DNS)

AN INTRODUCTION FOR POLICY MAKERS

OECD DIGITAL ECONOMY PAPERS
October 2022 **No. 331**

OECD
BETTER POLICIES FOR BETTER LIVES

Foreword

This report on "Security of the Domain Name System (DNS): an Introduction for Policy Makers" was prepared jointly by the OECD Working Party on Security in the Digital Economy (WPSDE) and Working Party on Communication Infrastructure and Services Policy (WPCISP), of the Committee on Digital Economy Policy (CDEP). It aims to inform policy makers about the current challenges and opportunities related to the digital security of the Domain Name System (DNS). This report should be read in conjunction with the accompanying report on "Security of Routing".

This report was drafted by Ghislain de Salins with contributions from Laurent Bernat, Verena Weber and Lauren Crean from the OECD Secretariat, and by WPSDE and WPCISP delegates. It was prepared under the supervision of Laurent Bernat and Verena Weber. It was approved and declassified by written procedure by the Committee on Digital Economy on 22 August 2022, and prepared for publication by the OECD Secretariat.

The Secretariat wishes to thank the external experts who contributed to the development of this report including, inter alia: Joe Abley; Einar Bohlin; Stéphane Bortzmeyer (Afnic); Chris Boyer (AT&T); Chris Buckridge; Graeme Bunton (DNS Abuse Institute); Gemma Carolillo (European Commission); David Conrad (ICANN); Cameron Dixon (DHS); Patrik Fältström (Netnod); Laurent Ferrali (ICANN); Marco Hogewoning; Geoff Huston (APNIC); Anne-Rachel Inné; Merike Kaeo; Olaf Kolkman (ISOC); Elena Plexida (ICANN); Paul Rendek; Andrei Robachevsky (ISOC); Chelsea J. Smethurst (Microsoft); Mark Svancarek (Microsoft); Bill Woodcock (PCH), and Suzanne Woolf (PIR).

Note to Delegations:

This document is also available on O.N.E under the reference code:

DSTI/CDEP/CISP/SDE(2021)5/FINAL.

This document, as well as any data and any map included herein, are without prejudice to the status of or sovereignty over any territory, to the delimitation of international frontiers and boundaries and to the name of any territory, city or area.

@ OECD 2022

The use of this work, whether digital or print, is governed by the Terms and Conditions to be found at http://www.oecd.org/termsandconditions.

Table of contents

Figures

Boxes

Executive summary

The Domain Name System (DNS) is an essential logical infrastructure that enables the mapping of names and services on the Internet and underpins its very functioning. In fact, almost every activity on the Internet starts with a DNS query, i.e. a request for information sent by a user's machine to a DNS server. As a result, the impact of incidents affecting the DNS can be significant. They include digital security attacks, i.e. incidents caused intentionally by malicious actors (e.g. DNSpionage and the Sea Turtle DNS hijacking in 2018 and 2019), as well as unintentional incidents, for instance resulting from a misconfiguration that would make a DNS server unavailable (e.g. the Facebook outage in October 2021).

This report focuses on DNS security, i.e. the area of digital security that covers incidents disrupting the availability, integrity and confidentiality (the "AIC triad") of parts of the DNS ecosystem. It does not discuss areas beyond this scope such as certain forms of "DNS abuse".

Each actor in the DNS ecosystem, and each relationship between those actors, contain potential vulnerabilities that can be exploited by malicious actors or lead to an unintentional digital security incident. The report looks at three types of vulnerabilities whose exploitation may affect the AIC triad of the DNS ecosystem, as well as at the existing efforts and emerging solutions to address them:

- **"DNS-specific" vulnerabilities**, which result from flaws in the DNS protocol, its original design as well as its implementation, enabling for instance DNS spoofing and cache poisoning. Key technical developments to address those include DNS Security Extensions (DNSSEC) and encrypted DNS transport, e.g. DNS-over-TLS (DoT) and DNS-over-HTTPS (DoH).
- **Vulnerabilities of DNS actors**, which may result from code vulnerabilities, misconfigurations, insufficient access controls and the human factor (e.g. social engineering), and include supply-chain attacks that may compromise registries and registrars. Key initiatives to address those include the mainstreaming of registry lock and zero trust approaches across the DNS ecosystem.
- **Dependencies and emerging concentration,** which could have significant consequences for DNS security (e.g. single points of failure with the risk of cascading effects).

The analysis highlights six common misconceptions about the DNS ecosystem and DNS security:

- **First misconception: the DNS is *only* a phonebook for the Internet**. Beyond the protocol that enables the translation (or "resolution") of human-readable names into machine-readable IP addresses, the DNS is an essential infrastructure that provides stables references on the Internet.
- **Second misconception: the importance of the DNS is decreasing**. Mobile applications and emerging technologies such as the Internet of Things (IoT), like almost any activity on the Internet, extensively rely on the DNS ecosystem, the importance of which is increasing in line with the digital transformation.
- **Third misconception: the DNS is an easy-to-understand and highly centralised system managed by ICANN**. The DNS is a complex ecosystem that combines some centralised functions with a highly distributed structure, which relies on thousands of systems and organisations across the world as well as on interactions with other systems and protocols.

- **Fourth misconception: easy fixes are available to solve DNS security issues**. There are often trade-offs between digital security and other key economic and social objectives such as technical performance, usability or profitability. Even within the realm of DNS security, technical solutions such as DNSSEC and encrypted DNS transport come with trade-offs.
- **Fifth misconception: nothing can be done to enhance DNS security**. Many initiatives have been launched by the multi-stakeholder community to enhance DNS security. They include economic incentives to support DNSSEC deployment, tools to better measure DNS security and solutions to enhance the confidentiality of DNS queries and user privacy.
- **Sixth misconception: DNS security is only a technical issue calling for technical remedies**. Economic factors such as misaligned market incentives play a key role in DNS security gaps. While technical solutions are the most effective means to fix vulnerabilities in the DNS protocol itself, their implementation, or lack thereof, are interrelated with economic and social incentives affecting DNS actors.

The role of governments in enhancing the digital security of the DNS ecosystem

Because the DNS is a key infrastructure that supports the very functioning of the Internet, there is a need for governments to better understand and prioritise DNS security. Enhancing DNS security should be considered as a co-operative journey, and the efforts of the multi-stakeholder community in this direction as an on-going process of innovation to better mitigate risk, in a constantly evolving environment.

In general, digital security measures may impact one dimension of the AIC triad positively, while negatively impacting another. DNS security is no exception: there is no panacea that would make the DNS entirely secure, and promising technical solutions often come with trade-offs. For both policy makers and actors of the DNS ecosystem, effective digital security policies and measures should aim to reduce digital security risk to an optimal level rather than to avoid the risk or seeking to entirely eliminate it and achieve “100% security”. **Policy makers therefore need to exercise caution** when introducing policies or initiatives to enhance DNS security, in order to avoid well-intentioned but ill-designed regulations that may lead to adverse effects. In particular, policy makers could significantly benefit from:

- **Consulting the DNS multi-stakeholder community and co-designing initiatives** regarding DNS security with its members. In particular, governments could work together with their ccTLDs to better measure and incentivise the adoption of DNS security best-practices such as DNSSEC signing, and with local ISPs to further develop DNSSEC validation and the use of encrypted DNS transport in their DNS resolution services;
- **Leading by example** with their own DNS infrastructure (e.g. by deploying DNSSEC signing for the authoritative DNS servers managed by the government);
- **Supporting stakeholder-led initiatives** to develop capacity building on DNS security, in particular targeting smaller organisations such as certain Internet Service Providers (ISPs), ccTLDs and registrars;
- **Promoting diversification** of the DNS ecosystem and its supply chain, in particular through the development of alternatives for key functions (e.g. DNS management software or resolvers);
- **Supporting research and development** in areas where significant technical gaps for DNS security remain unaddressed.
- **Co-operating at the international level** to enhance the security of the DNS ecosystem, preserve its functioning as a core global infrastructure and avoid Internet fragmentation. In that regard, enabling an international and multi-stakeholder dialogue to better understand and address DNS security challenges is essential.