Technical Impacts of DNS Privacy and Security on Network Service Scenarios

ATIS-I-0000079 | April 2020

atis

Abstract

The domain name system (DNS) is a key network function used to resolve domain names (e.g., atis.org) into routable addresses and other data. Most DNS signalling today is sent using protocols that do not support security provisions (e.g., cryptographic confidentiality protection and integrity protection). This may create privacy and security risks for users due to on-path nodes being able to read or modify DNS signalling.

In response to these concerns, particularly for DNS privacy, new protocols have been specified that implement cryptographic DNS security. Support for these protocols is being rapidly introduced in client software (particularly web browsers) and in some DNS servers.

The implementation of DNS security protocols can have a range of positive benefits, but it can also conflict with important network services that are currently widely implemented based on DNS. These services include techniques to mitigate malware and to fulfill legal obligations placed on network operators. This report describes the technical impacts of DNS security protocols in a range of network scenarios. This analysis is used to derive recommendations for deploying DNS security protocols and for further industry collaboration. The aim of these recommendations is to maximize the benefits of DNS security support while reducing problem areas.

Foreword

As a leading technology and solutions development organization, the Alliance for Telecommunications Industry Solutions (ATIS) brings together the top global ICT companies to advance the industry's business priorities. ATIS' 150 member companies are currently working to address network reliability, 5G, robocall mitigation, smart cities, artificial intelligence-enabled networks, distributed ledger/blockchain technology, cybersecurity, IoT, emergency services, quality of service, billing support, operations and much more. These priorities follow a fast-track development lifecycle from design and innovation through standards, specifications, requirements, business use cases, software toolkits, open source solutions and interoperability testing.

ATIS is accredited by the American National Standards Institute (ANSI). ATIS is the North American Organizational Partner for the 3rd Generation Partnership Project (3GPP), a founding Partner of the oneM2M global initiative, a member of the International Telecommunication Union (ITU), as well as a member of the Inter-American Telecommunication Commission (CITEL). For more information, visit www.atis.org. Follow ATIS on Twitter and on LinkedIn.

Notice of Disclaimer and Limitation of Liability

The information provided in this document is directed solely to professionals who have the appropriate degree of experience to understand and interpret its contents in accordance with generally accepted engineering or other professional standards and applicable regulations. No recommendation as to products or vendors is made or should be implied.

NO REPRESENTATION OR WARRANTY IS MADE THAT THE INFORMATION IS TECHNICALLY ACCURATE OR SUFFICIENT OR CONFORMS TO ANY STATUTE, GOVERNMENTAL RULE OR REGULATION, AND FURTHER, NO REPRESENTATION OR WARRANTY IS MADE OFMERCHANTABILITY OR FITNESS FOR ANY PARTICULAR PURPOSE OR AGAINST INFRINGEMENT OF INTELLECTUAL PROPERTY RIGHTS. ATIS SHALL NOT BE LIABLE, BEYOND THE AMOUNT OF ANY SUM RECEIVED IN PAYMENT BY ATIS FOR THIS DOCUMENT, AND IN NO EVENT SHALL ATIS BE LIABLE FOR LOST PROFITS OR OTHER INCIDENTAL OR CONSEQUENTIAL DAMAGES. ATIS EXPRESSLY ADVISES THAT ANY AND ALL USE OF OR RELIANCE UPON THE INFORMATION PROVIDED IN THIS DOCUMENT IS AT THE RISK OF THE USER.

NOTE: The user's attention is called to the possibility that compliance with this standard may require use of an invention covered by patent rights. By publication of this standard, no position is taken with respect to whether use of an invention covered by patent rights will be required, and if any such use is required no position is taken regarding the validity of this claim or any patent rights in connection therewith. Please refer to [http://www.atis.org/legal/patentinfo.asp] to determine if any statement has been filed by a patent holder indicating a willingness to grant a license either without compensation or on reasonable and non-discriminatory terms and conditions to applicants desiring to obtain a license.

Copyright Information

Alliance for Telecommunications Industry Solutions
1200 G Street, NW, Suite 500
Washington, DC 20005

Table of Contents

1 Introduction

The domain name system (DNS) provides an essential function for distributed applications of resolving human-readable names into network routable IP addresses. As such, DNS provides a bridge between the application domain and the network domain. The ubiquitous nature of DNS means it has also become a platform for distributing application-specific information such as domain-based message authentication, reporting and conformance (DMARC) email security policy.

Given the key role that DNS plays in network routing and operation, the network domain has employed DNS in support of local services, network optimization, fulfillment of legal requirements and to enhance the online security of network users.

The dual role of DNS—as an internet-wide database and a network service function—potentially creates tension between application and network interests, with contrasting perspectives in different technical communities. Encrypted DNS protocols such as DNS over HTTPS (DoH) and DNS over Transport Layer Security (TLS) (DoT) are now being rolled out, which brings the different perspectives about the role of DNS into sharp focus. Encrypted DNS protocols can increase user privacy and security, but deployments should consider the public and private network impacts because they may have deleterious impacts on the overall network operation and robustness.

This report will identify some of the most important public and private network scenarios that involve DNS network features and analyze the technical impacts of DNS privacy protocols. The focus will be on the client-to-server (including stub-to-recursive-resolver) interface. Based on this analysis, recommendations for how to deploy and operate DoH and DoT will be generated.

2 Executive Summary

Client operating systems and applications are rapidly introducing support for the encrypted DNS protocols DoT and DoH. These protocols provide integrity protection and confidentiality for DNS requests and responses between the client and the responding DNS server. This can improve user privacy and security in all deployment scenarios. Encrypted DNS protocols are a useful addition to the network security toolkit.

Given the important and diverse role of DNS in network operations and policy enforcement, any changes to DNS behavior in clients should be studied for impacts on the complete networked system. Measures should be taken, if necessary, to maintain the best possible service. In the case of support for DoT and DoH, there are impacts on systems in three main areas:

- The absence of industry norms for how to deploy and operationalize encrypted DNS in servers and clients is leading to the adoption of piecemeal solutions that differ in each implementation. This is creating a confusing situation, which risks a range of service problems or security loopholes due to incompatible assumptions in different implementations. In some cases, this may lead to users finding services or devices that fail to operate. They may also find that there is no single point of contact capable of understanding and resolving service problems due to the complex interactions between the different components.
- Some clients are disregarding DNS server provisioning information received from the network, e.g., in Dynamic Host Configuration Protocol (DHCP), and instead selecting their own DNS servers. These clients can disrupt a range of network services, including security and legally