Network Working Group
Internet-Draft
Intended status: Informational
Expires: May 8, 2020

J. Arkko
Ericsson

November 05, 2019

Centralised Architectures in Internet Infrastructure
draft-arkko-arch-infrastructure-centralisation-00

Abstract

Centralised deployment models for Internet services and Internet business consolidation are well-known Internet trends, at least when it comes to popular and user-visible service. This memo discusses the impacts of similar trends within the Internet infrastructure, on functions such as DNS resolution.

Status of This Memo

This Internet-Draft is submitted in full conformance with the provisions of BCP 78 and BCP 79.

Internet-Drafts are working documents of the Internet Engineering Task Force (IETF). Note that other groups may also distribute working documents as Internet-Drafts. The list of current Internet-Drafts is at https://datatracker.ietf.org/drafts/current/.

Internet-Drafts are draft documents valid for a maximum of six months and may be updated, replaced, or obsoleted by other documents at any time. It is inappropriate to use Internet-Drafts as reference material or to cite them other than as "work in progress."

This Internet-Draft will expire on May 8, 2020.

Copyright Notice

Table of Contents

1. Introduction

Centralised deployment models for Internet services and Internet business consolidation are well-known Internet trends, at least when it comes to popular and user-visible service [ISOC] [I-D.arkko-iab-internet-consolidation] [I-D.arkko-arch-dedr-report]. This memo discusses the impacts of similar trends within the Internet infrastructure, on functions such as DNS resolution.

This memo has been inspired by recent attempts to move DNS resolution from large number of local servers to a more centralized arrangements, but the principles outlined in this document apply more generally to other basic Internet services.

Section 2 introduces the context of the memo, Section 3 discusses some potential issues, and Section 4 makes a recommendation.

2. Context

For the purposes of this discussion, "Internet Infrastructure" is defined as those parts of the technical Internet infrastructure that are needed to form a communication substrate for applications to run on. Applications are not a part of the infrastructure, they run on it. But packet forwarding, routing, naming as well as higher level functions such as certificate authorities are included; anything that is needed to establish an end-to-end HTTPS connection between host is part of the infrastructure. This also includes all Internet

technology that is needed for these part to work.

The DNS [RFC1035] is a complex system with many different security issues, challenges, deployment models and usage patterns. While there are many parts of the DNS system and they are all part of the

infrastructure that is needed for the Internet to function, perhaps the most relevant for applications to connect is DNS resolution. Systems are typically configured with a single DNS recursive resolver, or a set of primary and alternate recursive resolvers. Recursive resolver services are offered by organisations such as enterprises, ISPs, and global providers.

3. Issues with Centralisation

The three primary issues are reliance on single points of failure, the creation of too attractive surveillance targets, and the concentration of information in a way that may affect other services.

3.1. Single point of failure

The first issue is having a concentrated point may become a single point of accidental failure, or an attack target. For instance, a single root for an Internet security system or a single trust anchor for a routing system increases the risk of something bad happening which affects everything. This seems a bad practice. Note that the issue is not necessarily a single physical node that somehow in control; even a distributed system that is under one administration is a weak point, as there are typically single management systems and internal components that, based on experience, can cause large parts of the distributed system to stop functioning. Or, legal or commercial structures cause an undesirable effect, such as ability to access private data across borders [MSCVUS].

Similarly, reliance on single piece of software can cause a single point of failure.

Weaknesses of single centralised designs is not limited to technical components. Even an administrative or governance system can become weak through too much power or imagined power concentratred in one place. For instance, the IANA system, when there was still a perception of US government tie to its management, was used as

argument in various debates. Without such a central tie-in, there would have not been any reason for tying IANA's important, but essentially clerical duties to political issues.

3.2. Surveillance

The surveillance problem relates to putting too much information or control in a single entity.

For instance, the DNS resolvers will learn the Internet usage patterns of their clients. A client might decide to trust a particular recursive resolver with information about DNS queries.

However, it is difficult or impossible to provide any guarantees about data handling practices in the general case. And even if a service can be trusted to respect privacy with respect to handling of query data, legal and commercial pressures or surveillance activity could result in misuse of data. Similarly, outside attacks may occur towards any DNS services. For a service with many clients, these risks are particularly undesirable.

3.3. Concentration of information

The concentration of information problem is about generating information (or providing control opportunities) in basic Internet communications service that may assist whoever gets that information to be more capable in providing other services on top of the Internet, in a manner that is not possible for competing other service providers. This problem appears in particular where there are machine-learning opportunities in the data being collected.

3.4. Effect scope

When a particular application, such as a social media system, reaches a dominant position in the market, this position still affects only that application. However, when Internet infrastructure changes, this has wide-encompassing effects across all users and all types of traffic.

Most things in the Internet are of course changeable or configurable, but while users move from some set of applications to other ones over time quite easily, normal users rarely configure their Internet

connectivity parameters in any fashion. As a result, the impact of defaults, operating system and browser settings are wide-ranging.

3.5. Interaction with other issues

The above issues do not, of course, appear in isolation, but are mixed with other potential developments and deployment models. For instance, the DNS resolver centralisation problem is growing, as some web browsers are choosing to deploy encrypted DNS query protocols such as DNS-over-HTTPS (DOH) [RFC8484], and are doing it with default servers being centralised ones.

One of the dilemmas in deploying some of these new technologies is the ability to both make improvements at a quick pace and find suitable other partners to interact with at the same quick pace.

3.6. The effect of differing expectations and jurisdictions

Many of the centralisation issues are also made more difficult through differing expectations in different user populations. Some gladly rely on a particular content provider, for instance, while others may fear what data collection and leaks may result. It should also be noted that legal and contractual situations throughout the world differ, for instance in terms of expectations on user privacy.

4. Recommendations

For background, the current consolidation in ownership of and control over the Internet infrastructure was not foreseen [Clark], and arguably the loss of decentralized control goes against its design objectives. For instance, [RFC1958] says:

This allows for uniform and relatively seamless operations in a competitive, multi-vendor, multi-provider public network.

and

Heterogeneity is inevitable and must be supported by design.

And [RFC3935] says:

We embrace technical concepts such as decentralized control, edge-user empowerment and sharing of resources, because those concepts resonate with the core values of the IETF community.

Given this background, and given the issues listed in Section 3, it seems prudent to recommend that whenever it comes to Internet infrastructure services, centralised designs should be avoided where possible. It is still important to deploy other important features, such as protected signaling or encryption, and use the most trustworthy services, but it needs to be done in a fashion that ensures no single points of failure are created, and no centralised storage of information are created in the process.

Where such centralised points are created, they will eventually fail, or they will be misused through surveillance or legal actions regardless of the best efforts of the Internet community. The best defense to data leak is to avoid creating that data store to begin with.

This memo is not an attempt to specify how specific issues can be solved in a distributed manner, but historically, the Internet community has been successful in doing this in a manner that does not

rely on a single service, be it about DNS root services, certificate authorities, mail service, and so on.

5. Informative References

[Clark] Clark, D., "The Design Philosophy of the DARPA Internet Protocols", In Symposium Proceedings on Communications Architectures and Protocols, 106-114. SIGCOMM '88. New York, NY, USA, ACM https://doi.org/10.1145/52324.52336 , 1988.

[I-D.arkko-abcd-distributed-resolver-selection] Arkko, J., Thomson, M., and T. Hardie, "Selecting Resolvers from a Set of Distributed DNS Resolvers", Internet Draft draft-arkko-abcd-distributed-resolver-

section-00.txt (Work In Progress), IETF , November 2019.

[I-D.arkko-arch-dedr-report]
Arkko, J. and T. Hardie, "Report from the IAB workshop on Design Expectations vs. Deployment Reality in Protocol Development", Internet Draft draft-arkko-arch-dedr-report-00.txt (Work In Progress), IETF , November 2019.

[I-D.arkko-iab-internet-consolidation]
Arkko, J., Trammell, B., Nottingham, M., Huitema, C., Thomson, M., Tantsura, J., and N. Oever, "Considerations on Internet Consolidation and the Internet Architecture", draft-arkko-iab-internet-consolidation-02 (work in progress), July 2019.

[ISOC] "Consolidation in the Internet economy", Internet Society, https://future.internetsociety.org/2019/ , 2019.

[MSCVUS] Wikipedia, ., "Microsoft Corp. v. United States", https://en.wikipedia.org/wiki/Microsoft_Corp._v._United_States , n.d..

[RFC1035] Mockapetris, P., "Domain names - implementation and specification", STD 13, RFC 1035, DOI 10.17487/RFC1035, November 1987, <https://www.rfc-editor.org/info/rfc1035>.

[RFC1958] Carpenter, B., Ed., "Architectural Principles of the Internet", RFC 1958, DOI 10.17487/RFC1958, June 1996, <https://www.rfc-editor.org/info/rfc1958>.

[RFC3935] Alvestrand, H., "A Mission Statement for the IETF", BCP 95, RFC 3935, DOI 10.17487/RFC3935, October 2004, <https://www.rfc-editor.org/info/rfc3935>.

[RFC8484] Hoffman, P. and P. McManus, "DNS Queries over HTTPS (DoH)", RFC 8484, DOI 10.17487/RFC8484, October 2018, <https://www.rfc-editor.org/info/rfc8484>.

Appendix A. Acknowledgements

The author would like to thank Christian Huitema, Mark Nottingham, Stephen Farrell, Gonzalo Camarillo, Mirja Kuehlewind, Ted Hardie,

Alissa Cooper, Martin Thomson, Daniel Migault, Goran AP Eriksson, Joel Halpern, and many others for interesting discussions in this problem space.

Author's Address

Jari Arkko
Ericsson

Email: jari.arkko@piuha.net