IntArea Working Group
Internet-Draft
Intended status: Informational
Expires: October 24, 2018

A. Andersdotter
ARTICLE 19

April 22, 2018

An update to RFC6302 on Logging Recommendations for Internet-Facing Servers
draft-andersdotter-intarea-update-to-rfc6302-00

Abstract

This draft seeks to update RFC6302 on Logging Recommendations for Internet-Facing Servers. The new recommendations aim to be a best practice for service providers and server maintainers, by following recommendations outlined in RFC6973 and taking into account new regulatory requirements in the privacy area.

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 October 24, 2018.

Table of Contents

1. Introduction

In 2013, the IETF adopted [RFC6973] Privacy Guidelines for Internet protocols to ensure robust procedures for evaluating existing protocols and standards with respect to privacy, and insert protective mechanisms for privacy in future protocol and standards work. In the past couple of years, new data privacy regulations with wide geographical scope are entering into effect with big effects for technology companies and technology consumers around the world. The combination of these changes, in IETF procedure and regulatory requirements, have caused some previously established best practices to become poor practices.

This draft proposes updates to specifically [RFC6302] on Logging Recommendations for Internet-Facing Servers with a view for it to serve as a useful reference for operators seeking to be compliant with modern regulatory requirements for the protection of end-users, e.g. [GDPR].

Earlier recommendations contained in [RFC6302] relied heavily on observations made in Section 12 of [RFC6269] that regulatory requirements could imply a broad obligation to log identifiers. At the time of the adoption of [RFC6302], it was known that European Union law mandated data retention and trace-ability of each and every telecommunications subscriber in the European Union. The regulatory landscape in Europe has since changed, for instance in the European Union through [C20315], and in the broader Council of Europe area through [Zakharov] and [SzaboVissy]. It is possible that [RFC6269]

should be revisited in light of these developments, but such work is outside the scope of this text.

The below text is intended to replace Section 1 in [RFC6302].

Service providers, in so far as they are a collection of individual persons, and subscribers, and the transactional relationships of these individuals with the service provision, all give rise to personal data. In [RFC6973] it is specified that data minimization and security are important mitigation strategies against privacy threats. Further, regulatory requirements place an obligation on protocol designers and operators of servers to implement privacy-by-design and data minimization techniques.

[RFC6973] as well as new regulatory requirements have been put in place to protect the privacy of internet users. They are in the vein of previous IETF work on pervasive monitoring as a security risk in and of itself [RFC7258], and have parallels in new developments in international human rights law, see e.g. [UNGA2013].

2. Terminology

This section is intended to be introduced in [RFC6302] as a separate terminology section, replacing the first paragraph of Section 2 of [RFC6302].

The key words *MUST*, *MUST NOT*, *REQUIRED*, *SHALL*, *SHALL NOT*, *SHOULD*, *SHOULD NOT*, *RECOMMENDED*, *MAY* and *OPTIONAL* in this document as to be interpreted as described in [RFC2119].

This document adheres to the privacy terminology established in [RFC6973].

3. Recommendations for Internet-facing servers

This section is intended to replace Section 2 of [RFC6302].

Providers of internet-facing servers

SHOULD only store entire incoming IP addresses for as long as is necessary to provide the specific service requested by the user.

SHOULD keep only the first two octets (of an IPv4 address) or the first three octets (of an IPv6 address) with remaining octets set to zero, when logging.

SHOULD NOT store logs of incoming IP addresses from inbound traffic for longer than three days.

SHOULD NOT log unnecessary identifiers, such as source port number, time stamps, transport protocol numbers or destination port numbers.

SHOULD ensure adequate log access control, with suitable mechanisms for keeping track of which entity accesses logged identifiers, for what reason and at what time.

It is RECOMMENDED that deviations from the above practices are carefully documented and communicated to subscribers.

3.1. Data minimization

Data minimization is proposed by Section 6.1 in [RFC6973] as an effective way of ensuring privacy protections. A data minimization principle is further a regulatory requirement in some parts of the world (e.g. [GDPR]).

Data minimization can be effectuated in a number of different ways, including by limiting collection, retention and identifiability to personal data. The recommendation to anonymize IP addresses intended for logging, the recommendation not to store logs for longer than a limited amount of time, and the recommendation not to log unnecessary identifiers are intended to advance such effectuations of data minimization.

A three-day logging period covers a week-end, which is convenient for professional server providers. It also accounts for the ability of content providers to geolocate subscribers for the duration of their content consumption, in those cases where this is necessary due to legal restrictions.

3.2. User involvement

In Section 6.2 of [RFC6973] it is established involving individuals in decisions about data collection and treatment of data is a way of mitigating privacy threats. The section proposes that individuals be informed, and that they are provided ways to signal their preferences, and make choices, about collection and sharing of data.

Identifiers about subscribers can be logged at an internet-facing server to enable provision of content that is geoblocked, but are only required for as long as the service is requested by the user. In these circumstances, data which is logged for longer than the time it takes to deliver the service should be subject to careful considerations and the subscriber should be informed thereof.

Similarly, there exists no duty of subscribers to assist internet-facing servers in their efforts to improve services or the Internet. Where IP addresses or identifiers about individuals are logged with a view to improving services or the Internet, and having no other technical justification, individuals should be given a way to signal preferences and make choices about such logging.

3.3. Security

Security is advanced by Section 6.3 of [RFC6973] as an effective way to mitigate privacy threats. Among the important security goals mentioned are confidentiality, unauthorized usage and inappropriate usage. The recommendation to have adequate access control is intended to ensure security in the handling of such logs that are kept even after the data minimization strategies are deployed.

4. Considerations for electronic communications providers

This section is intended to replace Section 3 of [RFC6302].

The new regulatory requirements referenced earlier in this document imply that electronic communications providers may also have to review their logging practices. It is advisable that they should do so, bearing in mind [RFC6973]. However, the details are outside the scope of this document.

5. Security considerations

This draft gives recommendations for logging at internet-facing servers. It is intended to protect internet users from the threats of pervasive monitoring [RFC7258] and to assist operators of internet-facing servers in adhering to regulatory requirements.

Operators seeking to deviate from the base-level of privacy and security assumed for internet users, should make time-limited, specific exceptions which have clearly stated and lawful aims. Deviations could for instance be included in employment contracts or consumer contracts that are tied to non-public services which are nevertheless provided through Internet-facing servers and which require authentication for access.

6. Acknowledgments

The author would like to thank Mallory Knodel, Linus Nordberg and Anders Jensen-Urstad for their comments during the drafting of this document.

7. References

7.1. Normative References

[RFC2119] Bradner, S., "Key words for use in RFCs to Indicate Requirement Levels", RFC 2119, DOI 10.17487/RFC2119, March 1997, <https://www.rfc-editor.org/info/rfc2119>.

7.2. Informative References

[C20315] Court of Justice of the European Union, "ECLI:EU:C:2016:970, Judgment of the Court (Grand Chamber) of 21 December 2016, Tele2 Sverige AB v Post- och telestyrelsen and Secretary of State for the Home Department v Tom Watson and Others", December 2016, <http://curia.europa.eu/juris/liste.jsf?num=C-203/15>.

[GDPR] European Union, "Regulation (EU) 2016/679 (General Data Protection Regulation)", May 2016, <http://data.europa.eu/eli/reg/2016/679/oj>.

[RFC6269] Ford, M., Boucadair, M., Durand, A., Levis, P., and P. Roberts, "Issues with IP Address Sharing", RFC 6269, DOI 10.17487/RFC6269, June 2011, <https://www.rfc-editor.org/info/rfc6269>.

[RFC6302] Durand, A., Gashinsky, I., Lee, D., and S. Sheppard, "Logging Recommendations for Internet-Facing Servers", RFC 6302, DOI 10.17487/RFC6302, June 2011, <https://www.rfc-editor.org/info/rfc6302>.

[RFC6973] Cooper, A., Tschofenig, H., Aboba, B., Petersen, J., Morris, J., Hansen, M., and R. Smith, "Privacy Considerations for Internet Protocols", RFC 6973, DOI 10.17487/RFC6973, July 2013, <https://www.rfc-editor.org/info/rfc6973>.

[RFC7258] Farrell, S. and H. Tschofenig, "Pervasive Monitoring Is an Attack", RFC 7258, DOI 10.17487/RFC7258, May 2017, <https://www.rfc-editor.org/info/rfc7258>.

[SzaboVissy] European Court of Human Rights, "Case of Szabo and Vissy v. Hungary, Application no. 37138/14, ECHR 2016", January 2016, <http://hudoc.echr.coe.int/eng?i=001-160020>.

[UNGA2013]
United Nations General Assembly, ""The right to privacy in the digital age" (A/C.3/68/L.45)", 2013, <http://daccess-ods.un.org/TMP/1133732.05065727.html>.

[Zakharov]
European Court of Human Rights, "Case of Zakharov v. Russia, Application no. 47143/06, ECHR 2015.", December 2015, <http://hudoc.echr.coe.int/eng?i=001-159324>.

Author's Address

Amelia Andersdotter
ARTICLE 19
Free Word Centre, 60 Farringdon Road
London EC1R 3GA
United Kingdom

Email: amelia@article19.org