Human Rights Protocol Considerations Research Group
Internet-Draft
Intended status: Informational
Expires: April 18, 2016

D. Gillmor
ACLU
N. ten Oever
Article19
A. Doria
APC

October 16, 2015

Human Rights Protocol Considerations Glossary
draft-dkg-hrpc-glossary-01

Abstract

This document presents a glossary of terms used to map between concepts common in human rights discussions and engineering discussions. It is intended to facilitate work by the proposed Human Rights Protocol Considerations research group, as well as other authors within the IETF.

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 http://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 April 18, 2016.

Table of Contents

1. Introduction

"There's a freedom about the Internet: As long as we accept the rules of sending packets around, we can send packets containing anything to anywhere."

[Berners-Lee]

The Human Rights Protocol Consideration Proposed Research Group aims to research whether standards and protocols can enable, strengthen or threaten human rights, as defined in the Universal Declaration of Human Rights [UDHR] and the International Covenant ons Civil and Political Rights [ICCPR], specifically, but not limited to the right to freedom of expression and the right to freedom of assembly.

Comunications between people working on human rights and engineers working on Internet protocols can be improved with a shared vocabulary.

This document aims to provide a shared vocabulary to facilitate understanding of the intersection between human rights and Internet protocol design.

Discussion on this draft at: hrpc@irtf.org // https://www.irtf.org/mailman/admindb/hrpc

This document builds on the previous IDs published within the framework of the proposed hrpc research group [ID]

2. Glossary

In the analysis of existing RFCs central design and technical concepts have been found which impact human rights. This is an initial glossary of concepts that could bridge human rights discourse and technical vocabulary. These definitions should be improved and further aligned with existing RFCs.

Accessibility Full Internet Connectivity as described in [RFC4084] to provide unfettered access to the Internet

The design of protocols, services or implementation that provide an enabling environment for people with disabilities.

The ability to receive information available on the Internet

Anonymity The condition of an identity being unknown or concealed. [RFC4949]

Anonymous A state of an individual in which an observer or attacker cannot identify the individual within a set of other individuals (the anonymity set). [RFC6973]

Authenticity The act of confirming the truth of an attribute of a single piece of data or entity.

Censorship resistance Methods and measures to prevent Internet censorship.

Confidentiality The non-disclosure of information to any unintended person or host or party

Connectivity The extent to which a device or network is able to reach other devices or networks to exchange data. The Internet is the tool for providing global connectivity [RFC1958].

Content-agnosticism Treating network traffic identically regardless of content.

Debugging Debugging is a methodical process of finding and reducing the number of bugs, or defects, or malfunctions in a protocol or its implementation, thus making it behave as expected and analyse the consequences that might have emanated from the error. Debugging tends to be harder when various subsystems are tightly coupled, as changes in one may cause bugs to emerge in another. [WP-Debugging]

The process through which people troubleshoot a technical issue, which may include inspection of program source code or device configurations. Can also include tracing or monitoring packet flow.

Decentralized Opportunity for implementation or deployment of standards, protocols or systems without one single point of control.

End-to-End The principal of extending characteristics of a protocol or system as far as possible within the system. For example, end-to-end instant message encryption would conceal communications from one user's instant messaging application through any intermediate devices and servers all the way to the recipient's instant messaging application. If the message was decrypted at any intermediate point-for example at a service provider-then the property of end-to-end encryption would not be present.

One of the key architectural guidelines of the Internet is the end-to-end principle in the papers by Saltzer, Reed, and Clark [Saltzer] [Clark]. The end-to-end principle was originally articulated as a question of where best not to put functions in a communication system. Yet, in the ensuing years, it has evolved to address concerns of maintaining openness, increasing reliability and robustness, and preserving the properties of user choice and ease of new service development as discussed by Blumenthal and Clark in [Blumenthal]; concerns that were not part of the original articulation of the end-to-end principle. [RFC3724]

communication that takes place between communication end-points of the same physical or logical functional level

Federation The possibility of connecting autonomous systems into a single distributed system.

Heterogenity The Internet is characterized by heterogeneity on many levels: devices and nodes, router scheduling algorithms and queue management mechanisms, routing protocols, levels of multiplexing, protocol versions and implementations, underlying link layers (e.g., point-to-point, multi-access links, wireless, FDDI, etc.), in the traffic mix and in the levels of congestion at different times and places. Moreover, as the Internet is composed of autonomous organizations and internet service providers, each with their own separate policy concerns, there is a large heterogeneity of administrative domains and pricing structures. As a result, heterogeneity principle is proposed in [RFC1958] to be supported by design. [FIArch]

Integrity Maintenance and assurance of the accuracy and consistency of data to ensure it has not been (intentionally or unintentionally) altered

Internet censorship Internet censorship is the intentional suppression of information originating, flowing or stored on systems connected to the Internet where that information is relevant for decision making to some entity. [Elahi]

Inter-operable A property of a documented standard or protocol which allows different independent implementations to work with each other without any restricted negotiation, access or functionality.

Internet Standards as an Arena for Conflict Pursuant to the principle of constant change, since the function and scope of the Internet evolves, so does the role of the IETF in developing standards. Internet standards are adopted on the basis of a series of criteria, including high technical quality, support by community consensus, and their overall benefit to the Internet. The latter calls for an assessment of the interests of all affected parties and the specifications' impact on the Internet's users. In this respect, the effective exercise of the human rights of the Internet users is a relevant consideration that needs to be appreciated in the standardization process insofar as it is directly linked to the reliability and core values of the Internet. [RFC1958] [RFC0226] [RFC3724]

Internationalization (i13n) The practice of the adaptation and facilitation of protocols, standards, and implementation to different languages and scripts.

Open standards Conform [RFC2606]: Various national and international standards bodies, such as ANSI, ISO, IEEE, and ITU-T, develop a variety of protocol and service specifications that are similar to Technical Specifications defined here. National and international groups also publish "implementors' agreements" that are analogous to Applicability Statements, capturing a body of implementation-specific detail concerned with the practical application of their standards. All of these are considered to be "open external standards" for the purposes of the Internet Standards Process.

Openness The quality of the unfiltered Internet that allows for free access to other hosts

Permissionless innovation The freedom and ability of to freely create and deploy new protocols on top of the communications constructs that currently exist

Privacy The right of an entity (normally a person), acting in its own behalf, to determine the degree to which it will interact with its environment, including the degree to which the entity is willing to share its personal information with others. [RFC4949]

The right of individuals to control or influence what information related to them may be collected and stored and by whom and to whom that information may be disclosed.

Privacy is a broad concept relating to the protection of individual autonomy and the relationship between an individual and society, including government, companies and private individuals. It is often summarized as "the right to be left alone" but it encompasses a wide range of rights including protections from intrusions into family and home life, control of sexual and reproductive rights, and communications secrecy. It is commonly recognized as a core right that underpins human dignity and other values such as freedom of association and freedom of speech.

The right to privacy is also recognized in nearly every national constitution and in most international human rights treaties. It has been adjudicated upon both by international and regional bodies. The right to privacy is also legally protected at the national level through provisions in civil and/or criminal codes.

Reliable Reliability ensures that a protocol will execute its function consistently and error resistant as described and function without unexpected result. A system that is reliable degenerates gracefully and will have a documented way to announce degradation. It also has mechanisms to recover from failure gracefully, and if applicable, allow for partial healing.

Resilience The maintaining of dependability and performance in the face of unanticipated changes and circumstances.

Robustness The resistance of protocols and their implementations to errors, and to involuntary, legal or malicious attempts to disrupt its mode of operations. [RFC0760] [RFC0791] [RFC0793] [RFC1122]

Scalable The ability to handle increased or decreased workloads predictably within defined expectations. There should be a clear definition of its scope and applicability. The limits of a systems scalability should be defined.

Stateless / stateful In computing, a stateless protocol is a communications protocol that treats each request as an independent transaction that is unrelated to any previous request so that the communication consists of independent pairs of request and

response. A stateless protocol does not require the server to retain session information or status about each communications partner for the duration of multiple requests. In contrast, a protocol which requires keeping of the internal state on the server is known as a stateful protocol. [WP-Stateless]

Strong encryption / cryptography Used to describe a cryptographic algorithm that would require a large amount of computational power to defeat it. [RFC4949]

Transparent: "transparency" refers to the original Internet concept of a single universal logical addressing scheme, and the mechanisms by which packets may flow from source to destination essentially unaltered. [RFC2775]

The combination of reliability, confidentiality, integrity, anonymity, and authenticity is what makes up security on the Internet

```
 ( Reliability    )
(  Confidentiality )
(  Integrity       ) =  communication and information
(  Authenticity    )                 security (technical)
 ( Anonymity      )
```

The combination of End-to-End, Interoperability, resilience, reliability and robustness is what makes us connectivity on the Internet

```
                     ( End-to-End      )
 connectivity =     (  Interoperability )
                   (   Resilience       )
                   (   Reliability      )
                   (   Robustness       )
                    (  Autonomy        )
                     ( Simplicity     )
```

3. Security Considerations

As this draft concerns a research document, there are no security considerations.

4. IANA Considerations

This document has no actions for IANA.

5. Research Group Information

The discussion list for the IRTF Human Rights Protocol Considerations proposed working group is located at the e-mail address hrpc@ietf.org [1]. Information on the group and information on how to subscribe to the list is at https://www.irtf.org/mailman/listinfo/hrpc

Archives of the list can be found at: https://www.irtf.org/mail-archive/web/hrpc/current/index.html

6. References

6.1. Informative References

[Berners-Lee] Berners-Lee, T. and M. Fischetti, "Weaving the Web,", HarperCollins p 208, 1999.

[Blumenthal] Blumenthal, M. and D. Clark, "Rethinking the design of the Internet: The end-to-end arguments vs. the brave new world", ACM Transactions on Internet Technology, Vol. 1, No. 1, August 2001, pp 70-109. , 2001.

[Clark] Clark, D., "The Design Philosophy of the DARPA Internet Protocols", Proc SIGCOMM 88, ACM CCR Vol 18, Number 4, August 1988, pp. 106-114. , 1988.

[Elahi] Elahi, T. and I. Goldberg, "CORDON - A taxonomy of Internet Censorship Resistance Strategies", 2012, <http://cacr.uwaterloo.ca/techreports/2012/cacr2012-33.pdf>.

[FIArch] "Future Internet Design Principles", January 2012, <http://www.future-internet.eu/uploads/media/FIArch_Design_Principles_V1.0.pdf>.

[ICCPR] United Nations General Assembly, "International Covenant on Civil and Political Rights", 1976, <http://www.ohchr.org/EN/ProfessionalInterest/Pages/CCPR.aspx>.

[ID] ten Oever, N., Doria, A., and J. Varon, "Proposal for research on human rights protocol considerations", 2015, <http://tools.ietf.org/html/draft-doria-hrpc-proposal>.

[RFC0226] Karp, P., "Standardization of host mnemonics", RFC 226, DOI 10.17487/RFC0226, September 1971, <http://www.rfc-editor.org/info/rfc226>.

[RFC0760] Postel, J., "DoD standard Internet Protocol", RFC 760, DOI 10.17487/RFC0760, January 1980, <http://www.rfc-editor.org/info/rfc760>.

[RFC0791] Postel, J., "Internet Protocol", STD 5, RFC 791, DOI 10.17487/RFC0791, September 1981, <http://www.rfc-editor.org/info/rfc791>.

[RFC0793] Postel, J., "Transmission Control Protocol", STD 7, RFC 793, DOI 10.17487/RFC0793, September 1981, <http://www.rfc-editor.org/info/rfc793>.

[RFC1122] Braden, R., Ed., "Requirements for Internet Hosts - Communication Layers", STD 3, RFC 1122, DOI 10.17487/RFC1122, October 1989, <http://www.rfc-editor.org/info/rfc1122>.

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

[RFC2606] Eastlake 3rd, D. and A. Panitz, "Reserved Top Level DNS Names", BCP 32, RFC 2606, DOI 10.17487/RFC2606, June 1999, <http://www.rfc-editor.org/info/rfc2606>.

[RFC2775] Carpenter, B., "Internet Transparency", RFC 2775, DOI 10.17487/RFC2775, February 2000, <http://www.rfc-editor.org/info/rfc2775>.

[RFC3724] Kempf, J., Austein., R., Ed., and IAB, "The Rise of the Middle and the Future of End-to-End: Reflections on the Evolution of the Internet Architecture", RFC 3724, DOI 10.17487/RFC3724, March 2004, <http://www.rfc-editor.org/info/rfc3724>.

[RFC4084] Klensin, J., "Terminology for Describing Internet Connectivity", BCP 104, RFC 4084, DOI 10.17487/RFC4084, May 2005, <http://www.rfc-editor.org/info/rfc4084>.

[RFC4949] Shirey, R., "Internet Security Glossary, Version 2", FYI 36, RFC 4949, DOI 10.17487/RFC4949, August 2007, <http://www.rfc-editor.org/info/rfc4949>.

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

[Saltzer] Saltzer, J., Reed, D., and D. Clark, "End-to-End Arguments in System Design", ACM TOCS, Vol 2, Number 4, November 1984, pp 277-288. , 1984.

[UDHR] United Nations General Assembly, "The Universal Declaration of Human Rights", 1948, <http://www.un.org/en/documents/udhr/>.

[WP-Debugging] "Debugging", n.d., <https://en.wikipedia.org/wiki/Debugging>.

[WP-Stateless] "Stateless protocol", n.d., <https://en.wikipedia.org/wiki/Stateless_protocol>.

6.2. URIs

[1] mailto:hrpc@ietf.org

Authors' Addresses

Daniel Kahn Gillmor
ACLU

EMail: dkg@fifthhorseman.net

Niels ten Oever
Article19

EMail: niels@article19.org

Avri Doria
APC

EMail: avri@apc.org