Proposed RG
Human Rights Protocol Considerations
(hrpc)

IETF 94
Tuesday November 3
15:20 – 16:50

Co-Chairs:
Niels ten Oever – Article19
Avri Doria – APC

Administrivia

- Mailinglist
- https://www.irtf.org/mailman/listinfo/hrpc
- Github
- https://github.com/nllz/IRTF-HRPC
- Meetecho

  http://www.meetecho.com/ietf94/hrpc
- Minutes
- http://etherpad.tools.ietf.org:9000/p/notes-ietf-94-hrpc

Agenda

- Agenda Bashing
- Jabber scribe, note takers
- Notewell
- Context of research
- Presentation and Discussion of 'A Case Study of Coding Rights'
- Presentation and Discussion of Methodology draft
- Discussion of Glossary draft
- Presentation and discussion of Report draft
- Discussion of 'The Internet is for End Users' draft
- Open discussion other drafts, papers, ideas
- Status of proposed research group
- Next steps
- AOB

Note Well

Any submission to the IETF intended by the Contributor for publication as all or part of an IETF Internet-Draft or RFC and any statement made within the context of an IETF activity is considered an "IETF Contribution". Such statements include oral statements in IETF sessions, as well as written and electronic communications made at any time or place, which are addressed to:

- The IETF plenary session
- The IESG, or any member thereof on behalf of the IESG
- Any IETF mailing list, including the IETF list itself, any working group or design team list, or any other list functioning under IETF auspices
- Any IETF working group or portion thereof
- Any Birds of a Feather (BOF) session
- The IAB or any member thereof on behalf of the IAB
- The RFC Editor or the Internet-Drafts function

All IETF Contributions are subject to the rules of RFC 5378 and RFC 3979 (updated by RFC 4879).

Statements made outside of an IETF session, mailing list or other function, that are clearly not intended to be input to an IETF activity, group or function, are not IETF Contributions in the context of this notice. Please consult RFC 5378 and RFC 3979 for details.

A participant in any IETF activity is deemed to accept all IETF rules of process, as documented in Best Current Practices RFCs and IESG Statements.

A participant in any IETF activity acknowledges that written, audio and video records of meetings may be made and may be available to the public.

Context of research

- Internet as tool for freedom of expression and freedom of association
    - By intention or by coincidence?
        - The Internet aims to be the global network of networks that provides unfettered connectivity to all users at all times and for any content. (RFC1958)
- But as the scale and the industrialization of the Internet has grown greatly, the influence of such world-views started to compete with other values.
- The starting assumption of the RG is that as the Internet continues to grow, the linkage of Internet protocols to human rights needs to become explicit, structured, and intentional

Context of the Research (2)

Working on this problem in the IRTF (in context of IETF), because this is where the protocols and standards that have shaped and are shaping the Internet are being developed

This proposed RG has two major aims:

- to expose the relation between protocols and human rights, with a focus on the rights to freedom of expression and freedom of assembly, and

- to propose guidelines to protect the Internet as a human-rights-enabling environment in future protocol development, in a manner similar to the work done for Privacy Considerations in RFC 6973. This research group suggests that similar considerations may apply for other human rights such as freedom of expression or freedom of association.

- Presentation and Discussion of 'A Case Study of Coding Rights'

- Presented by Corinne Cath

OII

UNIVERSITY · OF · OXFORD
DOMI NVS ILLV MINA TIO MEA
Oxford
Internet
Institute

Research Question

Should the right to freedom of speech be instantiated in the protocols and standards designed by the Internet Engineering Task Force?

Theory

- Highly normative question
- Builds on the academic discussion between Clark et al (2005) and Brown (2010)

Clark et al

Design for variation in outcome, so that the outcome can be different in different places, and the tussle takes place within the design (…) [as] Rigid designs will be broken; designs that permit variation will flex under pressure and survive (2005:2).

Brown

Some key, universal values – of which the UDHR is the most legitimate expression – should be baked into the architecture at design time (2010:3).

Argument #1

- A. The four architectural design principles [openness, interoperability, redundancy and end-to-end] on which the Internet is build are based upon a normative understanding of what the Internet is, and should do.
- B. This normative understanding is largely in line with the Western notion of the Internet as a connectivity enabling platform for freedom of speech.
- C. The personal norms and morals of engineers are transposed into the network [interviews]
- D. This normative understanding of what the Internet is, is reified by the fact that the IETF is relatively homogenous group with a particular normative understanding of the Internet’s nature and function to society.

- Hence, the IETF already bakes *some* values into protocols and standards

Argument #2

- Through various examples I try to show how values get baked into protocol, by referencing the:

A. 1990 debate on Carnivore and the IETF’s responsibility to support wiretapping for law enforcement purposes

B. Post-Snowden PM debate

C. OPES

D. Middleboxes

E. Status code 451

- On the basis of these examples I extract three conditions that need to be present for the IETF to encode values into protocols.

Argument #3

- Three conditions that need to be present:

1. There needs to be a clear technical reason for encoding a particular value.
2. It can only be done when there is no strong commercial or political resistance to encoding the value in the protocols.
3. Encoding the value needs to work towards maintaining the normative conceptualization of the Internet [open etc].

Argument #4

- I identify 3 specific challenges the IETF runs into trying to purposefully encode values into protocols that complicate their ability to purposefully instantiate freedom of speech in protocols.
- I also point out that these are not an excuse for the IETF to skirt its responsibility for ensuring its protocols are in line with the UDHR principles [!!] but…

Argument #5

- That considering the current challenges and danger of Internet fragmentation the IETF should perhaps focus on bringing its work in line with the UDHR without *directly* instantiating human rights into protocols.

- [*SPOILER ALERT*: This is also the answer to my main RQ]

Theoretical contribution

- These conclusions have various ramifications for the existing academic theories mentioned in my introduction. [As well as for Lessig's theory code = law. Because one does not simply do this type of research without mentioning Lessig]

Policy recommendation #1

Finding novel ways to have human rights guide protocol development. The IETF’s Internet Research Task Force’s (IRTF) research group on human rights is currently spearheading this attempt. The group is creating an RFC with ‘Human Rights Protocol Considerations’. These considerations are modelled on the protocol considerations for privacy (RFC 6973) and security (RFC 3532), but with a specific focus on human rights. This particular format fits the IETF’s structure: it is a procedure that engineers are accustomed to and it leaves enough flexibility to circumvent issues raised by Internet fragmentation or active resistance of large market players.

- See https://datatracker.ietf.org/rg/hrpc/charter/

Policy recommendation #2

- Increase the number of technical engineers that act as custodians for human rights at the IETF. Over the past twenty years technical engineers from the Centre for Democracy and Technology (CDT) and the American Civil Liberties Union (ACLU) actively participated in specific IETF working groups they identified as having a potential impact on human rights.

- Both these suggestions however run the same risk that security and privacy considerations suffer from: faulty implementation or partial deployment of RFCs. Which is why these two approaches need to happen conjointly with the third strategy.

Policy recommendation #3

- Emphasise the importance of the four key architectural principles as laid out by Clark et al. (2005) in protocol design. This would evade several of the problems of Internet fragmentation and the tendency amongst operators and implementers to ignore (from their perspective unnecessary) parts of the RFCs' specifications. This does not directly instantiate human rights in protocols but does strengthen the basic make-up of the Internet that has led to it become a crucial media for exercising the right to freedom of speech in the first place.

Q & A

Presentation and Discussion of Methodology draft

- Claudio Guarnieri
- Will Scott
- Niels ten Oever

Case studies

- IP
  - Network visibility of Source and Destination
  - Protocol visibility
  - Address Translation and Mobility

  + FoE, FoI, FoA, participation in cultural life, arts and science

Case studies

- DNS (RFC1035)
  - Privacy issues (DNSpriv / RFC7626))
  - Removal of records
  - Distortion of records
  - Injection of records

  + FoE, FoI, FoA, participation in cultural life, arts and science

Case studies

- HTTP (RFC 7230-7237)
  - Encryption not mandated
    - Traffic Interception
    - Traffic manipulation

    + FoE, FoI, FoA, participation in cultural life, arts and science

Case studies

- XMPP (RFC3920)
    - Enabeling freedom of association, freedom of expression
  - User identification
  - Character encoding / Internationalization
  - Group chat limitations
  - Issues with OTR

  + federated

  + decentralized

  + FoA, FoE

Case studies

- Peer to Peer (RFC7574)
  - Bitcoin, Bittorrent, Skype, Spotify
  - Poisoning attacks (index tables, routing tables)
  - Prone to throttling (Bittorrent)
  - Lack of anonymization

    + dissemination of information
  - + FoA, FoE, FoI

Case studies

- VPN
  - + Privacy
  - + Censorship circumvention
  - – False sense of anonymity
  - – IPv6 Leakage
  - – DNS Leakage
  - – Traffic correlation

Rights definitions

- Expansion and new definitions
- Mostly on level of design principles

Freedom of Expression

$$\begin{pmatrix} \begin{pmatrix} interoperability \\ resilience \\ reliability \\ robustness \end{pmatrix} = connectivity \\ \begin{pmatrix} resilience \\ reliability \\ confidentiality \\ anonymity \\ authenticity \end{pmatrix} = security \\ privacy \\ content\ agnosticism \\ internationalization \\ censorship\ resistance \\ open\ standards \\ heretogeneity\ support \end{pmatrix} = freedom\ of\ expression$$

Right to Security

$$\begin{pmatrix} reliability \\ confidentiality \\ integrity \\ authenticity \\ anonymity \end{pmatrix} = \mathrm{right\ to}\ security$$

Rights of Assembly and Association

$$\begin{pmatrix} \mathit{connectivity} \\ \mathit{decentralization} \\ \mathit{censorship\ resistance} \\ \mathit{pseudonomity} \\ \mathit{anonymity} \\ \mathit{security} \end{pmatrix} = \text{right to } \mathit{freedom\ of\ assembly} \text{ and } \mathit{association}$$

Rights of participation in cultural life, arts & science

$$\begin{pmatrix} \mathit{open\ standatds} \\ \mathit{localization} \\ \mathit{internationalization} \\ \mathit{censorship\ resistance} \end{pmatrix} = \text{right to } \mathit{participate} \text{ in } \mathit{cultural\ life}\ , \mathit{arts} \text{ and } \mathit{science}$$

Non discrimination, equal protection, presumed inocent & political particpation

$$\begin{pmatrix} \mathit{anonymity} \\ \mathit{privacy} \\ \mathit{pseudonymity} \\ \mathit{content\ agnosticism} \end{pmatrix} = \mathit{non} - \mathit{discrimination}$$

$$\begin{pmatrix} \mathit{content\ agnosticism} \\ \mathit{security} \end{pmatrix} = \mathit{equal\ protection}$$

$$\begin{pmatrix} \mathit{anonymity} \\ \mathit{privacy} \\ \mathit{security} \end{pmatrix} = \text{right to } \mathit{be\ presumed\ innocent}$$

$$\begin{pmatrix} \mathit{accessibility} \\ \mathit{internationalization} \\ \mathit{censorship\ resistance} \end{pmatrix} = \text{right to } \mathit{political\ participation}$$

Discussion of Glossary draft

- Defintions updated
- Further scouring through RFCs and other glossaries for terminology and other usage was done and is included.
- Does a working definiton need to be developed from instances of multiple definitions that links the engineering term with the rights issues?

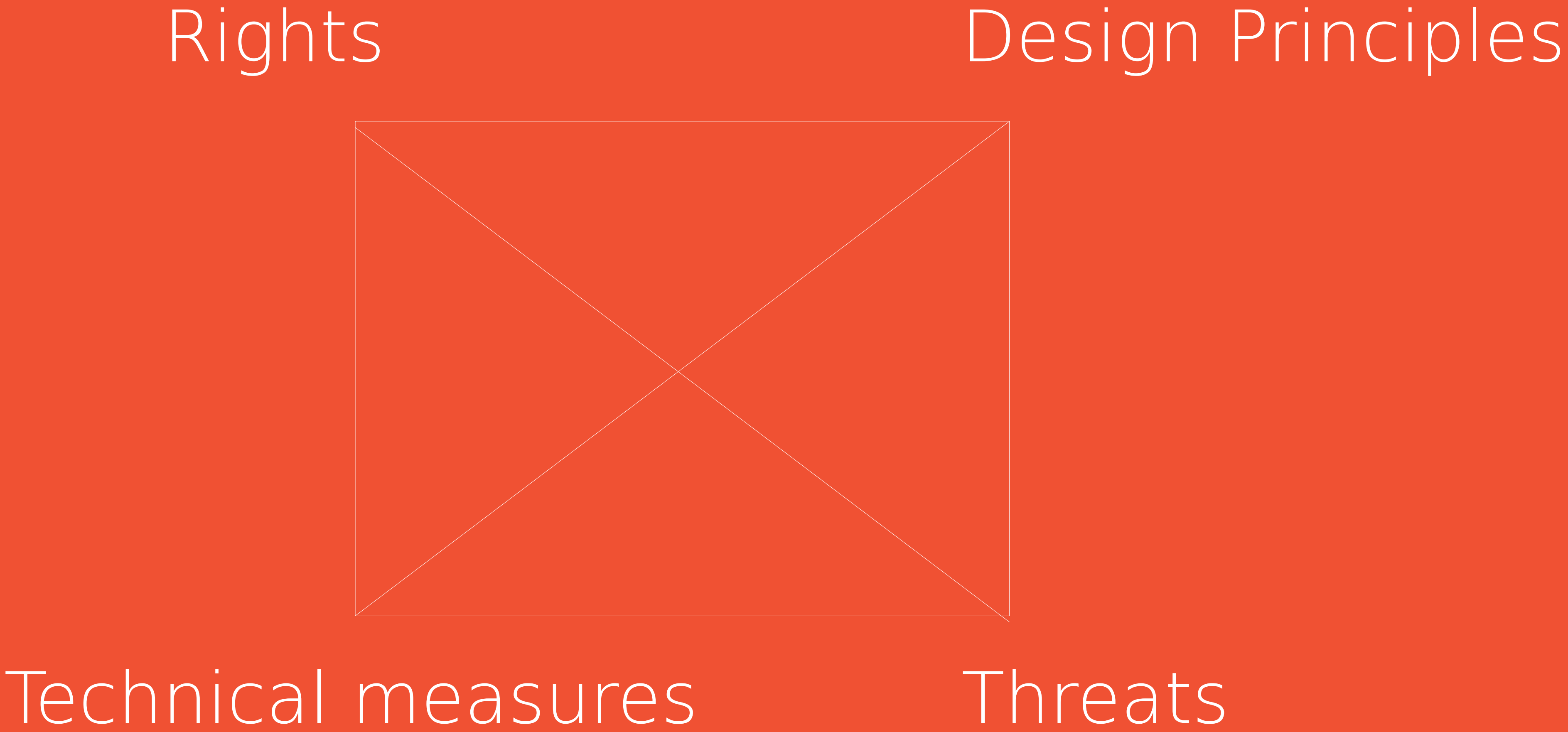
Presentation and discussion of Report draft

- Intention is to create a single document that present the research and initial take at considerations with a clear narrative
- Will build on raw materials in the other drafts
  - Finding commonalities
  - Delimiting protocol effects from exogenous effects
- Things that need to happen
  - Raw material in methodology needs to be worked through for similarities among the cases
  - Hypothesis on common factors need to be formed
  - Hypothesis tested in other areas

Report: fundamental question

- Are the considerations specific to a single protocol
- Or are there generalized considerations that can be applied to any protocol effort
- The cases begin to show individual protocol considerations
- Are these abstractable to a general set of considerations– as was done in the privacy considerations?.

Next steps



Rights

Design Principles

Technical measures

Threats

Discussion of 'The Internet is for End Users' draft

By Mark Nottingham

draft-nottingham-for-the-users

> “In case of conflict, consider users over authors over implementors over specifiers over theoretical purity. In other words costs or difficulties to the user should be given more weight than costs to authors; which in turn should be given more weight than costs to implementors; which should be given more weight than costs to authors of the spec itself, which should be given more weight than those proposing changes for theoretical reasons alone. Of course, it is preferred to make things better for multiple parties at once.”

– HTML Design Principles

1. Document ~~Constituents~~ ~~Stakeholders~~ Relevant Parties.

2. Don’t allow anyone to have a higher priority than end users.

Documenting Relevant Parties

- Discuss involvement, relationships explicitly
- Aid discussion when there is conflict
- Advertise who the work benefits

Putting Users First

- Is this part of the IETF culture?
- How do WGs apply this?
- Can we know what is “best for users?”

“This also does not mean that the IETF community has any specific insight into what is “good for end users”; as before, we will need to interact with the greater Internet community and apply our process to help us make decisions, deploy our protocols, and ultimately determine their success or failure.”

Status of proposed research group

- October, 27, 2014 - Publication of Proposal for research on human rights protocol considerations - 00

  ID 00 - www.ietf.org/id/draft-doria-hrpc-proposal-00.txt
- IETF91 - November, 13, 2014: Presentation during saag session

  https://datatracker.ietf.org/meeting/91/agenda/saag/
- March 9, 2015 - Publication of Proposal for research on human rights protocol considerations - 01

  http://www.ietf.org/id/draft-doria-hrpc-proposal-01.txt
- January 2015 - Proposed research group in the IRTF
- March 22 to 27, 2015 IETF92 – Session & Interviews with members from the community
- June 2015 - Interim Meeting
- July 2015 Publication of Methodology and Glossary

  ID 00 - https://tools.ietf.org/html/draft-varon-hrpc-methodology-00

  ID 00 - https://tools.ietf.org/html/draft-dkg-hrpc-glossary-00
- July 2015, IETF93 - Session
- November 2015, IETF93 – Screening of film, three IDs (01, 01 and 00), paper, session
- https://tools.ietf.org/html/draft-dkg-hrpc-glossary-01 https://tools.ietf.org/html/draft-varon-hrpc-methodology-01
- https://tools.ietf.org/html/draft-doria-hrpc-report-00

Screening tomorrow 15:00

Room 301 - 304

Comments, Questions