Network Working Group J.
Arkko
Internet-Draft
Ericsson
Intended status: Informational T.
Hardie
Expires: May 7, 2020
Google

November 04, 2019

# Report from the IAB workshop on Design Expectations vs. Deployment Reality in Protocol Development
## draft-arkko-arch-dedr-report-00

Abstract

The Design Expectations vs. Deployment Reality in Protocol Development Workshop was convened by the Internet Architecture Board (IAB) in June 2019. This report summarizes its significant points of discussion and identifies topics that may warrant further consideration.

Table of Contents



## 1. Introduction

The Design Expectations vs. Deployment Reality in Protocol Development Workshop was convened by the Internet Architecture Board (IAB) in June 2019. This report summarizes its significant points of

discussion and identifies topics that may warrant further consideration.

Note: While late in being submitted, this report is still an early version. Comments and contributions are appreciated. We expect to call for review of the -01 version.

The background for the workshop was that a number of protocols have presumed specific deployment models during the development or early elaboration of the protocol. Actual deployments have, however, often run contrary to these early expectations when economies of scale, DDoS resilience, market consolidation, or other factors have come into play. These factors can result in the deployed reality being highly concentrated.

This is a serious issue for the Internet, as concentrated, centralized deployment models present risks to user choice, privacy, and future protocol evolution.

On occasion, the differences to expectations were almost immediate, but they also occur after a significant time has passed from the protocol's initial development.

Examples include:

Email standards, which presumed many providers running in a largely uncoordinated fashion, but which has seen both significant market consolidation and a need for coordination to defend against spam and other attacks. The coordination and centralized defense mechanisms scale better for large entities, which has fueled additional consolidation.

The DNS, which presumed deep hierarchies but has often been deployed in large, flat zones, leading to the nameservers for those zones becoming critical infrastructure. Future developments in DNS may see concentration through the use of globally available common resolver services, which evolve rapidly and can offer better security. Paradoxically, concentration of these queries into few services creates new security and privacy concerns.

The Web, which is built on a fundamentally decentralized design, but which is now often delivered with the aid of Content Delivery Networks. Their services provide scaling, distribution, and Denial of Service prevention in ways that new entrants and smaller systems operators would find difficult to replicate. While truly small services and truly large ones may operate using only their own infrastructure, many others are left with the only practical choice being the use of a globally available commercial service.

Similar developments may happen with future technologies and services. For instance, the growing use of Machine Learning technology presents challenges for distributing effective implementation of a service throughout a pool of many different providers.

In [RFC5218] the IAB tackled what made for a successful protocol. In [RFC8170], the IAB described how to handle protocol transitions. This purpose of the workshop was to explore cases where the initial system design assumptions turned out to be wrong, looking for patterns in what caused those assumptions to fail (e.g., concentration due to DDoS resilience) and in how those failures impact the security, privacy, and manageability of the resulting deployments.

While the eventual goals might include proposing common remediations for specific cases of confounded protocol expectations.

The workshop call for papers invited the submission of position papers which would:

- Describe specific cases where systems assumptions during protocol development were confounded by later deployment conditions.
- Survey a set of cases to identify common factors in these confounded expectations.
- Explore remediations which foster user privacy, security and provider diversity in the face of these changes.

A total of 21 position papers were received, listed in Section 3. On site or remote were 30 participants, listed in Appendix A.

## 2. Workshop Agenda

After opening and discussion of goals for the workshop, the discussion focused on five main topics:

- Past experiences. What have we learned?
- Principles. What forces apply to deployment? What principles to take into account in design?
- Centralised deployment models. The good and the bad of centralisation. Can centralisation be avoided? How?
- Security. Are we addressing the right threats? What should we prepare ourselves for?
- Future. What can we do? Should we get better at predicting, or should we do different things?

## 3. Position Papers

The following position papers were submitted to the workshop:

- Jari Arkko. "Changes in the Internet Threat Model" [Arkko2019]
- Vittorio Bertola. "How the Internet Was Won and Where It Got Us" [Bertola2019]
- Carsten Bormann. "WiFi authentication: Some deployment observations from eduroam" [Bormann2019]

- Stephane Bortzmeyer. "Encouraging better deployments" [Bortzmeyer2019]

- Brian Carpenter and Bing Liu. "Limited Domains and Internet Protocols" [Carpenter2019]

- Alissa Cooper. "Don't Forget the Access Network" [Cooper2019]

- Stephen Farrell. "We're gonna need a bigger threat model" [Farrell2019]

- Phillip Hallam-Baker. "The Devil is in the Deployment" [HallamBaker2019]

- Ted Hardie. "Instant Messaging and Presence: A Cautionary Tale" [Hardie2019]

- Paul Hoffman. "Realities in DNSSEC Depployment" [Hoffman2019]

- Christian Huitema. "Concentration is a business model" [Huitema2019]

- Geoff Huston. "The Border Gateway Protocol, 25 years on" [Huston2019]

- Dirk Kutscher. "Great Expectations: Protocol Design and Socioeconomic Realities" [Kutscher2019]

- Julien Maisonneuve. "DNS, side effects and concentration" [Maisonneuve2019]

- John Mattsson. "Privacy, Jurisdiction, and the Health of the Internet" [Mattsson2019]

- Moritz Muller. "Rolling Forward: An Outlook on Future Root Rollovers" [Muller2019]

- Joerg Ott. "Protocol Design Assumptions and PEPs" [Ott2019]

- Lucas Pardue. "Some challenges with IP multicast deployment" [Pardue2019]

- Jim Reid. "Where/Why has DNS gone wrong?" [Reid2019]

- Mohit Sethi and Tuomas Aura. "IoT Security and the role of Manufacturers: A Story of Unrealistic Design Expectations" [Sethi2019]

- Andrew Sullivan. "Three kinds of concentration in open protocols" [Sullivan2019]

These papers are available from the IAB website [CFP] [POS].

## 4. Discussions

### 4.1. Past experiences

The workshop investigated deployment cases from WebPKI to DNSSEC, from BGP to NATs, from DNS resolvers to CDNs, and from IOT to instant messaging and social media applications.

### 4.2. Principles

Several underlying principles can be observed in the example cases that were discussed. Deployment failures tend to be associated with cases where interdependencies make progress difficult and there's no major advantage for early deployment. Despite persistent problems in the currently used technology, it becomes difficult for the ecosystem to switch to better technology. For instance, there are a number of areas where the Internet routing protocol, BGP, is lacking, but success in deploying significant improvements has been lacking, for instance in the area of security.

Another principle appears to be first mover advantage. Several equally interesting technologies have fared in very different ways, depending whether there was an earlier system that provided most of the benefits of the new system. Again, despite potential problems in an already deployed technology, it becomes difficult to deploy improvements due to lack of immediate incentives and due to the competing and already deployed alternative that is proceeding forward in the ecosystem. For instance, WebPKI is very widely deployed and used, but DNSSEC is not. Is this because the earlier commercial adoption of WebPKI, and the initially more complex interdependencies between systems that wished to deploy DNSSEC.

The workshop also discussed different types of deployment patterns on the Internet:

- Delivering functionality over Internet as a web service. The Internet is an open and standardised system, but the service on top may be closed, essentially running two components of the service provider's software against each other over the browser and Internet infrastructure. Several large application systems

have grown in the Internet in this manner, encompassing large amounts of functionality and a large fraction of Internet users.

- Delivering concentrated network services that offer the standard capabilities of the Internet. Examples in this category include the provisioning of DNS resolution, some mail services, and so on.

The second case is more interesting for an Internet architecture discussion. There can, however, be different underlying situations in that case. The service may be simply a concentrated way to provide a commodity service. The market should find a natural equilibrium for such situations. This may be fine, particularly, where the service does not provide any new underlying advantage to whoever is providing it (in the form of user data that can be commercialized, for instance, or as training data for an important machine learning service).

Secondly, the service may be an extension beyond standard protocols, leading to some questions about how well standards and user expectations match. But those questions could be addressed by better or newer standards. But the third situation is more troubling: the service are provided in this concentrated manner due to business patterns that make it easier for particular entities to deploy such services.

### 4.3. Centralised deployment models

Many of the participants have struggled with these trends and their effect on desirable characteristics of Internet systems, such as distributed, end-to-end architecture or privacy. Yet, there are many business and technical drivers causing the Internet architecture to become further and further centralised.

The hopeful side of this issue is that there are some potential answers:

- DDOS defenses do not have to come through large entities, as layered defenses and federation also helps similarly.

- Surveillance state data capture can be fought with data object encryption, and not storing all of the datal in one place.

- Open interface help guard against the bundling of services in one large entity; as long as there are open, well-defined interface to specific functions these functions can also be performed by other parties.

- Commercial surveillance does not seem to curbed by current means. But there are still possibilities, such as stronger regulation, data minimisation, or browsers acting on behalf of users. There

are hopeful signs that at least some browsers are becoming more aggressive in this regard. But more is needed.

One comment made in the workshop that the Internet community needs to move back from regulation to trying to curb the architectural trend of centralization instead. Another comment was that discussing this in the abstract is not as useful as more concrete, practical actions.
For instance, one might imagine DOH deployments with larger number of trusted resolvers.

## 4.4. Security

This part of the discussed focused on whether in the current state of the Internet we actually need a new threat model.

Many of the communications security concerns have been addressed in the past few years, with increasing encryption. However, issues with trusting endpoints on the other side of the communication have not been addressed, and are becoming more urgent with the advent or centralised service architectures.

The participants in the workshop agreed that a new threat model is needed, and that non-communications-security issues need to be treated.

Other security discussions were focused on IOT systems, algorithm agility issues, and experiences from difficult security upgrades such as the DNSSEC key rollover.

The participants cautioned against relying too much on device manufacturers for security, and being clear on security models and assumptions. Security is often poorly understood, and the assumptions about who the system defends against and not are not clear.

## 4.5. Future

The workshop turned into a discussion of what actions we can take:

- Documenting our experiences?
- Providing advice (to IETF, to others)
- Waiting for the catastrophe that will make people agree to changes? (hopefully not this)

- Work at the IETF?

- Technical solutions/choices?

The best way for ietf to do things is through standards; convinging people through other requests is difficult. The IETF needs to:

- pick pieces that it is responsible for
- being reactive for the rest, be available as an expert in other discussions, provide Internet technology clue where needed, etc.

One key question is what other parties need to be involved in any discussions. Platform developers (mobile platforms, cloud systems, etc) is one such group. Specific technology or business groups (such as email provider or certificate authority forums) are another.

The workshop also discussed specific technology issues, for instance around IOT systems. One observation in those systems is that there is no single model for applications, they vary. There are a lot of different constraints in different systems and different control points. What is needed perhaps most today is user control and transparency (for instance, via MUD descriptions). Another issue is management, particularly for devices that could be operational for decades. Given the diversity of IOT systems, it may also make more sense to build support systems for the broader solutions that specific solutions or specific protocols.

There are also many security issues. While some of them are trivial (such as default passwords), one should also look forward and be prepared to have solutions for, say, trust management for long time scales, or be able to provide data minimization to cut down on potential for leakages. And the difficulty of establishing peer-to-peer security strengthens the need for a central point, which may also be harmful from a long-term privacy perspective.

## 5. Conclusions

### 5.1. Summary of discussions

The workshop met in sunny Finnish countryside and made the non-suprising observation that technologies sometimes get deployed in surprising ways. But the consequences of deployment choices can have an impact on security, privacy, centralised vs. distributed models, competition, surveillance, and the IETF community cares deeply about these aspects, so it is worthwhile to spend time in analysis of these choices.

The prime factor driving deployments is perceived needs; expecting people to recognise obvious virtues and therefore deploy is not likely to work.

And the ecosystem is complex, including for instance many parties: different business roles, users, regulators, and so on, and perceptions of needs and ability to act depends highly on what party one talks to.

While the workshop discussed actions and advice, there is a critical question of who these are targeted towards. There is need to construct a map of what parties need to perform what actions.

The workshop also made some technical observations. One recent trend is that technology is moving up the stack, e.g., in the areas of services, transport protocol functionality, security, naming, and so on. This impacts how easy or hard changes are, and who is able to perform them.

It was also noted that interoperability continues to be important, and we need to explore what new interfaces need standardisation -- this will enable different deployment models & competition. Prime factor driving deployments is actual needs; we cannot force anything to others but can provide solutions for those that need them. Needs and actions may fall on different parties.

The workshop also considered the balancing of user non-involvement and transparency and choice, relevant threats such as communicating with malicious endpoints, the role and willigness of browsers in increasing the ability to defending the users' privacy, and concerns around centralised control or data storage points

The workshop also discussed specific issues around routing, denial-of-service attacks, IOT systems, role of device manufacturers, the DNS, and regulatory reactions and their possible consequences.

## 5.2. Actions

The prime conclusion from the workshop was that the topic is not completed in the workshop. Much more work is needed. The best way for ietf to do things is through standards. The IETF should focus on the parts that it is responsible for, and be available as an expert on other discussions.

The documents/outputs and actions described in the following were deemed relevant by the participants.

### 5.2.1. Potential architecture actions and outputs

- Develop and document a modern threat model
- Continue discussion of consolidation/centralisation issues
- Document architectural principles, e.g., (re-)application of the end-to-end principle

The first receiver of these thoughts is the IETF and protocol community, but combined with some evangelising & validation elsewhere

### 5.2.2. Potential other actions

- Pursue specific IETF topics, e.g., work on taking into account reputation systems in IETF work, working to ensuring certificate scoping can be appropriately limited, building end-to-end encryption tools for applications, etc.
- General deployment experiences/advice, and documenting deployment assumptions possibly already in WG charters
- A report, and a short summary article will be produced from the workshop.

## 5.3. Other publications

The workshop results have also been reported at [ISPColumn] by Geoff Huston.

## 5.4. Feedback

Feedback regarding the workshop is appreciated, and can be sent to the program committee, the IAB, or the architecture-discuss list.

# 6. Informative References

[Arkko2019]
Arkko, J., "Changes in the Internet Threat Model", Position paper submitted for the IAB DEDR workshop , June 2019.

[Bertola2019]
Bertola, V., "How the Internet Was Won and Where It Got Us", Position paper submitted for the IAB DEDR workshop , June 2019.

[Bormann2019]
Bormann, C., "WiFi authentication: Some deployment observations from eduroam", Position paper submitted for the IAB DEDR workshop , June 2019.

[Bortzmeyer2019]
Bortzmeyer, S., "Encouraging better deployments", Position paper submitted for the IAB DEDR workshop , June 2019.

[Carpenter2019]
Carpenter, B. and B. Liu, "Limited Domains and Internet Protocols", Position paper submitted for the IAB DEDR workshop , June 2019.

[CFP]
IAB, ., "Design Expectations vs. Deployment Reality in Protocol Development Workshop 2019", https://www.iab.org/activities/workshops/dedr-workshop/ , April 2019.

[Cooper2019]
Cooper, A., "Don't Forget the Access Network", Position paper submitted for the IAB DEDR workshop , June 2019.

[Farrell2019]
Farrell, S., "We're gonna need a bigger threat model", Position paper submitted for the IAB DEDR workshop , June 2019.

[HallamBaker2019]
Hallam-Baker, P., "The Devil is in the Deployment", Position paper submitted for the IAB DEDR workshop , June 2019.

[Hardie2019]
Hardie, T., "Instant Messaging and Presence: A Cautionary Tale", Position paper submitted for the IAB DEDR workshop , June 2019.

[Hoffman2019]
Hoffman, P., "Realities in DNSSEC Depployment", Position paper submitted for the IAB DEDR workshop , June 2019.

[Huitema2019]
Huitema, C., "Concentration is a business model", Position paper submitted for the IAB DEDR workshop , June 2019.

[Huston2019]
Huston, G., "The Border Gateway Protocol, 25 years on", Position paper submitted for the IAB DEDR workshop , June 2019.

[ISPColumn]
Huston, G., "Network Protocols and their Use", https://www.potaroo.net/ispcol/2019-06/dedr.html , June 2019.

[Kutscher2019]
Kutscher, D., "Great Expectations: Protocol Design and Socioeconomic Realities", Position paper submitted for the IAB DEDR workshop , June 2019.

[Maisonneuve2019]
Maisonneuve, J., "DNS, side effects and concentration", Position paper submitted for the IAB DEDR workshop , June 2019.

[Mattsson2019]
Mattsson, J., "Privacy, Jurisdiction, and the Health of the Internet", Position paper submitted for the IAB DEDR workshop , June 2019.

[Muller2019]
Muller, M., "Rolling Forward: An Outlook on Future Root Rollovers", Position paper submitted for the IAB DEDR workshop , June 2019.

[Ott2019] Ott, J., "Protocol Design Assumptions and PEPs", Position paper submitted for the IAB DEDR workshop , June 2019.

[Pardue2019]
Pardue, L., "Some challenges with IP multicast deployment", Position paper submitted for the IAB DEDR workshop , June 2019.

[POS] IAB, ., "Position Papers: DEDR Workshop", https://www.iab.org/activities/workshops/dedr-workshop/position-papers/ , June 2019.

[Reid2019]
Reid, J., "Where/Why has DNS gone wrong?", Position paper submitted for the IAB DEDR workshop , June 2019.

[RFC5218] Thaler, D. and B. Aboba, "What Makes for a Successful Protocol?", RFC 5218, DOI 10.17487/RFC5218, July 2008, <https://www.rfc-editor.org/info/rfc5218>.

[RFC8170] Thaler, D., Ed., "Planning for Protocol Adoption and Subsequent Transitions", RFC 8170, DOI 10.17487/RFC8170, May 2017, <https://www.rfc-editor.org/info/rfc8170>.

[Sethi2019] Sethi, M. and T. Aura, "IoT Security and the role of Manufacturers: A Story of Unrealistic Design Expectations", Position paper submitted for the IAB DEDR workshop , June 2019.

[Sullivan2019] Sullivan, A., "Three kinds of concentration in open protocols", Position paper submitted for the IAB DEDR workshop , June 2019.

## Appendix A. Particant List

The following is a list of participants on site and over a remote connection:

- Arkko, Jari
- Aura, Tuomas
- Bertola, Vittorio
- Bormann, Carsten
- Bortzmeyer, Stephane
- Cooper, Alissa
- Farrell, Stephen
- Flinck, Hannu
- Gahnberg, Carl
- Hallam-Baker, Phillip
- Hardie, Ted
- Hoffman, Paul

- Huitema, Christian (remote)
- Huston, Geoff
- Komaitis, Konstantinos
- Kuhlewind, Mirja
- Kutscher, Dirk
- Li, Zhenbin
- Maisonneuve, Julien
- Mattson, John
- Muller, Moritz
- Ott, Joerg
- Pardue, Lucas
- Reid, Jim
- Rieckers, Jan-Frederik
- Sethi, Mohit
- Shore, Melinda (remote)
- Soininen, Jonne
- Sullivan, Andrew
- Trammell, Brian

## Appendix B. Acknowledgements

The authors would like to thank the workshop participants, the members of the IAB, and the participants in the architecture discussion list for interesting discussions. The workshop organizers would also like to thank Nokia for hosting the workshop in excellent facilities in Kirkkonummi, Finland.

## Authors' Addresses

Jari Arkko
Ericsson

Email: jari.arkko@piuha.net

Ted Hardie
Google

Email: ted.ietf@gmail.com