Stream: Internet Architecture Board (IAB)
RFC: 8980
Category: Informational
Published: February 2021
ISSN: 2070-1721
Authors: J. Arkko T. Hardie

RFC 8980
Report from the IAB Workshop on Design Expectations vs. Deployment Reality in Protocol Development

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 the workshop's significant points of discussion and identifies topics that may warrant further consideration.

Note that this document is a report on the proceedings of the workshop. The views and positions documented in this report are those of the workshop participants and do not necessarily reflect IAB views and positions.

Status of This Memo

This document is not an Internet Standards Track specification; it is published for informational purposes.

This document is a product of the Internet Architecture Board (IAB) and represents information that the IAB has deemed valuable to provide for permanent record. It represents the consensus of the Internet Architecture Board (IAB). Documents approved for publication by the IAB are not candidates for any level of Internet Standard; see Section 2 of RFC 7841.

Information about the current status of this document, any errata, and how to provide feedback on it may be obtained at https://www.rfc-editor.org/info/rfc8980.

Copyright Notice

Table of Contents

1. Introduction

The Internet Architecture Board (IAB) holds occasional workshops designed to consider long-term issues and strategies for the Internet, and to suggest future directions for the Internet architecture. This long-term planning function of the IAB is complementary to the ongoing engineering efforts performed by working groups of the Internet Engineering Task Force (IETF).

The Design Expectations vs. Deployment Reality in Protocol Development Workshop was convened by the IAB in June 2019. This report summarizes the workshop's significant points of discussion and identifies topics that may warrant further consideration.

The background for the workshop was that during the development and early elaboration phase for a number of protocols, there was a presumption of specific deployment models. Actual deployments have, however, often run contrary to these early expectations when economies of scale, Distributed Denial-of-Service (DDoS) attack 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 from the original expectations were almost immediate, but they also occur after significant time has passed since the protocol's initial development.

Some examples are given below.

- Email standards, which presumed many providers running in a largely uncoordinated fashion but have 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; these have fueled additional consolidation.
- The Domain Name System (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 a few services creates new security and privacy concerns.
- The Web, which is built on a fundamentally decentralized design but is now often delivered with the aid of Content Delivery Networks (CDNs). Their services provide scaling, distribution, and prevention of denial of service in ways that new entrants and smaller systems operators would find difficult to replicate. While truly small services and truly large services may each 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. The purpose of this 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, this workshop and thus this report focused on identifying patterns.

The workshop call for papers invited the submission of position papers that 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 that foster user privacy, security, and provider diversity in the face of these changes.

A total of 21 position papers were received and are listed in Section 3. On site or remote were 30 participants; they are 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?
- Centralized deployment models. The good and the bad of centralization. Can centralization 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 by the following people (listed in alphabetical order):

- Jari Arkko. "Changes in the Internet Threat Model" [Arkko2019]
- Vittorio Bertola. "How the Internet Was Won and Where It Got Us" [Bertola2019]

- Carsten Bormann and Jan-Frederik Rieckers. "WiFi authentication: Some deployment observations from eduroam" [Bormann2019]
- Stéphane 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 Deployment" [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. "Consolidation, Privacy, Jurisdiction, and the Health of the Internet" [Mattsson2019]
- Moritz Müller. "Rolling Forward: An Outlook on Future Root Rollovers" [Muller2019]
- Jörg 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 certificate authorities for web connections (WebPKI) to DNS Security (DNSSEC), from the Border Gateway Protocol (BGP) to Network Address Translators (NATs), from DNS resolvers to CDNs, and from Internet of Things (IoT) systems to instant messaging and social media applications.

In many cases, (1) there was a surprise in how technology was deployed, (2) there was a lack of sufficient adoption, or (3) the business models associated with chosen technologies were not in favor of broader interoperability.

In general, the protocol designers cannot affect market forces but must work within them. But there are often competing technical approaches or features that are tailored for a particular deployment pattern. In some cases, it is possible to choose whether to support, for instance, a clear need for an established business, a feature designed to support collaboration among smaller players, or some kind of disruption through a more speculative new feature or technology.

Lessons learned include the following:

- Feedback from those who deploy often comes too late.
- Building blocks get repurposed in unexpected ways.
- User communities come in too late.
- The Web is getting more centralized, and counteracting this trend is difficult. It is not necessarily clear what technical path leads to distributed markets and decentralized architectures, for instance.
- There are also many forces that make it easier to pursue centralized models than other models. For instance, deployment is often easier in a centralized model. And various business and regulatory processes work best within a small, well-defined set of entities that can interact with each other. This can lead to, for instance, regulators preferring a situation with a small number of entities that they can talk to, rather than a diverse set of providers.
- It is important but hard to determine how useful new protocols are.
- It is difficult for the IETF community to interact with other communities, e.g., specific business sectors that need new technology (such as aviation or healthcare) or regulators.

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 [RFC4271] is lacking, but there has been only limited success in deploying significant improvements -- 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 on 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 a 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 [RFC4033] is not. Is this because of the earlier commercial adoption of WebPKI, the more complex interdependencies between systems that wished to deploy DNSSEC, or some other reason?

The definition of "success" in [RFC5218] appears to be part of the problem. The only way to control deployments up front is to prevent wild success, but wild successes are actually what we want. And it seems very difficult to predict these successes.

The workshop also discussed the extent to which protocol work even should be controlled by the IETF, or the IESG. It seems unproductive to attempt to constrain deployment models, as one can only offer possibilities but not force anyone to use a particular possibility.

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

- Delivering functionality over the Internet as a web service. The Internet is an open and standardized system, but the service on top may be closed, essentially running two components of the same 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. This makes it easier for web applications to grow by themselves without cross-fertilization or interoperability.
- Delivering concentrated network services that offer the standard capabilities of the Internet. Examples in this category include the provisioning of some mail services, DNS resolution, and so on.

The second case is more interesting for an Internet architecture discussion. There can, however, be different underlying situations even 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. Thirdly, and potentially most disturbingly, the service may be provided in this concentrated manner due to business patterns that make it easier for particular entities to deploy such services.

The group also discussed monocultures, and their negative effect on the Internet and its stability and resistance to various problems and attacks.

Regulation may affect the Internet businesses as well. Regulation can exist in multiple forms, based on economic rationale (e.g., competition law) or other factors. For instance, user privacy is a common regulatory topic.

4.3. Centralized 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 centralized.

Some observations that were made:

- When standardizing new technology, the parties involved in the effort may think they agree on what the goals are but in reality are often surprised in the end. For instance, with DNS (queries) over HTTPS (DoH) [RFC8484], there were very different aspirations, some around improvements in confidentiality of the queries, some around operational and latency improvements to DNS operations, and some about shifting business and deployment models. The full picture was not clear before the work was completed.
- In DNS, DDoS is a practical reality, and only a handful of providers can handle the traffic load in these attacks.

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 help similarly.
- Surveillance state data capture can be fought with data object encryption and by not storing all of the data in one place.
- Web tracking can be combatted by browsers choosing to avoid techniques that are sensitive to tracking. Competition in the browser market may help drive some of these changes.
- Open interfaces help guard against the bundling of services in one large entity; as long as there are open, well-defined interfaces to specific functions, these functions can also be performed by other parties.
- Commercial surveillance does not seem to be curbed by current means. But there are still possibilities, such as stronger regulation, data minimization, 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 was that the Internet community needs to curb the architectural trend of centralization. Another comment was that discussing this in the abstract is not as useful as more concrete, practical actions. For instance, one might imagine different DoH deployments with widely different implications for privacy or tolerance of failures. Getting to the specifics of how a particular service can be made better is important.

4.4. Security

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

Many of the security concerns regarding communications 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 of centralized service architectures.

Further effort may be needed to minimize centralization, as having only a few places to tap increases the likelihood of surveillance.

There may be a need to update [RFC3552] and [RFC7258].

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

Other security discussions were focused on IoT systems, algorithm agility issues, experiences from difficult security upgrades such as DNSSEC key rollovers, and routing security.

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 who it does 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 the IETF or to others)?
- Waiting for the catastrophe that will make people agree to changes? The participants of course did not wish for this.
- Work at the IETF?
- Technical solutions/choices?

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

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

One key question is what other parties need to be involved in any discussions. Platform developers (mobile platforms, cloud systems, etc.) are 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 perhaps most needed today is user control and transparency (for instance, via Manufacturer Usage Descriptions (MUDs) [RFC8520]). 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 broader solutions than for 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 the 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 the sunny Finnish countryside and made the unsurprising observation that technologies sometimes get deployed in surprising ways. But the consequences of deployment choices can have an impact on security, privacy, centralized vs. distributed models, competition, and surveillance. As the IETF community cares deeply about these aspects, it is worthwhile to spend time on the analysis of these choices.

The prime factor driving deployments is perceived needs; expecting people to recognize obvious virtues and therefore deploy them 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 the ability to act depend 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 a need to construct a map of what parties need to perform what actions.

The workshop also made some technical observations. One issue is that the workshop identified a set of hard issues that affect deployment and for which we have no good solutions. These issues include, for instance, dealing with DDoS attacks and how to handle spam. Similarly, a lack of good solutions for micropayments is one factor behind a lot of the Internet economy being based on advertisements.

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 standardization -- this will enable different deployment models and competition. The prime factor driving deployments is actual needs; we cannot force anything on others but can provide solutions for those that need them. Needs and actions may fall to different parties.

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

The workshop also discussed specific issues around routing, DoS attacks, IoT systems, the 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 topics we discussed were not completed in the workshop. Much more work is needed. The best way for the IETF to make an impact is through standards. The IETF should focus on the parts that it is responsible for and be available as an expert on other discussions.

5.2.1. Potential Architecture Actions and Outputs

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

- Develop and document a modern threat model.
- Continue discussion of consolidation/centralization 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 evangelizing and validation elsewhere.

5.2.2. Other Potential Actions

- Pursuit of specific IETF topics, e.g., working on taking into account reputation systems in IETF work, working to ensure that 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 will be produced from the workshop (this RFC).

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. Security Considerations

Proposals discussed at the workshop would have significantly different security impacts, and each workshop paper should be read for its own security considerations.

7. 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. and J. Rieckers, "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", June 2019, <https://www.iab.org/activities/workshops/dedr-workshop/>.

[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 Deployment", 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", June 2019, <https://www.potaroo.net/ispcol/2019-06/dedr.html>.

[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., "Consolidation, Privacy, Jurisdiction, and the Health of the Internet", position paper submitted for the IAB DEDR workshop, June 2019.

[Muller2019] Müller, 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", June 2019, <https://www.iab.org/activities/workshops/dedr-workshop/position-papers/>.

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

[RFC3552] Rescorla, E. and B. Korver, "Guidelines for Writing RFC Text on Security Considerations", BCP 72, RFC 3552, DOI 10.17487/RFC3552, July 2003, <https://www.rfc-editor.org/info/rfc3552>.

[RFC4033] Arends, R., Austein, R., Larson, M., Massey, D., and S. Rose, "DNS Security Introduction and Requirements", RFC 4033, DOI 10.17487/RFC4033, March 2005, <https://www.rfc-editor.org/info/rfc4033>.

[RFC4271] Rekhter, Y., Ed., Li, T., Ed., and S. Hares, Ed., "A Border Gateway Protocol 4 (BGP-4)", RFC 4271, DOI 10.17487/RFC4271, January 2006, <https://www.rfc-editor.org/info/rfc4271>.

[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>.

[RFC7258] Farrell, S. and H. Tschofenig, "Pervasive Monitoring Is an Attack", BCP 188, RFC 7258, DOI 10.17487/RFC7258, May 2014, <https://www.rfc-editor.org/info/rfc7258>.

[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>.

[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>.

[RFC8520] Lear, E., Droms, R., and D. Romascanu, "Manufacturer Usage Description Specification", RFC 8520, DOI 10.17487/RFC8520, March 2019, <https://www.rfc-editor.org/info/rfc8520>.

[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. Participant List

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

- Arkko, Jari
- Aura, Tuomas
- Bertola, Vittorio
- Bormann, Carsten
- Bortzmeyer, Stéphane
- Cooper, Alissa
- Farrell, Stephen
- Flinck, Hannu
- Gahnberg, Carl
- Hallam-Baker, Phillip
- Hardie, Ted
- Hoffman, Paul
- Huitema, Christian (remote)
- Huston, Geoff
- Komaitis, Konstantinos

- Kühlewind, Mirja
- Kutscher, Dirk
- Li, Zhenbin
- Maisonneuve, Julien
- Mattsson, John
- Müller, Moritz
- Ott, Jörg
- Pardue, Lucas
- Reid, Jim
- Rieckers, Jan-Frederik
- Sethi, Mohit
- Shore, Melinda (remote)
- Soininen, Jonne
- Sullivan, Andrew
- Trammell, Brian

IAB Members at the Time of Approval

Internet Architecture Board members at the time this document was approved for publication were:

Jari Arkko
Alissa Cooper
Stephen Farrell
Wes Hardaker
Ted Hardie
Christian Huitema
Zhenbin Li
Erik Nordmark
Mark Nottingham
Melinda Shore
Jeff Tantsura

Martin Thomson

Brian Trammell

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 notes from Jim Reid were instrumental in writing this report. 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
Email: ted.ietf@gmail.com