

Internet Architecture Board Open Meeting

Mirja Kühlewind & Tommy Pauly
IETF 108 — July 2020

Note Well

- This is a reminder of IETF policies in effect on various topics such as patents or code of conduct. It is only meant to point you in the right direction. Exceptions may apply. The IETF's patent policy and the definition of an IETF "contribution" and "participation" are set forth in BCP 79; please read it carefully.
- As a reminder:
 - By participating in the IETF, you agree to follow IETF processes and policies.
 - If you are aware that any IETF contribution is covered by patents or patent applications that are owned or controlled by you or your sponsor, you must disclose that fact, or not participate in the discussion.
 - As a participant in or attendee to any IETF activity you acknowledge that written, audio, video, and photographic records of meetings may be made public.
 - Personal information that you provide to IETF will be handled in accordance with the IETF Privacy Statement.
 - As a participant or attendee, you agree to work respectfully with other participants; please contact the ombudsteam if you have questions or concerns about this.
- Definitive information is in the documents listed below and other IETF BCPs.
For advice, please talk to WG chairs or ADs:
 - BCP 9 (Internet Standards Process)
 - BCP 25 (Working Group processes)
 - BCP 25 (Anti-Harassment Procedures)
 - BCP 54 (Code of Conduct)
 - BCP 78 (Copyright)
 - BCP 79 (Patents, Participation)
 - <https://www.ietf.org/privacy-policy/> (Privacy Policy)

Agenda

Welcome & Status Updates (10 min.)

Documents (5 min.)

Workshops (5 min.)

Programs (20 min.)

Open Mic (10 min.)

What's IABopen?

IAB organized session focusing on technical and architectural aspects

Goals

Increase visibility of the work the IAB is doing

Collect feedback and community input to on-going and new work

Mailing lists to use

architecture-discuss@iab.org for architectural discussions and IAB documents

iab@iab.org for comments and concerns directly to the IAB

Program mailing lists for direct comments on work of a specific program

IAB virtual retreat

In preparation: Internal IAB survey about challenges and opportunities for the IAB, as well as general trends

June 1-5: 3x 1h all-IAB meetings + break-out groups:

- Architectural guidance
- Mission of the IAB: strategic/long term issues of the Internet
- COVID-19: Impact on technical work
- COVID-19: Impact on the IETF working model
- Technical factors related to deployment of increased security
- Impact/disruptions by other parties
- Evaluate/review the success of the IETF

Social interactions based on 3 coffee breaks/happy hour slots on each Tuesday and Thursday (joint with IESG)

See also <https://www.ietf.org/blog/iab-all-virtual-retreat-june-2020/> and https://www.iab.org/wiki/index.php/2020_Retreat

Documents

Active IAB Documents

- draft-iab-for-the-users (in RFC editor queue) - see next
- draft-iab-dedr-report (workshop report)

Recently published IAB Documents (2019/2020)

- RFC 8546: The Wire Image of a Network Protocol
- RFC 8558: Transport Protocol Path Signals
- RFC 8752: Report from the IAB Workshop on Exploring Synergy between Content Aggregation and the Publisher Ecosystem (ESCAPE)

The Internet is for End Users

draft-iab-for-the-users

“This document explains why the IAB believes that, when there is a conflict between the interests of end users of the Internet and other parties, IETF decisions should favour end users. It also explores how this can more effectively be achieved.”

- August 2015: Started as individual I-D
- August 2019: Adopted by IESG
- March 2020: Approved by the IAB

Community review helped shape the document:

- More clearly identify as suggestions from the IAB
- Expand suggestions for how to better represent user needs

Next steps?

Workshops

Recent Workshops

- IAB workshop on Design Expectations vs. Deployment Reality in Protocol Development (DEDR), June 2019

Proposed Workshops

- IAB workshop on COVID-19 Network Impacts, virtual, Nov 2020

DEDR Workshop (2019) Report

“Report from the IAB workshop on
Design Expectations vs. Deployment Reality
in Protocol Development”
(draft-iab-dedr-report-00.txt)

Report authors: Jari Arkko & Ted Hardie
- highly influenced by notes from Jim Reid, Geoff Huston, etc

IETF 108 IABOPEN

Reason for this discussion

Ask for reviews before we publish it as an RFC

- Any feedback or missing pieces?
- In particular, if you were there, can you review?
- Workshops typically have public reports/conclusions (this draft) and the any position papers that were submitted (21 in this case, see <https://www.iab.org/activities/workshops/dedr-workshop/>)

More general thoughts about deployment expectations topic can be discussed too

- But maybe a better topic for the architecture-discuss list or the open discussion part of this meeting

Workshop Topic

Often, Internet technology development has presumed specific deployment models

But actual deployments often differ

- Impacted by economies of scale, DDoS resilience, market consolidation, etc.
- Resulting in an impact on interoperability, centralisation, etc.
- Generally, interesting interaction between economics, technology, and deployments

Workshop agenda

- i. Experiences
- ii. Principles
- iii. Centralised deployment
- iv. Security
- v. Future

Some Conclusions

The non-surprising confirmation that technologies sometimes get deployed in surprising ways. Economics!

There are also technical issues that make things harder, e.g., lack of DDoS defence or micropayments solutions

Architecture work: Threat model? Continue discussion of centralization? Document principles (e.g., re-application of e2e principle)?

Technical work: Reputation systems? Tools to limit certificate scopes? E2e encryption for apps?

Thank you!

Questions, comments, feedback, interest?

COVID-19 Network Impacts Workshop

Organizing Committee:

Jari Arkko, Stephen Farrell, Cullen Jennings,
Colin Perkins, Ben Campbell, Mirja Kühlewind

IETF 108 IABOPEN

Background

The pandemic has had a tremendous impact on all of us, but also on networking

Large numbers of people working from home or otherwise depending on the network for their daily lives, network traffic has surged.

- ISP, mobile operator, and IXP traffic growth
- Conversational multimedia traffic and #users growth

Internet has coped relatively well (but not perfectly) with this traffic growth. Many things changed, however.

Goals

Learn about traffic patterns and their changes

It is interesting to see how the technology, operators and service providers have responded to large changes in traffic patterns

This is an opportunity to share our understanding of what the impacts were, what type of actions were needed, what worked and what didn't, etc.

Perhaps also an opportunity to learn for future

Topics in Scope

Measurements about traffic, user experience, performance, and other relevant aspects

Discussion about the behind-the-scenes network management and expansion activities

Experiences in general connectivity, conferencing, media/entertainment, and Internet infrastructure

Lessons learned for preparedness and operations

Lessons learned for Internet tech and architecture

Tentative logistics

This is an over-the-Internet virtual workshop

- Several sessions will be scheduled for the different topics on the week of November 9, 2020 (one week before IETF-109)

Participation is by invitation, based on position paper submissions

- Submissions Due: 9 October 2020
- Invitations Issued by: 15 October 2020

Thank you!

Questions, comments, feedback, interest?

IAB technical programs

Active:

- Internet Threat Model (model-t) Program

Recently concluded (2019):

- Privacy and Security (privsec) Program
- IP Stack Evolution (stackEvo) Program

Currently under discussion:

- Proposed Program on Evolvability, Deployability, and Maintainability (EDM)

Internet Threat Model (model-t) Program

Jari/Stephen “helping”

- Sadly, this time around, nothing much happened;-)
- Had a good call April 20th but lack of follow up (mea culpa mostly)

Planning to do a virtual meeting soon – will start to schedule on the list this week

Anyone about this Thursday 30th at 1610 UTC – let’s meet for an informal chat?

- Details of both the above will be on list

Goal: consider evolution of threat model and possibly offer updates to BCP72 for IETF consideration

Charter: <https://www.iab.org/activities/programs/internet-threat-model-model-t-program/>

List: <https://www.iab.org/mailman/listinfo/model-t>

Despite my utter inactivity as a helper, a bunch of people have written/revised/split drafts...

Drafts being discussed

draft-thomson-tmi

draft-mcfadden-smart-endpoint-taxonomy-for-cless

draft-mcfadden-smart-threat-changes

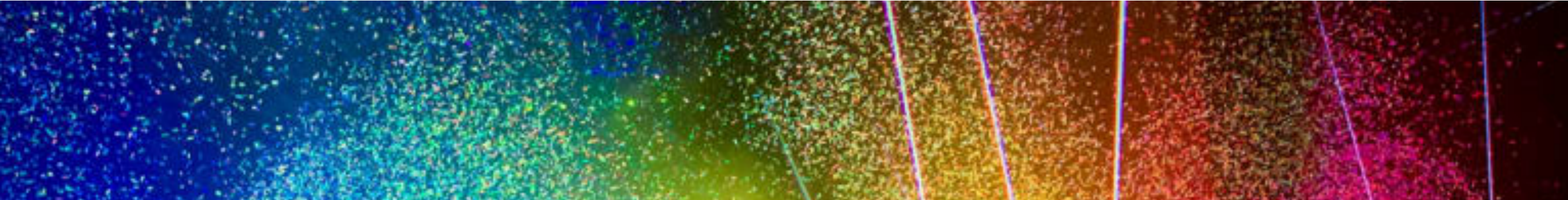
draft-lazanski-protocol-sec-design-model-t

draft-lazanski-users-threat-model-t

draft-arkko-farrell-arch-model-t

draft-arkko-farrell-arch-model-t-7258-additions

draft-arkko-farrell-arch-model-t-3552-additions



Evolvability, Deployability, & Maintainability

Proposed IAB Program



Evolvability

Design for greasing

draft-iab-use-it-or-lose-it, draft-iab-protocol-maintenance

QUIC greasing, HTTP greasing

Explain extension points

e.g., RFC 5507 Design Choices When Expanding the DNS

Which are preferred

Which are stable or ossified

Encourage practices for codepoint allocations that make extension easy

Deployability

Allow working groups to track running code

Catalog implementations and versions

Interoperability results

Active experiments

7 contributors



41 lines (36 sloc) | 4.81 KB

Raw

Blame



TLS 1.3 Implementations

name	language	role(s)	version	features/limitations
fizz	C++	C/S	RFC 8446	Based on libsodium, includes secure design abstractions. Zero-copy for advanced performance.
NSS	C	C/S	RFC 8446	Almost everything, except some crypto primitives
Mint	Go	C/S	-18	PSK resumption, 0-RTT, HRR
nqsb	OCaml	C/S	-11	PSK/DHE-PSK, no EC*, no client auth, no 0RTT -- live server at tls13test.nqsb.io port 4433, records traces, ping @hannesm , contains a static PSK/DHE_PSK token: id: 0x0000 ► secret:
ProtoTLS	JavaScript	C/S	-13	EC/DHE/PSK, no HelloRetryRequest
miTLS	F*	C/S	RFC 8446	EC/DHE/PSK/0-RTT, no RSA-PSS, no post-HS-auth, no ESNI
Tris	Go	C/S	RFC 8446	ECDHE/PSK/0-RTT, no HelloRetryRequest
BoringSSL	C	C/S	-23, -28, RFC 8446	P-256, X25519, HelloRetryRequest, resumption, 0-RTT, KeyUpdate
Wireshark	C	other	-18 to -28, RFC 8446	Full decryption and dissection support for drafts 19-21 since 2.4.0 (keylog format). Supports 18-21 since 2.4.2, -22 since 2.4.3, -23 since 2.4.5, -24 to -28 (+0RTT trial decryption) since 2.6.0. Tracking bug .
picotls	C	C/S	-18,-21,-23,-26	P-256, X25519, HelloRetryRequest, resumption, 0-RTT
rustls	Rust	C/S	-28 (final on branch)	P-256/P-384/curve25519, HRR, resumption, 0-RTT client
Haskell tls	Haskell	C/S	-28	ECDHE w/ P* and X*, full, HRR, PSK, 0RTT

Implementations

Alessandro Ghedini edited this page on Jun 23 · 415 revisions

[Edit](#)[New Page](#)

This wiki tracks known implementations of QUIC. See also our [Tools listing](#). Current [interop status](#); make sure you are looking at or editing the correct tab.

Please add your implementation below. Keep sorted alphabetically. There are three sections, one for "IETF QUIC Transport", one for "IETF HTTP over QUIC", and one for "QPACK". Entries may appear in multiple sections e.g. where a stack provides both IETF QUIC Transport and IETF HTTP over QUIC.

Note

If you are working on a QUIC implementation, please consider joining the [QUIC Developers Slack Channel](#). Also, if possible, please set up a public server and publish its details below, so others can try and interoperate with your code.

IETF QUIC Transport

The following stacks implement the IETF versions of QUIC Transport. They may include an application layer mapping other than IETF HTTP over QUIC e.g. HTTP/0.9

[aioquic](#)

QUIC implementation using Python and asyncio.

- **Language:** Python
- **Version:** draft-29
- **Roles:** client, server, library
- **Handshake:** TLS 1.3
- **Protocol IDs:** `0xff00001d`, `0xff00001c`
- **Public server:**
 - quic.aiortc.org:443
 - quic.aiortc.org:4434 (Stateless Retry)

AppleQUIC

AppleQUIC is a client and server implementation.

► Pages 38

Top pages

- [Current "Implementation Draft"](#)
- [QUIC Implementations](#)
- [QUIC Tools](#)
- [QUIC Versions](#)
- [Related Activities](#)
- [Temporary IANA Registry](#)
- [QUIC Extensions Interop](#)

Clone this wiki locally

<https://github.com/quic>



The following are known prototype implementations of [draft-ietf-dnsop-svcb-https](#)

Note some prototypes started off using TYPE65479 and other private types but are now switching over to the production types now that the wire format is stable.

Please feel free to submit PRs to update this page.

Production / shipped implementations

(TBD)

Work-in-progress and prototype implementations

BIND9

[Work-in-progress implementation for BIND9](#)

- Author: Mark Andrews <marka@isc.org>
- Tracker: [BIND9 GL 1132](#)
- Version: Implement draft-ietf-dnsop-svcb-https-01 (work-in-progress) ** Previous versions implemented draft-nygren-httpbis-httpssvc-02 (and -01) and draft-nygren-dnsop-svcb-httpssvc-00 ** Previous versions used TYPENN of HTTPS/65482 and SVBC/65481

Unbound

- Prototype of draft-nygren-httpbis-httpssvc-02 during IETF 105 hackathon

dnspython

[Work-in-progress implementation for dnspython.](#)

Others



IETF QUIC Interop Matrix



File Edit View Insert Format Data Tools Add-ons Help



100% \$ % .0 .00 123 Arial 9 B I A

server →	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W
1	server →	h2o/quickly	quant	ngtcp2	mvfst	picoQUIC	msquic	f5	f5_test	ATS	quiche	lsquic	nginx-cloudflare	AppleQUIC	quic-go	Quinn	AkamaiQUIC	aiolite	~gQUIC	wi	Nego	Haskell QUIC	indur
2	client ↓																						
3	h2o/quickly																						
4	quant		VHDCRSQ MBAUPELT	VHDCRSQ MBAU 3	VHDCRZQ MB 3	VHDCRSQ MBAUP 3	VHDCRSQ MBUP	VHDCRSQ UEL 3			VHDCRSQ 3	VHDCRSQ MBAUPE 3	VHDCRZQ 3			VHDCRSQ MBAUPE 3		VHDCRSQ MBAUP 3	VHDCRQ 3			VHDCRSQ MB 3	
5	ngtcp2			VHDCRS MBAU 3dp	VHDCRZ MBA 3d	VHDCRZS MBAU 3		VHDCRZS U 3d			VHDCRS 3	VHDCRZS MBAU 3dp	VHDCR 3			VHDCRZS MBAU 3d		VHDCRZS MBAU 3dp	VHDCRZ 3d			VHDCRZS MBA 3d	
6	mvfst				VHDCRZQ B 3	VHDCRSQ MBAUP 3																	
7	picoQUIC		VHDCRSQ MBAUPLT	VHDCRSQ MBAUT 3	VHDCRZQ MBAT 3	VHDCRSQ MBAUPLT 3	VHDCRSQ MBAUPT	VHDCRSQ UPLT 3		VHDCRSQ MBA 3	VHDCRSQ 3	VHDCRSQ MBAUPT 3	VHDCRQ 3			VHDCRSQ MBAUP 3		VHDCRSQ MBAUPLT 3	VHDCRQ 3			VHDCRSQ MBATL 3	
8	msquic		VHDCRSQ MBUPL		VHDCRZQ MB 3	VHDCRSQ MBAUP 3	VHDCRSQ MBAUP	VHCRSQ U			VHDCRZQ							VHDCRSQ MBUPL				VHCRSQ MB	
9	f5		VHDCS PELT	VHDCS T 3	VHDC T 3d	VHDCS PL 3	VHDCS P	VHDCS PLT 3d		VHDCS L 3	VHDCS 3d	VHDCS PE 3d	VHDC 3d			VHDCS P 3d		VHDCS P 3d	VHDC 3d			VHDCS T 3	
10	f5_test																						
11	ATS																						
12	quiche																						
13	lsquic			VHDCRSQ MAT 3dp	VHDCRQ T 3d	VHDCRSQ MPT 3	V	VHDCRSQ ET 3d			VHDCRSQ 3	VHDCRSQ MPET 3dp	VHDCRQ 3			VHDCRSQ MP 3d		VHDCRSQ MPT 3dp	VHDCRQ 3d			VHDCRSQ 3d	
14	nginx-cloudflare																						
15	AppleQUIC																						
16	quic-go																						
17	Quinn		VHDCRZS BU	VHDCRZS BU 3d		VHDCRZS BU 3	VHDCRZS BU	VHDCRZS BU 3d			VHDCRZS B 3	VHDCRZS BU 3d	VHDCRZ B					VHDCRZS BU 3d	VHDCRZ B 3d			VHDCRZS B	
18	AkamaiQUIC																						
19	aiolite		VHDCRSQ MBAULT	VHDCRSQ MBAU 3dp	VHDCRZQ MBLT 3dp	VHDCRSQ MBAUPLT 3	VHDCRSQ MBAUPL				VHDCRSQ 3	VHDCRSQ MBAUPT 3dp	VHDCQ 3					VHDCRSQ MBAUPLT 3dp	VHDCRZQ M 3d			VHDCRSQ MBAL 3	
20	~gQUIC		V					VHDCRSQ 3d			VHDCRSQ 3							VHDCRZQ B 3d	VHDCRZQ B 3d				
21	Kwik&Flupke		HDCRZS		HDCRZS 3	HDCRZS 3	HDCRZS				HDCRZS 3				HDCRZS 3			HDCRZS 3					

Maintainability

Support a community of implementers

Current deployment practices

Non-RFC content: wikis and FAQs

Discussion venues

What happens when a working group closes?

TLS Testing Resources

This page lists correctness and safety testing resources for TLS implementations and related software dependencies. It excludes implementation-specific tests.

*Note that **there is no official conformance test suite**.*

- [badssl](#) - Insecure and uncommon server configurations
- [BoGo](#) - Test harness for (D)TLS, supported by BoringSSL and [NSS](#). See [PORTING.md](#) for information about supporting other implementations.
- [TLS Attacker](#) - TLS-Attacker is a Java-based framework for analyzing TLS libraries.
- [tlsfuzzer](#) - Fuzzer and test suite for TLS (SSLv2, SSLv3, v1.0, v1.1, v1.2, v1.3) implementations.
- [Frankencerts](#) - Specially crafted certificates for testing certificate validation code in TLS implementations.

The following tools lists may help identify features or properties of different TLS implementations:

- [SSL Labs Browser and Server Tester](#) - Browser-based tool for checking features of TLS servers and browser implementations.

Tasks

Get representatives from IESG, Tools Team,
broader community

Review successful models in working groups

Review cases where protocols struggle

Output

Write documents

Hold workshops

Build new IETF tools

Provide guidance for WGs and IETF reviews

Open Mic

How did you like the IABopen session? Should we do it again? Is it useful?

What would you expect from future IABopen meeting?

Other technical comments or feedback on the IAB work or Internet architecture in general?