HotRFC Lightning Talks at IETF-114

Sunday, July 24, 2022
18:00-20:00 US EDT
Room: Liberty B
Organizers: Aaron Falk, Spencer Dawkins
Email: hotrfc@ietf.org
Call for Participation

MEETING AGENDA

What has the IETF ever done for Energy

Challenges and Opportunities in Green Networking

Challenges and Opportunities in Post-Quantum Cryptography for networks and protocols

Internet Of Secure Elements

Attestation within TLS

The LEO satellite networking, the flying infrastructure for future Internet.

Beyond End-to-End security

Challenges in Operations and Control Networks (OCN)

Enterprises and Organizations need help from ECH work on how to organize their operational security

A Data-driven Approach to Tackle Network Diversity with Heterogeneous Protocol Configurations.

Multicast QUIC

Network Latency — why it matters, how to measure it, what to do about it

---

ABSTRACTS

What has the IETF ever done for Energy

Presenter: Toerless Eckert, <tte@cs.fau.de>
Affiliation: Futurewei USA

Datatracker slides here

Abstract: This memo provides an overview of work performed by or proposed within the IETF related to energy and/or green: awareness, management, control or reduction of consumption of energy, and sustainability as it relates to the IETF.

Target: Enlightenment, spur interest in new work
Goal: looking for collaborators
URL: https://github.com/toerless/energy
Slides:
https://github.com/toerless/energy/raw/main/what-has-the-ietf-ever-done-for-energy.pdf

---

Challenges and Opportunities in Green Networking

Presenter: Alexander Clemm (Futurewei, USA), ludwig@clemm.org

Datatracker slides here

Abstract: Reducing technology's carbon footprint is one of the big challengesof our age. Networks are an enabler of applications that reduce this footprint, but also contribute to this footprint substantially themselves. The biggest opportunities to reduce the energy footprint may not be networking specific, for instance general power efficiency gains in hardware or hosting of equipment in more cooling-efficient buildings. However, methods to make networking technology itself "greener" also need to be explored. One of the prerequisites here concerns related network instrumentation providing metrics that, when provided visibility into, can help to optimize a network's energy efficiency and "greenness". This presentation gives a brief pitch on those topics and some freshly submitted companion Internet Drafts.

References:

Green Networking Metrics (draft-cx-green-metrics-00),
https://datatracker.ietf.org/doc/html/draft-cx-green-metrics-00

Challenges and Opportunities in Green Networking (draft-cx-green-ps-00),
https://datatracker.ietf.org/doc/html/draft-cx-green-ps-00

Goal: find collaborators - contact me via email or look for me in the hallway

---

Challenges and Opportunities in Post-Quantum Cryptography for networks and protocols

Presenter, Affiliation: Sofía Celi, Brave

Datatracker slides here

Abstract: The Post-Quantum NIST process for selecting post-quantum algorithms have reached its first milestone: selecting algorithms for confidentiality and authentication that are safe from quantum attacks. However, these selected algorithms have parameters or computational times that are bigger than non-post-quantum ones, which could pose a problem for the protocols and networks as we use them today: TLS, DNSSEC, IPSEC and more. In this talk, we will walk to an overview of the post-quantum algorithms, how they affect the protocols and network (challenges and opportunities), and what we can as IETF to migrate them.

Coordinates to learn more, contact those involved, &/or relevant formal or side meetings:
Contact: Sofía Celi, cherenkov@riseup.net,

https://sofiaceli.com/PQNet-Workshop/,
https://sofiaceli.com/slides/PQC_KEMTLS.pdf ,
https://sofiaceli.com/PQNet-Workshop/dnssec.html ,
https://sofiaceli.com/PQNet-Workshop/tls.html ,
https://sofiaceli.com/2022/07/05/pq-signatures.html ,
https://datatracker.ietf.org/meeting/111/materials/slides-111-saag-how-should-the-ietf-approach-post-quantum-security-02,
https://github.com/rdanyliw/ietf-pq-maintenance/blob/main/pqm-charter.md

---

Internet Of Secure Elements

Presenter: Pascal Urien Telecom Paris

Datatracker slides here

Abstract: Secure elements are widely used in bank cards, SIM modules, electronic passports. More than 6 billion javacards are deployed. They communicate through the ISO7816 interface, and are able to support TLS1.3 stacks. Internet of secure element is an IETF draft that defines a server (IOSE servers) based on secure element TLS server (TLS-SE). Open implementations are available on github for IOSE server and associated TLS-SE secure elements. Secure elements are identified by TLS server name (SEN), they act as a back end server connected to a front TLS server.

Secure element resources are identified by URI such as schemeS://sen:psk@server.com:port/?query, in which psk is a TLS pre-shared-key. The definition of protocols used above TLS-PSK, in order to access secure element resources, is an open issue.

References:
https://datatracker.ietf.org/doc/draft-urien-coinrg-iose/05/
https://github.com/purien/IoSE
https://github.com/purien/TLS-SE

Contact: Pascal.urien@gmail.com

Attestation within TLS

Presenter: Hannes Tschofenig (Arm)

Datatracker slides here

Abstract: Attestation is an important building block in modern hardware security technologies, such as confidential computing. To offer interoperability attestation formats have been standardized. These attestation tokens need to be conveyed to a relying party to be useful and we have made an attempt to integrate these tokens into the TLS handshake.

Reference: https://datatracker.ietf.org/doc/html/draft-fossati-tls-attestation-00

Contact: Hannes.Tschofenig@arm.com

The LEO satellite networking, the flying infrastructure for future Internet.

Presenter: Lin Han, Futurewei Technologies, Inc.

Datatracker slides here

Abstract: The massive number of LEO satellites connected by Inter-satellite link will make the LEO satellite network an infrastructure network. It can be integrated with the latest wireless technologies, 5G and beyond, for future Internet. 3GPP has expected that the LEO satellite network will provide the IP transport for its NTN integration architecture. As a complementary part of terrestrial network, LEO satellite network can provide truly global coverage with shorter latency for people's communication, massive IOT and even edge computing service from space. However, all the benefits are not free. Due to the fast and special moving pattern of LEO satellite network, there are many challenges to the current IETF technologies, such as addressing, routing, multi-path, mobility, traffic engineering, security, etc. Some sporadic drafts have been in IETF recently, but there is no dedicated group for all those works. We expect that more coordinated work is done in IETF/IRTF for this area.

For follow-up:

- We will have side meeting at IETF 115 (London)
- Reach out to me lin.han@futurewei.com or send to etosat@ietf.org, if you want to present something in the side meeting; or want to discuss details; or want to collaborate.

Beyond End-to-End security

Presenter: Phillip Hallam-Baker <phill@hallambaker.com>, Threshold Secrets LLC

Datatracker slides here

End-to-End security has always been held as the gold standard for personal security. Recent events require this assumption to be reconsidered. The current model of proprietary service providers offering end-to-end security within separate walled gardens is no longer acceptable.

End-to-End security only protects the data in transit between the end-points and in storage at the service provider. It does not provide protection against key substitution attacks or compromise of the messaging applications. Nor do 'warrant canaries' provide an effective control.

Providing adequate security in the new threat environment requires that the messaging system be open and the user be in complete control of their contacts catalog. The Mathematical Mesh plus WebRTC provides such an infrastructure for messaging, voice and video modalities.

Next Steps: The Mesh + WebRTC provides more than enough mechanisms to support an open, end-to-end secure and warrant resistant communication system. The question is what parts of the WebRTC infrastructure to choose.

Coordinates for following up: I am interested in talking to people who are interested in collaborating on such a project, in particular people with WebRTC expertise.

Challenges in Operations and Control Networks (OCN)

Presenter: Lijun Dong, Futurewei Technologies Inc., USA

Datatracker slides here

Abstract: The emergence of applications in industry verticals based on machine-to-machine communications require control systems to be extended beyond their closed environments. Specifically, such systems that bring about physical and mechanical changes to an environment, heavily rely on their remote operations and control.

While IETF has produced standards for constrained IoT devices, industrial device operations differ in many ways. There are issues associated with the network-based remote operations in such control systems when those operations are extended beyond closed networks. These issues and candidate scenarios are captured in the following documents [1-4].

The term Operations and Control networks (OCN) describes the communication characteristics for such control systems. There are several customized and proprietary network technologies available, however a common network reference model and framework would allow operators from different verticals to leverage open protocols.

We invite the IETF community to a side-meeting OCN discussion on the requirements for establishing common interfaces and functions.

Coordinates to learn more, contact those involved, &/or relevant formal or side meetings

Date : Monday 25 July (see: https://trac.ietf.org/trac/ietf/meeting/wiki/114sidemeetings#point1)
Time: 12:30 to 1:20 pm (50 minutes)
Room: Horizon at rooftop (R Floor)
contact: lijun.dong@futurewei.com , kiran.ietf@gmail.com

Webex:
https://futurewei.my.webex.com/futurewei.my/j.php?MTID=m8482bdb06635d5ef021e6dcc11d1cd29

References:

[1] https://datatracker.ietf.org/doc/draft-km-intarea-ocn/
[2] https://datatracker.ietf.org/doc/draft-tf-ocn-ps/
[3] https://datatracker.ietf.org/doc/draft-dong-remote-driving-usecase/
[4] https://datatracker.ietf.org/doc/draft-wmdf-ocn-use-cases/

Enterprises and Organizations need help from ECH work on how to organize their operational security

Presenter: Arnaud Taddei, Broadcom

Datatracker slides here

Abstract:

https://datatracker.ietf.org/doc/html/draft-taddei-ech4ent-introduction-00.html

This paper reviews some of the Enterprises and Organizations requirements and constraints and tests the current Encrypted Client Hello (ECH) proposal in these environments. In particular it highlights the need for several clarifications as well as highlights known attack vectors which will become easier with the current ECH proposal. The current ECH drafts should consider how they want to include enterprises' operational security capabilities to mitigate these attacks.

Modalities: I will unfortunately be remote in Europe

Followup:

Proposal to have an adhoc call by google meet on 26th at 7:30pm CEST
Contact the contributor for anything: Arnaud.Taddei@broadcom.com

---

A Data-driven Approach to Tackle Network Diversity with Heterogeneous Protocol Configurations.

Presenter: Usama Naseer, Brown University

Datatracker slides here

Contact: usama_naseer@brown.edu

Coordinates to learn more:
https://www.usenix.org/conference/nsdi22/presentation/naseer

Abstract: The web serving protocol stack is constantly evolving to tackle the technological shifts in networking infrastructure, end-user devices and website complexity. As a result of this evolution, CDN edge servers can use a plethora of protocols and configuration parameters to address a variety of realistic network conditions. Yet, today, despite the significant diversity in end-user networks and devices, most content providers have adopted a “one-size-fits-all” approach towards configuring the edge networking stack.

In this work, we demonstrate that the status quo results in sub-optimal performance and our measurements show that dynamic tuning can significantly improve web performance, as compared to today’s edge network configurations. However, dynamic tuning at the edge requires a flexible data-path that can tune configurations on a per-connection manner, and a data-driven control-plane that can minimize the costs associated with searching the optimal configurations. Our framework, Configanator, makes contributions across both dimensions and leverages data across connections to identify their network and device characteristics, and learn the optimal configuration parameters to improve end-user performance. The optimal configurations are then used for serving the content from the edge, based on a connection’s network and device’s characteristics. Our real-world deployment and trace-driven evaluation shows that Configanator improves tail (p95) web performance by 32-67% across diverse websites and networks.

Multicast QUIC

Presenter: Jake Holland, Akamai

Datatracker slides here

Abstract: A proposed extension to QUIC aims to use IP Multicast to securely solve the thundering herd problem of too-high traffic demand for popular content, ultimately including web video.

Coordinates to learn more:
- QUIC wg session: https://datatracker.ietf.org/meeting/114/materials/agenda-114-quic-00
- Datatracker: https://datatracker.ietf.org/doc/draft-jholland-quic-multicast/
- Document repo: https://github.com/GrumpyOldTroll/draft-jholland-quic-multicast
- W3C Multicast Community Group: https://www.w3.org/community/multicast/
  (currently working on a reference implementation)
- write the authors: draft-jholland-quic-multicast@ietf.org

Network Latency — why it matters, how to measure it, what to do about it

Stuart Cheshire, Apple

Datatracker slides here

Abstract: Everyone at the IETF thinks they know about bandwidth and latency, but do we really? We're learning that working latency (latency while a link is being used) can be 100x more than the idle latency, or worse. We need better tools to measure working latency, and we need technologies like L4S that allow links to deliver latency while in use that's as good as their latency when idle. Armed with better measurement tools, we can then use those tools to evaluate L4S and similar network improvements and to guide their continued development and deployment.

Background

Latency Explained
<https://www.bitag.org/latency-explained.php>
Apple WWDC 2022: Reduce networking delays for a more responsive app
<https://developer.apple.com/videos/play/wwdc2022/10078/>
Introducing a Better Measure of Latency (background)
<https://www.ookla.com/articles/introducing-loaded-latency>

At IETF 114:

Meet the L4S team at Hackdemo (Monday, 17:30-18:30, in Liberty A)

Responsiveness under Working Conditions
(to be discussed in IPPM on Friday)
<https://datatracker.ietf.org/doc/html/draft-ietf-ippm-responsiveness>
