Compiled by Dr. Balaji Rajendran and Ms. Akanskha Gupta with inputs from Shri. Anil Kumar V, Shri. Jitendra Kumar, Shri. Harish Chowdhary and Shri. Anoop Kumar Pandey.

Table of Contents

ABSTRACT

This report summarizes the major developments in IETF 104. The following IIREF Fellows selected and attended the meeting, Shri Jitendra Kumar (Principal Technical Officer, CDAC Bangalore), Shri Anoop kumar Pandey (Principal Technical Officer, CDAC Bangalore), Shri Harish Chowdhury (Technology Analyst National Internet Exchange of India), Shri Anil Kumar V (Senior Principal Scientist, CSIR Fourth Paradigm Institute).

This report brings out the major developments in the following Working Groups in IETF 104:

•Development in TLS 1.3 (Transport Layer Security) and Internet Research labs including IoT, IPV6, Dprive (DNS PRIVate Exchange), DNSOP (DNS Operations), QUIC (Quick UDP Internet Connection), DNS over HTTPS, BOF (Birds of feather) discussions, EMU (EAP Method Update), ANIMA (Autonomic Networking Integrated Model and Approach), SUIT (Software Updates for Internet of Things), ACME (Automated Certificate Management Environment), DOTS (DDoS Open Threat Signalling), WAP (Web Authorization Protocol), Security Area Open Meeting" (SAAG), Domain Name System Operations (Dnsop), Information-Centric Networking (ICNRG),Multipath TCP (mptcp).

• E-mail address internationalization and Universal Acceptance Issues.

• Establishment of Remote hubs in INDIA through IETF processes.

1. Mooting the Establishment of Internet Research Labs

Shri Harish Chowdhury (IIREF Fellow) described his draft on Internet Research Labs and requested to share thoughts on the possible infrastructural requirements for setting a lab for future works in T2TRG.

The abstract of the draft [*draft-chowbat-irl*]: Many people learn technical concepts best in a hands-on environment, and Internet protocols and standards are no exception. Internet Research Labs (IRL) will facilitate a platform and encourage the technical community (seasoned professionals and newcomers alike) to discuss, collaborate, design and develop utilities, ideas, sample code and solutions that show practical implementations (Proof of Concept) of existing IETF standards. These labs may also be used by the IETF Mentoring Program and/or EDU teams for hands-on training to mentees or newcomers. This base draft [*draft-chowbat-irl*] intends to provide a high-level overview of the concept of Internet Research Labs in terms of objectives, requirements, challenges and deliverables without going into details of a specific lab, technology or an IETF Working Group (WG). After this draft matures and gains traction within the IETF community, they foresee more and more Internet drafts for the specific labs.

2. Quick UDP Internet Connection (QUIC)

QUIC represents the most significant evolution of the transport layer since the advent of TCP. QUIC takes the stream model of HTTP/2 and embeds it in the transport layer, so that a single connection can make progress on a stream even if packets containing data from other streams are lost– thereby mitigating the head-of-line blocking problem in the transport as well as the application layer. QUIC is built on top of UDP.QUIC hides much of this state from observers, ensuring that it remains a flexible, end-to-end protocol.

The IETF isn't work on QUIC from scratch. In 2012, Google designed its own version of QUIC and then deployed it both in its popular Chrome browser and most of its services, including Youtube and search. This allowed them to observe the protocol in action and tweak its design before submitting it to the IETF for consideration in 2016. The IETF QUIC Working Group took Google's documents as input, and has created a set of drafts that used them as a starting point.

QUIC now has several important changes from Google's input documents. In fact, every aspect of the wire protocol has been changed. The biggest change is in how negotiation is encrypted. Google QUIC's bespoke encryption handshake was new to many, whereas Transport Layer Security (TLS) is more widely understood, has more features, and is much more widely supported in both implementations, and deployment. Considering the investment, the community has in TLS research, security analysis, implementation, and deployment, the QUIC Working Group was chartered to use it as the basis of encryption in QUIC.

When an QUIC handshake starts, the TLS handshake takes place inside of the QUIC frames, so that the peers can authenticate each other and derive session keys form encryption. Once that takes place, those keys are used to encrypt the QUIC frames.

As a result, when an QUIC handshake starts, the TLS handshake takes place inside of the QUIC frames, so that the peers can authenticate each other and derive session keys form encryption. Once that takes place, those keys are used to encrypt the QUIC frames. There are currently more than fifteen experimental implementations of QUIC.

3.DNS OVER HTTPS - (DOH)

Discussions about deployment considerations for DNS confidentiality in the DNS Over HTTPS (DNS Over HTTPS) and DNS PRIVate Exchange (DNS PRIVate Exchange) working groups as well as a side meeting allowed participants to air their concerns and explore in more detail the specific deployment plans of individual providers. Discussion will continue on the Applications Doing DNS (ADD) mailing list.

Paul Hauffman presented the agenda of Resolving issues in the draft [draft-ietf-doh-resolver-associated-doh], "Associating a DoH Server with a Resolver". Brian Dickson mentioned one important issue with the use of possibly DoH servers where there are existing chains of forwarders. It need to be able to disambiguate entities in the forward chain, who identify themselves separate from this. Later Jason Livingood and Jim Reid presented draft [draft-livingood-doh-implementation-risks-issues] on Centralized DNS over HTTPS (DoH) Implementation Issues and draft [draft-reid-doh-operator] on Risks and DNS over HTTPS (DoH) Considerations for Operator Networks.

4.Birds of A Feather Sessions (BOF)

Sometimes an issue that has been discussed on a mailing list or a proposal for a new idea cannot be fully understood without an opportunity for those interested to gather together in physical space for discussion. IETF 104 showcased the many different ways in which having a physical meeting can substantially advance the work of IETF community over the course of time. Before each IETF meeting, the Internet Engineering Steering Group (IESG) collects proposals for Birds of a Feather (BOF) sessions. These, sessions help determine the path for new work in the IETF or to generate discussion about a topic within the IETF community.

BOF (Birds of a Feather) Session 1: Collaborative Automated Course of Action Operations (CACAO): The goal of the CACAO work is to enable collaborative courses of action (known as playbooks) to be shared between security operations centers on timescales fast enough to help organizations mitigate ongoing attacks.

Playbooks in use today are typically written as formal documents that spell out step-by-step instructions for how an organization can respond to a specific type of attack on its infrastructure.

Playbooks in use today are typically written as formal documents that spell out step-by-step instructions for how an organization can respond to a specific type of attack on its infrastructure. This is a working-group-forming BOF.

BOF (Birds of a Feather) Session 2: Broadband Network Gateway Control-Plane and User-Plane Separation (BCAUSE): The rise of virtualization and disaggregation in broadband access networks has created interest among network operators in separating the subscriber management control plane from the traffic forwarding user plane. A series of Internet-Drafts have been developed in the Routing Area Working Group (RTGWG) to specify a separation architecture and solution. This BOF seeks to form a working group to advance these documents outside of the RTGWG. Participants have been in active correspondence with the Broadband Forum (BBF), which has been working on requirements in this area.

BOF (Birds of a Feather) Session 3: Key Signing Key Futures (KSKF): The key signing key (KSK) for the DNS root was changed for the first time on 11 October 2018. This non-working-group forming BOF hosted discussion about the future of the root zone KSK, including how often to change the KSK, requirements to be met before making the next change, adding additional standby KSKs to the root zone, and changing the signing algorithm.

BOF (Birds of a Feather) Session 4: Brand Indicators for Message Identification (BIMI): The aim of the BIMI work is to permit owners of domain names to coordinate with providers of mail clients to display brand-specific indicators (such as logo images) next to properly authenticated messages when recipients view messages in their mail clients.

Permit owners of domain names to coordinate with providers of mail clients to display brand-specific indicators

Work on BIMI has been motivated by a desire to mitigate phishing attacks and to drive adoption of email authentication protocols. Mailing list discussion of concerns with this proposal as well as its potential benefits has been robust already. The

5. TLS 1.3 Sessions

The Datagram Transport Layer Security (DTLS) Protocol Version 1.3:

Abstract of the Draft [draft-ietf-tls-dtls13]: This document specifies Version 1.3 of the Datagram Transport Layer Security (DTLS) protocol. DTLS 1.3 allows client/server applications to communicate over the Internet in a way that is designed to prevent eavesdropping, tampering, and message forgery. The DTLS 1.3 protocol is intentionally based on the Transport Layer Security (TLS) 1.3 protocol and provides equivalent security guarantees. Datagram semantics of the underlying transport are preserved by the DTLS protocol. In addition to the above following drafts at TLS WG were presented:

- **Deprecating TLSv1.0 and TLSv1.1 [draft-ietf-tls-oldversions-deprecate]:** This document, if approved, formally deprecates Transport Layer Security (TLS) versions 1.0 [RFC2246] and 1.1 [RFC4346] and moves these documents to the historic state. These versions lack support for current and recommended cipher suites. TLSv1.2 has been the recommended version for IETF protocols since 2008.

This document updates many RFCs that normatively refer to TLS1.0 or TLS1.1. This document also updates RFC 7525 and hence is part of BCP195.

- **TLS 1.3 Extension for Certificate-based Authentication with an External Pre-Shared Key [draft-ietf-tls-tls13-cert-with-extern-psk]:** This document specifies a TLS 1.3 extension that allows a server to authenticate with a combination of a certificate and an external pre-shared key (PSK). First, the server can be authenticated by providing a signature certificate and creating a valid digital signature to demonstrate that it possesses the corresponding private key. Second, the server can be authenticated by demonstrating that it possesses a pre-shared key (PSK) that was established by a previous handshake. A PSK that is established in this fashion is called a resumption PSK. A PSK that is established by any other means is called an external PSK.

- **TLS Authentication using ETSI TS 103 097 and IEEE 1609.2 certificates:** This specifies the use of a new certificate type to authenticate TLS entities. The first type enables the use of a certificate specified by the Institute of Electrical and Electronics Engineers (IEEE) and the European Telecommunications Standards Institute (ETSI).

- **Encrypted Server Name Indication for TLS 1.3**

This draft [draft-ietf-tls-esni] describes the general problem of encryption of the Server Name Identification (SNI) parameter. The proposed solutions hide a Hidden Service behind a Fronting Service, only disclosing the SNI of the Fronting Service to external observers. The draft lists known attacks against SNI encryption, discusses the current" co-tenancy fronting" solution, and presents requirements for future TLS layer solutions. This draft is adopted as the WG draft in IETF 102. This document defines a simple mechanism for encrypting the Server Name Indication for TLS 1.3 with the disclaimer: "*This is very early a work-in progress design and has not yet seen significant (or really any) security analysis. It should not be used as a basis for building production systems*".

6. EAP Method Update (EMU)

6 drafts [draft-ietf-emu-rfc5448bis], [draft-ietf-emu-eap-tls13], [draft-dekok-emu-eap-session-id], [draft-aura-eap-noob], [draft-lear-eap-teap-brski], [draft-pala-eap-creds] were presented. The draft [draft-ietf-emu-eap-tls13] recommended pervasive monitoring of the mandatory privacy protection of identities and also differentiating between TLS fatal alerts and warning alerts. Another draft about "large certificates and long chain certificates" addresses considerations about the contents of certificates. The draft was not reviewed. Review has been already sent and further discussion is going on through email. EAP-NooB (Nimble out of band)" described EAP method for bootstrapping devices out-of-the-box without professional administration – without the assumption that the device has any identity. The major change since last meet was an addition of one round trip to each exchange to deliver the latest PeerId and peer state to the server without updating NAI (to comply with RFC 3648) and better randomization.

Misbinding attacks are possible - if the UI is compromised on a device, then the user might be tricked in pairing with another device instead of the desired (compromised) one.

The author mentioned, "misbinding attacks are possible - if the UI is compromised on a device, then the user might be tricked in pairing with another device instead of the desired (compromised) one. There are different ways to mitigate that problem: device certificates, asset tracking through organization, etc. The report is available as a research *paper and more in SAAG.*" Another draft "Bootstrapping Key Infrastructure over EAP" addressed autonomous on boarding of wired devices (requires initial IP configuration).

7. Autonomic Networking Integrated Model and Approach (ANIMA)

Michael Richardson presented Bootstrapping Remote Secure Key Infrastructures (BRSKI) and Constrained Voucher Artifacts for Bootstrapping Protocols. BRSKI specifies automated bootstrapping of an Autonomic Control Plane. To do this a remote secure key infrastructure (BRSKI) is created using manufacturer installed X.509 certificate, in combination with a manufacturer's authorizing service, both online and offline. Peter Van Stok presented Constrained Join Proxy for Bootstrapping Protocols. There was a lot of discussion on unconstrained BRSKI vs constrained one. Michael Richardson opined that unsigned pledge requests from BRSKI should be removed. Eliot Lear presented a variation of BRSKI over IEEE 802.11 and EAP. Bing Liu (remote participation) discussed Scenarios and Requirements for Layer 2 Autonomic Control Planes.

8. Software Updates for Internet of Things (SUIT)

David Waltermire presented an overview of the draft [draft-ietf-suit-architecture] that discussed SUIT architecture, information model, manifest format and hash-based signatures, Firmware Image, Homogeneous Storage Architecture (HoSA), System on Chip (SoC). Firmware Image etc. Brendan Moran presented the draft [draft-ietf-suit-information-model], the chair asked whether the document is ready for WG Last Call. Chairs proposed to begin four-week WG Last Call, which should allow time for people to get caught up after the IETF meeting and then review the document. In another draft [draft-moran-suit-manifest-04], describes the format of a manifest

A manifest is a bundle of metadata about the firmware for an IoT device, where to find the firmware, the devices to which it applies, and cryptographic information protecting the manifest. Emmanuel Baccelli (INRIA) mentioned, "There is a significant increase in code size in the current version. Based on Hackathon coding, the previous version was about 600 bytes of code size. This version is 3x larger. For a device with 64kB of flash memory, this is a significant increase."

A manifest is a bundle of metadata about the firmware for an IoT device, where to find the firmware, the devices to which it applies, and cryptographic information protecting the manifest.

After the conclusion of the meeting Shri Jitendra kumar (IIREF Fellow) met Russ Housley (in the picture below) and discussed the *draft [draft-enhanced-xml-digital-signature-algorithm-01]* and asked about finding a suitable working group as this draft suggest few modifications in the RFC 3275 and the working group which devised RFC 3275 is now not active. Russ Housley further suggested Shri Jitendra to talk to Roman Danyliw area director Security Dispatch (secdispatch), interaction with Roman was fruitful.

9. Automated Certificate Management Environment (ACME)

Discussion was mostly focused on device certificate, code signing certificate, STAR (Short-term Automatically Renewed Certificates) and 3rd-party device attestation for ACME.

10. Crypto Forum

Randomness improvements for Security Protocols draft [draft-cremers-cfrg-randomness-improvements], BLS (Boneh–Lynn–Shacham) signatures draft [draft-boneh-bls-signature] and Hybrid Public Key Encryption draft [draft-barnes-cfrg-hpke-00] were discussed. Authors of BLS Signature Scheme requested feedback on securing the scheme against rogue public-key attacks and which cipher suites to support. Stanislav V. Smyshlyaev gave overview of existing PAKEs and PAKE (Password-Authenticated Key Agreement) selection criteria. Brook Schofield gave an invitation to bid for research/innovation funding in support of NGI (Next Generation Internet).

11. Web Authorization Protocol (WAP)

Aaron Parecki presented the current status and incremental change in the draft "OAuth 2.0 for Browser-Based Apps". It is written in JavaScript with no backend and require auth code flow with PKCE without any implicit flow. Browser based apps should not get refresh tokens. Torsten suggests that all the oauth processing can be pushed to backend, so one proposal is to make this all about Oauth in browser, not about backend. Hannes Tschofenig presented PoP Key Distribution. The OAuth 2.0 Proof-of-Possession security concept extends bearer token security and requires the client to demonstrate possession of a key when accessing a protected resource. Drafts like MTLS Update, Nested JWT and DPoP (Demonstrating Proof-of-Possession) were discussed: [draft-ietf-oauth-pop-key-distribution], [draft-ietf-oauth-mtls], [draft-yusef-oauth-nested-jwt].

12. DDoS Open Threat Signalling (DOTS)

Kaname Nishizuka presented a draft [draft-nishizuka-dots-signal-control-filtering-04] on controlling Filtering Rules Using DOTS Signal Channel. Jon Shallow presented Interoperability and Hackathon Report. Tiru Reddy discussed draft [draft-ietf-dots-multihoming-01] "Multihoming Deployment Considerations". He mentioned that the mid in forking cases may cause problems because different servers may return different results. Yuhei Hayashi discussed draft [draft-hayashi-dots-dms-offload-usecase-00] and various DDoS Mitigation Offload use cases.

13. Security Area Open Meeting (SAAG)

Tuomas Aura presented on a misbinding attack possiblity in many pairing protocols. He illustrated the case of EAP-NooB which may involves relay of out-of-band message from compromised device to attacker. Aura claimed that it can't be mitigated entirely, but some methods can make attacker's life more difficult. Few suggestions are to bind non-modifiable device identifiers, use device certificates to attest device and asset tracking.

Shri Anoop kumar pandey (IIREF Fellow) asked several questions and gave suggestion on how EAP NooB can be improvised to tackle misbinding attack.

Mattson presented on the SNOW-V cipher. The motivation comes from the fact that minimum 20G bps downlink speed is there in 5G, so similar performance is desired for encryption. SNOW V belongs to Lund University, based on earlier SNOW 3G. The software implementation of encryption can reach 50Gbps on a single-thread on laptop CPU.

14. Domain Name System Operations (DNSOP)

Pallavi Aras and Shumon Huque presented a draft [draft-ietf-dnsop-multi-provider-dnssec], which illustrates problems about enterprises employing service of multiple DNS providers to distribute their authoritative DNS service. Deploying DNSSEC in such an environment can have some challenges depending on the configuration and feature set in use. The draft presents several deployment models that may be suitable.

15. Information-Centric Networking (ICNRG)

In the Information-Centric Networking (ICNRG) discussion, several important topics like "A keyword-based naming for in-network computing", "Pub-Sub with ICN", "Efficient Blockchain access via ICN" were addressed. The working group members observed that there has not been a significant contribution to NDN (Named Data Networking) Tools Overview, Status, and future plans, NFN (Named Function Networking) Update and Broadcast-only communication models and also discussed about summary of Berkeley CFN workshop (relates to INC and NFN topics).

16. Multipath TCP (mptcp)

Shri V Anil Kumar participated in the Multipath TCP (mptcp) working group which develops mechanisms that add the capability of simultaneously using multiple paths to a regular TCP session. Key goals for MPTCP are: to be deployable and usable without significant changes to existing Internet infrastructure; to be usable by unmodified applications; and to be stable and congestion-safe over the wide range of existing Internet paths, including NAT interactions. Discussion was held on meta and sub-socket level interaction of MPTCP framework in Linux kernel, design and implementation of adaptive scheduler for mptcp, design issues for low-latency (low-RTT) mptcp option exchange, etc. some of these points were discussed in depth in the mptcp working group side meeting, which was held prior to the main meeting of mptcp working group.

The following Individual Drafts were presented in this group:

[draft-ietf-mptcp-rfc6824bis], [draft-defoy-mptcp-considerations-for-5g], [draft-defoy-5g-session-continuity-support-in-mptcp], [draft-kang-mptcp-initial-path-selection].

17. Acknowledgement

We would like to thank Internet Governance division, Ministry of Electronics and Information Technology (MeitY), Government of India.

Photographs:

Shri T Santosh, Shri Harish Chowdhury, Shri Anoop kumar Pandey,

Shri V Anil Kumar, Shri Jitendra Kumar

Shri Jitendra kumar (IIREF Fellow) with Russ Housley and Roman Danyliw

References

1. IETF Hackathon Presentations:

   https://github.com/IETF-Hackathon/ietf104-project-presentations

2. QUIC WG Link of Implementation:
   https://github.com/quicwg/base-drafts/wiki/Implementations

3. DNS over HTTPS

   https://datatracker.ietf.org/doc/draft-ietf-doh-resolver-associated-doh/

4. EAP NooB Hackathon Summary:

   https://github.com/IETF-Hackathon/ietf104-project-presentations/blob/master/IETF104-EAP-NOOB-hackathon-2019-prague.pdf

5. TLS 1.3 Sessions:

   https://datatracker.ietf.org/meeting/104/materials/agenda-104-tls-03

6. EMU MoM:
   https://datatracker.ietf.org/meeting/104/materials/minutes-104-emu-00

7. ETF104-SAAG-20190328-1350:
   https://www.youtube.com/watch?v=j5icH62blf4 from 34:45

8. DoH Implementation Risks and Operations Considerations:
   https://datatracker.ietf.org/meeting/104/materials/slides-104-doh-draft-ietf-doh-resolver-associated-doh-00

9. IETF 104 Agenda:

   https://datatracker.ietf.org/meeting/104/agenda/

10. draft-huque-dnsop-multi-provider-dnssec-04
    https://tools.ietf.org/html/draft-huque-dnsop-multi-provider-dnssec-04

11. Multipath TCP

- https://datatracker.ietf.org/doc/draft-ietf-mptcp-rfc6824bis/
- https://datatracker.ietf.org/doc/draft-defoy-mptcp-considerations-for-5g/
- https://datatracker.ietf.org/doc/draft-defoy-5g-session-continuity-support-in-mptcp/
- https://datatracker.ietf.org/doc/draft-kang-mptcp-initial-path-selection/

Glossary

IETF	: Internet Engineering Task Force
IAOC	: IETF Administrative Over-Site Committee
IAB	: Internet Architecture Board
EDCO	: Enterprise Data Center Operators
QUIC	: Quick UDP Internet Connections
IESG	: Internet Engineering Steering Group
IRTF	: Internet Research Task Force
HRPC	: Human Right Protocol Considerations
IAD	: IETF Administrative Director
IIREF	: Indian Internet Research & Engineering Forum
ISOC	: Internet Society
IIESoc	: India Internet Engineering Society
HoSA	: Homogeneous Storage Architecture
NCSC	: National Cyber Security Centre
CACAO	: Collaborative Automated Course of Action Operations
BCAUSE	: Broadband Network Gateway Control-Plane and User-Plane Separation
KSKF	: Key Signing Key Futures
BIMI	: Brand Indicators for Message Identification
DTLS	: Datagram Transport Layer Security
PSK	: Pre-shared key
ETSI	: European Telecommunications Standards Institute
SNI	: Server Name Identification
EMU	: EAP Method Update)