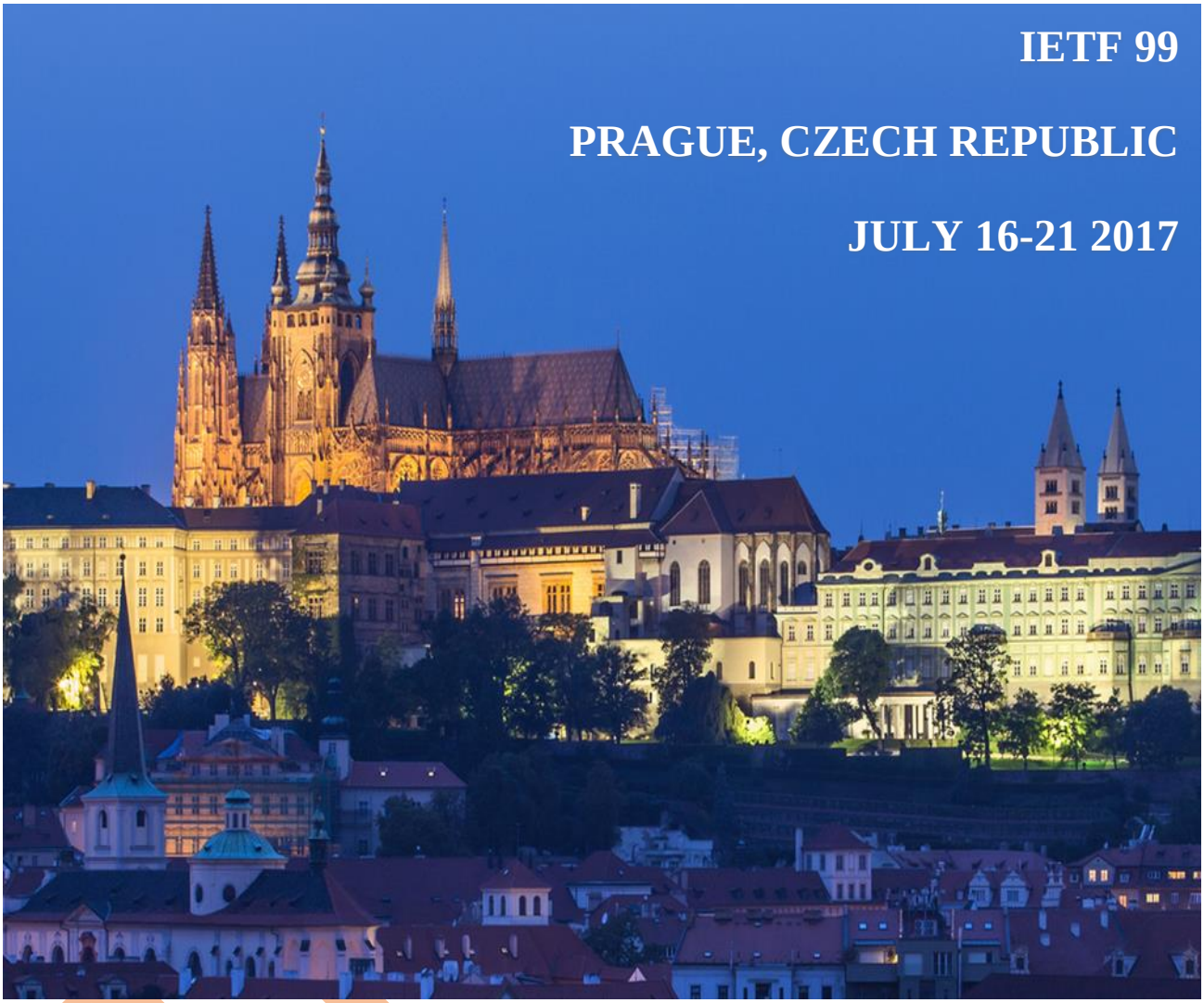
IETF 99
PRAGUE, CZECH REPUBLIC
JULY 16-21 2017

CONTENTS

1. EXECUTIVE SUMMARY

In this report we are sharing the experiences and outcomes of the Internet Engineering Task Force (IETF) 99 meeting in Prague, Czech Republic from July 16-21 2017 by our IIREF fellows Dr. Balaji Rajendran (Principal Technical Officer, Centre for Development of Advanced Computing) & Mr. Harish Chowdhary (Technology Analyst, National Internet Exchange of India).

IETF 99 meeting was important due to the following reasons like actively work in the process for RFC (Internet Standard) creation, To discuss work on TLS 1.3 (Transport Layer Security) and Internet Research labs including IoT,EAI,IPV6,Dprive and security. Establishment of Remote hubs in INDIA through IETF processes, discuss "Internet Research Labs (IRL)" internet Draft with the IETF Community, discuss "Geographically focused IETF activities Internet Draft.

There are several benefits and learnings that Dr.Balaji Rajendran & Mr. Harish Chowdhary gained from the visit which otherwise could not have been possible.

2. MAJOR DISCUSSIONS IN DIFFERENT WORKING GROUPS

2.1 ACE – Authentication and Authorization for Constrained Environments of working group of IETF had their meeting. An important draft that was discussed was: Authentication and Authorization for Constrained Environments - that is yet to be approved by IESG as a standard. However there were many drafts that were discussed in this area. One of the protocol draft that came up for discussion was CBOR Web Token – (CWT) that is derived from JWT (JSON Web Token) but uses CBOR – Concise Binary Object Representation.

2.2 6TISCH – IPv6 over the TSCH mode of IEEE 802.15.4 working group of IETF had their meeting. One of the drafts authored by Mr. Lijo Thomas from C-DAC Trivandrum (a former IIREF Fellow) was scheduled for discussion. However due to lack of time and due to the overlapping of the draft with another working group it was postponed. Also there were drafts discussed under dynamic scheduling and security.

2.3 LAMPS - Limited Additional Mechanisms for PKIX and SMIME working group of IETF had their meeting. A draft on Internationalized Email Addresses in X.509 certificates draft-ietf-lamps-eai-addresses-12. Discovery issues during DNS resolution were brought out. A draft on adding SHA3 – the latest crypto hash algorithm to PKIX/SMIME also was brought up for discussion. A draft titled first-issued certificate extension was brought in for discussion, which claimed to provide an indication of trustworthiness of the certificate subject based on its age of use. They are trying to work out as a standard by Jun 2018.

2.4 SECEVENT – Security Events working group of IETF had their meeting. A security token is conceptualized to deliver messages related to Security event. The tokens are defined in the format of JWT. The draft on SET token delivery over HTTP was presented. The main point was how to avoid confusion with similar tokens – ID Tokens, access tokens, and other kinds of JWT, for which the group had registered the content type extension “application/secevent+jwt”. Other drafts like delivery of SETS over HTTP using Push and Pull methods was discussed.

2.5 T2TRG – Thing-to-Thing Research group of IRTF had their meeting. The main theme is to create a true IoT infrastructure wherein low-resource nodes can communicate among themselves and with wider Internet. Privacy issues related to identifiers and discovery was brought out. The idea of Edge Computing, Authorizing network access of IoT Devices were discussed.

2.6 6LO – IPv6 over Networks of Resource-Constrained Nodes working group of IETF had their meeting. One of the draft on Packet Expiration Time in 6lo Routing header, proposed by Mr. Lijo Thomas from C-DAC Trivandrum (a former IIREF Fellow) and other authors came up for discussion. Mr. Charlie Perkins a co-author of the draft presented it. Changes had been made to the draft based on the inputs from the previous IETF meeting, and it was mentioned that the appropriate word is "deadline time" rather than "expiration time", and is used in the draft. But the draft name is not changed. A request for adoption of the draft was sought for, but owing to a number of queries and discussions, it was decided to put it up in mailing lists for further discussions before adoption.

2.7 TLS – Transport Layer Security working group of IETF had their meeting.

2.7.1 The revised TLS 1.3 internet draft version 21 was presented by Mr. Eric Rescorla. New changes on 0-RTT and anti-replay were discussed. Approval was sought for making anti-replay mandatory was sought, and later decided to keep discussing on it. TLS 1.3 showed increased connection failures during some cases of testing, and the problem was figured out as Middleboxes or NAT, and the current proposed solution was to fall back to TLS 1.2 till more data emerges.

2.7.2 A draft on Data Centre use of Static Diffie-Hellman in TLS 1.3 was proposed, that sparked a big controversy over information leakage and privacy issues. The background was to enable enterprises to monitor TLS-encrypted sessions inside the datacentre. Thought there was lot of apprehensions, the house was divided on the issue, when put to vote, and was decided to take it further for discussions.

2.7.3 IDEAS - Identity Enabled Networks working group of IETF had their meeting. This was a BoF – Birds of Feather session, wherein the goal is to

formulate a framework to provide ID-based services. The central point is having an identity separate from identifiers and location and provide services based on identity. The difference between identity and identifier was brought out, wherein identity for an entity is unique, while there could be multiple identifiers for the same entity. Also the privacy issues were also brought out. It was then decided to put up the latest version to the mailing list and then discuss further on the charter of this working group.

2.7.4 GAIA – Global Access to the Internet for All research group of IRTF had their meeting. A draft based on community clouds – cloudy was presented by the author from Trinidad. A brief update on Internet Measurements in Africa was presented, wherein Intra-African country was discussed. A 'Gram Marg' solution for rural broadband carried out by Prof. Abhay Karandikar of IIT Bombay was presented, wherein the TV Whitespace (TVWS) – unutilized space of the TV spectrum was utilized for providing Internet access to rural areas. The TVWS serves in the middle mile of Network architecture, and at the end points Wi-Fi access points are put up. GreenApps – Anoff-grid Cellular Edge Apps Ecosystem work was presented by Mr. Lakshminarayanan Subramanian from New York University, wherein a solar powered cell power of a radius of 2-3 miles for providing cellular edge services at remote locations in Ghana was presented. Also the apps are hosted on the edge.

2.7.5 SACM – Security Automation and Continuous Monitoring working group of IETF had their meeting. ROLIE – Resource oriented Lightweight Information Exchange draft was presented. The objective is to provide metadata to allow clients to discover and search information resources, which will enable automatic machine communication. ROLIE is a profile of the Atom syndicate format as it lends itself to provide an extensible mechanism to characterize to different types of security. ROLIE can work with both Publish-Subscribe, Request-Response models. This was followed by drafts of ROLIE extensions.

2.7.6 QUIC – Designed to provide protection equivalent to SSL/TLS, it is a transport layer network protocol with reduced latency and works over UDP (but falls back to TCP for users who have blocked UDP). The hackathon exercises related to QUIC were discussed. A 2nd implementation draft of

QUIC with goal of 0-RTT was discussed that brought strategies for achieving the same. A proposal to encrypt parts of the headers in the packet, leaving few elements like Version, Packet Number etc.…were opposed by network operators as they will lose a lot of info, and would not be able to perform queue and congestion management. Few options were also presented to overcome the problem, but no conclusion could be reached, and they decided to take it over intersessional meeting before next IETF.

2.7.7 UTA - Using TLS in Applications working group of IETF had their meeting. As the draft on MTA-STS (Mail Transfer Agent - Strict Transport Security) is in advanced stages, the holding issue is the format to go for – JSON Vs Key: Value representation. A voting (or sense of the room) was called for, but there was no strong opinions, and therefore decided to go as such and take it up later, if required. A BCP (Best common practice) for use of TLS for email submission and access was presented. The authors were still dwelling about presenting it as BCP. The core ideas were to encrypt the Email traffic between UA and MSP, Port 465 to be still recommended for SMTP submission over TLS and preferring implicit TLS over STARTTLS.

2.7.8 ACME - Automated Certificate Management Environment working group of IETF had their meeting. This draft proposes a protocol for certification authority (CA) and a domain name applicant to automate the process of domain name verification and certificate issuance. The protocol also provides facilities for other certificate management functions, such as certificate revocation. A presentation on Short term auto renewed (STAR) certificates was presented first, which was already presented and approved in last meeting and then followed by another draft requesting for STAR certificate. There are 3 entities here – DNO – Domain Name Owner, NDC – Name Delegation Consumer, and ACME Server. In future, generic tokens are being considered.

2.7.9CORE – Constrained Restful Environments working group of IETF had their meeting. Formats for sensor measurement lists –SenML - was discussed. A draft on ER (Entity-relationship) model for resource directory came up for discussion. Few corrections including making it consistent and clean-up was suggested and will be put up again in IETF 100. A draft on Discovery mapping

that uses DNS based service discovery (DNS-SD) was discussed, wherein format for service instances were discussed.

2.8 MEETING WITH RAY PELLETIER (IETF ADMINISTRATIVE IRECTOR)

As a follow up from the last meeting, several important points regarding India's engagement with IETF were discussed, including the possibility of IETF in India, and on the expectations of IETF from India in terms of Contribution and participation. More involvement in Working Groups (WGs) through physical as well as e-mail lists, to build the IETF community in INDIA

2.9 MEETING WITH IRTF CHAIR

They have discussed" Geographically-Focused IETF Activities" Internet draft. This Internet Draft defines how Geographically-Focused IETF Activities are organized and how IETF policies apply. It is intended for eventual publication as a BCP but this is currently an initial strawman proposal based upon the existing variety of experience with the experimental activities in this space over the past several years. IETF security area director, IETF EDU team representatives with Shri T. Santhosh was also present in the meeting.

2.10 NEW WORK AT IETF 99

1. **Opportunity for India to involve in the 5GResearch work:** 3GPP and 3G Research work where Indian Government may involve .It will help in deployment of 5G in India, in future and will support Digital India program.5G is the latest generation of cellular network standards. The 5G work happens to a large extent in 3GPP, as did previous generations. The work on 5G is planned to take place in two releases, of which the first one is Release 15, scheduled to be stable and all protocols completed latest by September 2018, just 14 months away. Additional work will be done in Release 16, which will complete by March 2020.

2. **BOF(Birds of a Feather) Session 1**: Bandwidth Aggregation for internet Access (BANANA) BANANA is concerned with providing coordinated

Internet Access to a device over multiple links of different types to allow for increased bandwidth utilization, load balancing and/or higher reliability. The goal of this BOF is to determine whether the scope of the problem is well defined and understood, whether there is a critical mass of participants willing to work on the problem, and whether in general the working group would have a reasonable probability of success.

3. **BOF (Birds of a Feather) Session 2**: Identity Enabled Networks (IDEAS) The goal of this work is to standardize a framework that provides identity-based services that can be used by any identifier-location separation protocol.

4. **BOF (Birds of a Feather) Session 3**: Network Slicing (NETSLICING) it was a non-working group-forming BOF. In this work proposal, a "network slice" is conceptualized as a logical network comprised of the union of resources (connectivity, storage, computing), network functions, and service functions. Network slicing is a concept garnering much attention as part of 5G standardization and development efforts.

5. One newly chartered working group meeting for the first time at IETF 99: DKIM Crypto Update (DCRUP). The DCRUP working group is chartered to update Domain Keys Identified Mail (DKIM, RFC 6376) to handle more modern cryptographic algorithms and key sizes.

Photographs

(Clockwise from L to R: IETF Badge, IIREF Fellows – Dr. R Balaji & Mr. Harish , Indian Community Dinner, IIREF Promotion at IETF, TLS Sessions, Mr. Santosh and Dr. Balaji and Tokbind session)

3. IIREF fellowship

IREF is being carried out as a project by C-DAC (Center for Development of Advanced Computing), Bangalore, sponsored by the Internet Governance Division of Department of Electronics & Information Technology (DeitY), Ministry of Communications and IT, Government of India.

The fellowship applications for each IETF meeting was called through the IIREF portal and the received applications were sent to MeitY constituted committee for selection of candidates for the fellowship. IIREF provides fellowship to attend IETF events. IIREF invites applications from qualified internet professionals from Academia, Industries, and Research labs for participation in upcoming IETF Events.

4. Acknowledgement

We would like to thank Internet Governance division, Ministry of Electronics and Information Technology (MietY), Government of India to support the IIREF fellowship to participate in IETF99 meeting.