
IETF 98
Chicago

Contents

1 EXECUTIVE SUMMARY

In this report we are sharing the experiences and outcomes of attending the Internet Engineering Task Force (IETF) 98 meeting in Chicago, USA from March 26th to 31st 2017 by our IIREF fellows Mr. Lijo Thomas(Senior Engineer, CDAC Thiruvananthapuram) & Smt. Smitha Vinod (Associate Professor, Christ University). This report summarizes the major developments in IETF 96 and also his perceptions.

There are several benefits and learnings that Mr. Lijo Thomas & Smt. Smitha Vinod gained from the visit which otherwise could not have been possible. The meeting motivated him to participate and involve in IETF activities in much more rigorous fashion. It was a great feeling for them to meet and to converse with members of the WGs with whom they had been interacting with over mailing list. In addition to the exposure to the way IETF meetings get conducted and the processes involved.

The IETF meeting motivates to involve and participate more in IETF activities. The meeting helped to discuss drafts with co-authors as well as with Working Group members to pursue the future works.

2 MAJOR DISCUSSIONS WITH DIFFERENT WORKING GROUPS

2.1 ACE Working Group

(Authentication and Authorization for Constrained Environments)

There were eight drafts presented in this meeting. One of the presentation was on the requirements for the secure bootstrapping of low resource devices. A presentation was made on possible disconnection cases between nodes in the ACE framework. Discussion was done on Application layer security protocols suitable for IoT platforms and ACE client token mechanism for authorization information and keys in Client and Resource Server.

2.2 DETNET Working Group

(Deterministic Networking)

The first presentation was on flow information model for Deterministic Networking based on the mature TSN. The presentation on DetNet Security considerations was very much in line with our current work. Detailed nearly 10 different types of threats and charted a table based on the attacker type.

2.3 6TiSCH Working Group

(IPv6 over the TSCH mode of IEEE 802.15.4e)

The major discussion was on the 6tisch minimal security. Introduced new terminology for Joining Node, Join Coordinating Entity and Join Assistant. The pledge node will listen for Enhanced beacons to become aware of available networks. After receiving the beacon the pledge node will send the Join Request to Join Registrar/Coordinator (JRC). The JRC will send back Join Response to the pledge node. Discussed about zero touch and one touch joining procedures in detail. Presented the 6tisch-minimal-rekey which directs standard track definition of management interface for rekey operations.

2.4 CoRE

(Constrained RESTful Environments)

A presentation was on the COAP compression mechanism for LPWAN network where the payload was limited to 10 Bytes to 200 Bytes. Presented the details of CBOR encoding data modelled with YANG and message size overhead of CoAP security protocols. Another presentation was on object security of CoAP (OSCOAP) in which a security option is built in CoAP protocol. This can provides end-to-end confidentiality, integrity and replay protection for CoAP over any/mixed transport.

2.5 6lo

(IPv6 over Networks of Resource-constrained Nodes)

The first presentation was on Transmission of IPv6 packets over Near Field Communication (NFC). The Header compression mechanism was discussed on the presentation of IPv6 Mesh over Bluetooth Low Energy using IPSP. The presentation Transmission of IPv6 packets over PLC networks talks about the protocol stack for IPv6 over PLC, Fragmentation and reassembly, Header compression and connectivity and topology. Highlighted the problems during basic implementation of RFC 4944 caused due to the reassembly at every L3 hop.

2.6 Draft: Packet Expiration Time in 6LoWPAN Routing Header

The Packet Expiration Time draft which was co-authored BY Mr. Lijo Thomas was presented in this meeting by Charles Perkins. Explained the new format for the Deadline-6LoRH message with representation of each bits. Gabriel Montenegro commented that the user defined bits should be removed as it will cause interoperability issues. Pascal Thubert supported the draft and it is very much required to meet QoS in deadline applications. Finally Charlie asked for adoption of this document in the Working Group, since only few people gave support it was not adopted. Samita Chakrabarti, 6lo Chair concluded by requesting more members to read the draft and provide valuable feedback.

Fig 3: Presentation of Packet expiration time in 6lo WG

2.7 OAuth (Web Authorization Protocol) Working Group Meeting

This specification enables OAuth 2.0 implementations to apply Token Binding to Access Tokens, Authorization Codes, and Refresh Tokens. This cryptographically binds these tokens to a client's Token Binding key pair, possession of which is proven on the TLS connections over which the tokens are intended to be used. This use of Token Binding protects these tokens from man-in-the-middle and token export and replay attacks.

2.8 TLS Security Working Group Meeting

In Transport Layer Security (TLS) handshakes, certificate chains often take up the majority of the bytes transmitted. This describes how certificate chains can be compressed to reduce the amount of data transmitted and avoid some round trips. In order to reduce latency and improve performance it can be useful to reduce the amount of data exchanged during a Transport Layer Security (TLS) handshake. This describes a mechanism that allows a client and a server to avoid transmitting certificates already shared in an earlier handshake, but it doesn't help when the client connects to a server for the first time and doesn't already have knowledge of the server's certificate chain. This describes a mechanism that would allow server certificates to be compressed during full handshakes.

2.9 UTA (Using TLS in Applications) Working Group

This WG has the following tasks:

Update the definitions for using TLS over a set of representative application protocols. This includes communication with proxies, between servers, and between peers, where appropriate, in addition to client/server communication.

Consider, and possibly define, a standard way for an application client and server to use unauthenticated encryption through TLS when server and/or client authentication cannot be achieved. Create a document that helps application protocol developers use TLS in future application definitions.

2.10 TokBind (Token Binding) Working Group Meeting

Token binding allows HTTP servers to bind bearer tokens to TLS connections. In order to do this, clients or user agents must prove possession of a private key. However, proof-of-possession of a private key becomes truly meaningful to a server when accompanied by an attestation statement. This specification describes extensions to the existing token binding protocol to allow for attestation statements to be sent along with the related token binding messages.

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 IETF98 meeting.