Indian Internet Research and Engineering Forum – IIREF

Mr. B S Bindhumadhava
Dr. Balaji Rajendran

Centre for Development of Advanced Computing (C-DAC)
No.68, Electronics City, Bengaluru

New Delhi, 7th February 2017

Aim of IIREF

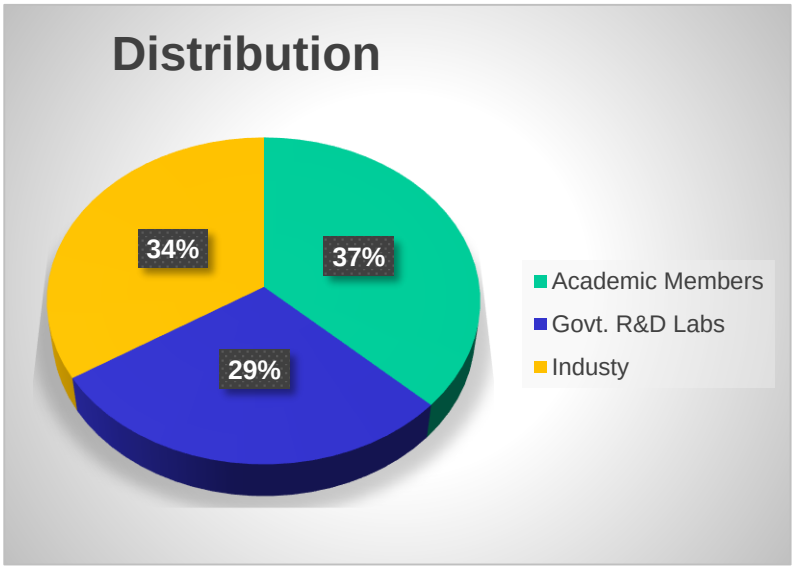
- To create an ecosystem for developing competencies in Internet Protocol Standards
- To propose and contribute to ongoing drafts in the select areas of Internet drafts

IIREF Strategy

- Create and foster focus groups to work on specific technical issues of interest
- Propose new standards & Contribute to ongoing drafts
- Encouraging direct participation in meetings of Internet Organizations
- Engage with academic community and industry
- Scholarships and Fellowships to deserving Candidates

Fellowships

- IIREF Fellowships to attend IETF Meetings
  - Total applications received: 38
  - Total members awarded: 4
    - Fellowships awarded to attend:
      - IETF 94 – Yokohama, Japan
      - IETF 96 – Berlin Germany
      - IETF 97 – Seoul, Korea
      - IETF 98 fellowship is in progress;

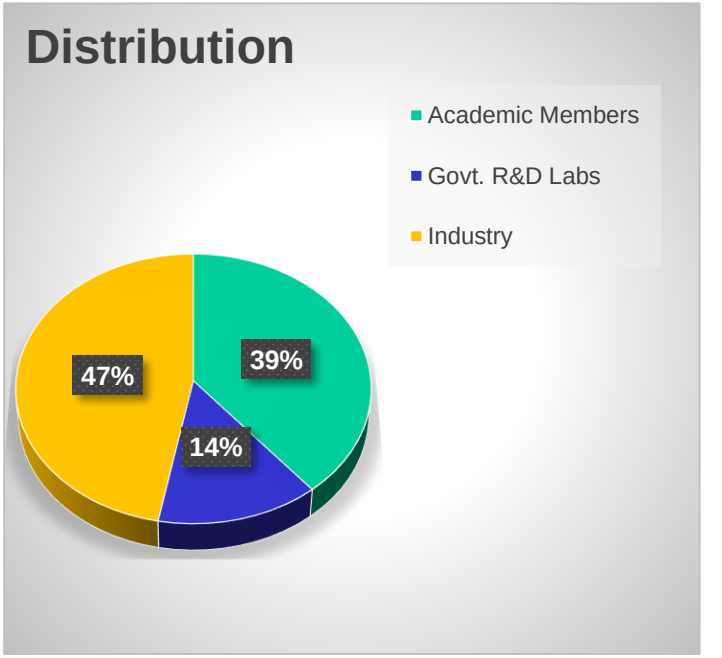


Awareness Programs

- Awareness on
  - Need for Internet standards
  - IETF – Structure & Process
  - Current trending areas in IETF
- Stats
  - Reached 1120+ members so far
  - Conducted 13 programs, including 2 NIT’s;

Expert Meetings

- Theme-based Brainstorming Sessions
  - Internet Standard Development in India
    - Organized in Mar 2016
    - 20 members participated
  - Security Protocols for Smart Devices
    - Organized in Jan 2017
    - 20 members participated



Contributions

- Develop internal capabilities for development of Internet Standards in various domains of Internet Security including
  - Digital Time Stamping and Digital Tokens
  - Transport Layer Security - TLS, DTLS
  - DNS Security
  - IoT Security

Focused Area under IETF – Security Area (sec)

Focused Working Groups under sec area

- PKIX
- Token Binding
- TLS
- DTLS
- DANE

Potential Industry Stakeholders

RTFM,Inc.
ARM Ltd.
Google
Verisign
Microsoft

Focused RFC's/Internet Drafts related to working Groups

- ID – TLS Protocol V 1.3
- ID – TLS Cached Information Extension
- ID – TLS False Start

- RFC 6698 – The DNS Based Authentication of Named Entities (DANE) TLS Protocol : TLSA
- ID - TLS Client Authentication via DANE TLSA records

- RFC 3161 - Internet X.509 Public Key Infrastructure Timestamp Protocol (TSP)
- Internet Draft - Token Binding over HTTP

- RFC 4347 – Datagram Transport Layer Security
- RFC 7457 - Summarizing known attacks on TLS and DTLS

- RFC 5280 – Internet X.509 Certificate Standards including Revocation

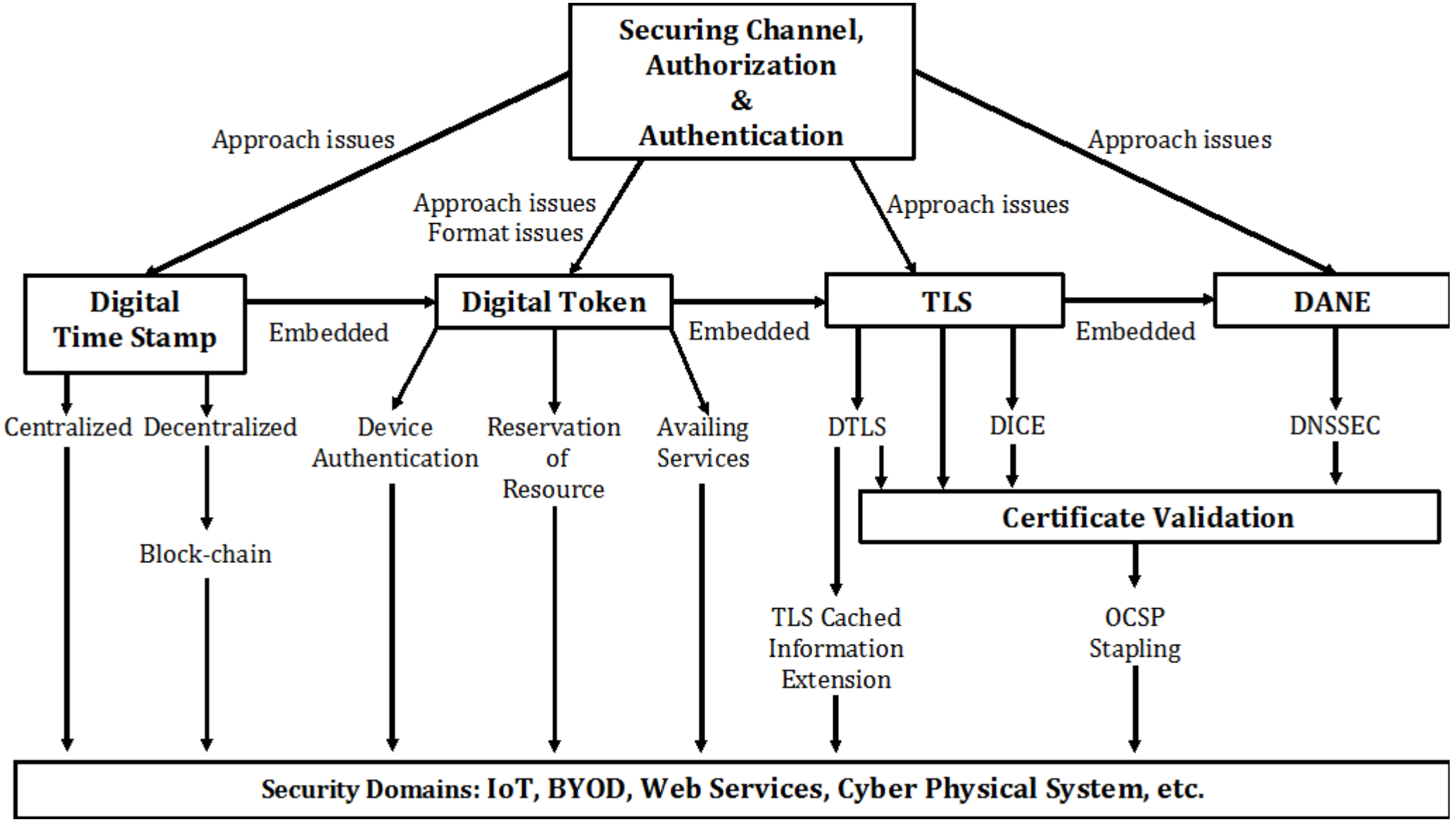
Identified Concepts for Contribution

- Digital Certificates
- Digital Tokens

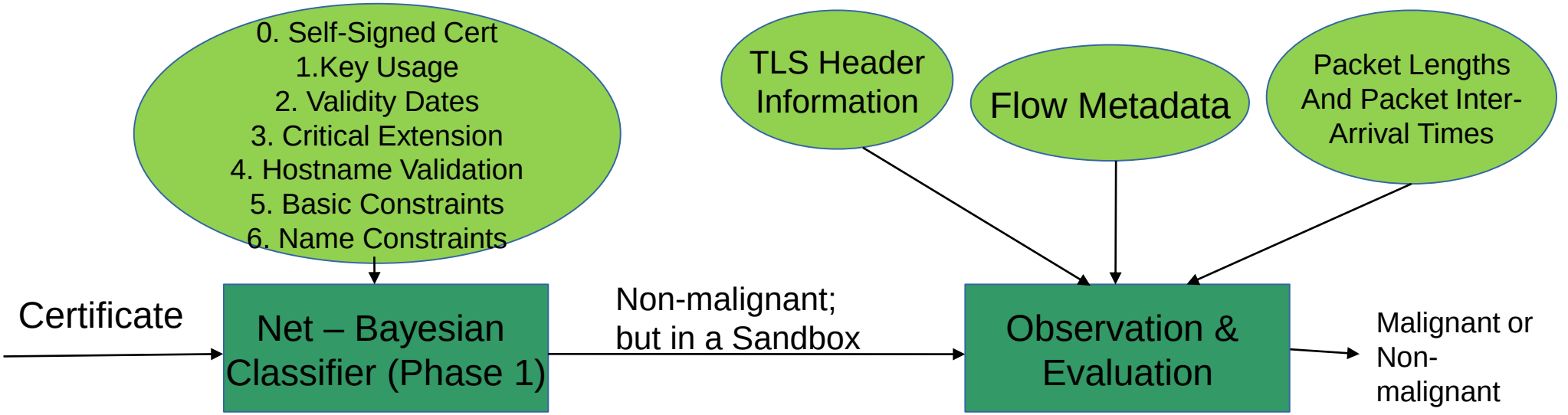
Future Potential Areas

- IoT (DTLS)
- Access Management (TLS, PKIX)
- DNSSec (DANE)
- Identity Management (PKIX)

In a Perspective …



Detecting Malignant TLS Servers Using ML Techniques



Server (S)

Remote Administrator (R)

Digital Token Generation Process

I = {PubKey(R), StartTime, EndTime, Priv}

ServerSgn = Sign (I, PvtKey(S))

DigTok = {I, ServerSgn}

Digital Token Sharing Process

SDigTok = Encrypt(DigTok, PubKey(R))

DigTok = Decrypt(SDigTok, PvtKey(R))

Remote Administration using Digital Token

RSgn = Sign (DigTok, PvtKey(R))

Req = {DigTok, RSgn}

RSgnVerify = SgnVerify(RSgn, DigTok, PubKey(R)) where PubKey(R) is part of I

If(RSgnVerify)
ServerSgnVerify = SgnVerify(ServerSgn, I, PubKey(S))

If(ServerSgnVerify)
TimeCheck = TimePeriodCheck (CurrentTime, StartTime, EndTime)

If(TimeCheck)
GrantRemoteAccess(R, Priv)
Monitor(CurrentTime, EndTime) for Ending Session

S: Entity whose access to be delegated, R: Person/System to whom access is delegated
PubKey(X): Public Key of X, PvtKey(X): Private Key of X
Priv: Privilege to be granted to R on S, DigTok: Digital Token
StartTime: Starting Time of Delegation, EndTime: Ending Time of Delegation

Plugtest for Digital Tokens

- An environment for testing the design being created to test for interoperability:
  - Authentication and authorization in domains (Eg Windows Domain)
  - BYOD where user credential is checked for access of network without compromising security
  - IoT devices of different types

Thank You

 www.iiref.in

 /iiref

 @iirnef