Welcome to Brainstorming Session on "Secure Protocols for Smart Devices"

Indian Internet Research and Engineering Forum (IIREF)

Centre for Development of Advanced Computing (C-DAC)

No. 68, Electronics City, Bangalore 560100

30th January 2017

Internet Standard Development

- Internet Engineering Task Force (IETF)
  - Organization responsible for development of Internet Standards
    - Egs. include: TCP, IP Protocols
- Indian Internet Research and Engineering Forum (IIREF)
  - An effort carried out by C-DAC Bangalore, and sponsored by MeitY, Govt. of India

What we do?

- 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

What we can do for You?

- Sponsor you to attend IETF Meetings, provided
  - You demonstrate your abilities and work with respect to Internet Standards
  - You apply for fellowship

IIREF
Indian Internet Research & Engineering Forum

About IIREF

- IIREF - Indian Internet Engineering Forum aims to serve as a platform for Indian researchers and practitioners to come together and collaborate among themselves in their specific areas of interest in alignment with the IETF working groups.
- The forum aims to build and nurture competencies through conduction of awareness and training programs, and also in future, provide mentors to specific areas that have fairly evolved within the forum.

About IIREF

- IIREF therefore aims to evolve as a community driven forum, wherein increasing and active contributions from the Indian community, towards development of protocols in various areas under the IETF is envisaged.

Lead Questions

- Define the spectrum of Security Challenges in Smart Devices
- Pros and Cons of Hard-coding of credentials in the device – for authentication (including Mutual Authentication)
- What can we learn from the strong authentication and communication security prevailing in Cellular Networks? (as they can fit to a proportion of the scale of IoT networks)
- Public key Cryptography vs Identity based Cryptography scheme in the context of Smart devices
- IPSec Vs DTLS for establishing secure channels
- What are the implications of DNSSEC, SHA3 in the emerging world of Smart Device Networks ?

Lead Questions

- Why is it difficult to detect a breach originating through a smart device?
- Should smart devices come with security backdoors?
- Control devices in unconstrained environment running apps based on Android / iOS / HTML 5 have number of vulnerabilities – How can security protocols overcome them?

Thank You

www.iiref.in

/iiref

@iirnef

IIREF
Indian Internet Research & Engineering Forum