सत्यमेव जयते

Indian Telecom Security Assurance Requirements

For

Set Top Box (STB)

NCCS

Securing Networks

Security Assurance Standards (SAS),

National Centre for Communications Security, Bengaluru

Department of Telecom, Ministry of Communications

Government of India

Security Outline document for Set Top Box (STB)

National Centre for communication Security (NCCS), with headquarters at Bengaluru was set up in 2018 with the objective to establish and operationalize a framework of security testing and certification within the country.

Security Assurance Standards (SAS) division of NCCS has been assigned the responsibility to spearhead the efforts for development of Indian Telecom Security Assurance Standards (ITSAR) for defining security requirements.

In view of this, SAS division has taken up the work of defining baseline security requirements for Set Top Box (STB) and vide this outline document, our division is opening a platform for discussions on security of STB devices and inviting experts from the industry to actively participate in the development of the ITSAR for STB devices.

The purpose of consultation for STB security outline document is to seek inputs / comments / suggestions from all stakeholders viz., Regulatory bodies/ Standard Development Organisations / OEMs/ MSO's /distributors /CAS vendors for developing ITSARs.

Note:

1) Standards that are under consideration is at Annexure 1

2) Proforma for participation for Members is at Annexure 2

Inputs are requested on following points/questions

I. General Questions

1. which are the areas of STB functionality for which security is a concern?
2. Are there any existing standards/industry practices that prescribe security guidelines for STB?
3. Please provide the categorisation of STB models based on the features/functionality?
4. What user/operational data is collected by STB ?
5. Which are the recommended standards to be followed for CAS module security?
6. For the interfaces of STB that are towards internet what are the security threats perceived ? Are there any existing security standards / practices that are followed by STB industry?
7. What are the existing mechanisms in Industry to test SoC of STB?
8. How does supply chain security ensured in importation of STB devices?
9. Which are the critical sub-assemblies / Critical parts of STB that needs security testing?

II. PRIVACY Related Questions

User privacy concerns are listed below,

1. whether user data collected, remains in the STB ? or what part of the data will be sent to the central server of the operator?

2. Does user will get a choice to share or not share the data to the server?

3. Is the data format / API documented / publicly available, allowing a user to uses their data without the app / cloud service?

4. Does user be given an option for raising a request to the deletion of the user's data in the central storage? Can users request data for local storage (their home computer)?

5. Does the user will know who has access to their personal and device data? (3rd party companies, data research companies, marketing, IT administrators, technical support, developers, users, user's friends/family, etc.)

6. Is RBAC implemented for different types of data of consumers that gets collected by the STB?

7. Does the data (device & user) that gets collected by STB gets stored using an encrypted mechanism?

8. If so, who can decrypt such data and the purpose of accessing such data is documented?

9. Is the device data stored according to an anonymized user ID with the personal information stored separately?

10. does the device send data that makes it (and the user) identifiable to sniffers?

The existing security measures addressing the concerns of user privacy for the above mentioned points can be provided. If not, are there any international standards/industry best practices that STB industry suggests/recommends for incorporating the same in to the ITSAR for STB

.

III. Further Questions on STB Security

1. What are the authentication (password/passcode) and authorisation mechanisms/policies currently that are implemented to get information from the device? From the app? From the server?
2. what is the password policy that is currently implemented in the STB?
3. Do authorized users get logged off automatically after a timeout?
4. Does the data in STB gets backed up? Is that protected to the same level as the live data? Does the backup ever expire or is it retained indefinitely?
5. How to assess an STB is hacked or not? Which are the measures followed by Industry to check integrity of STB?
6. What are the measures to prevent STB cloning?
7. Are firmware / Software updates secure, signed, and verified?
8. Is the data encrypted as it travel across the network (from device to app, from app to server, from server to backup, from server to user interface)? Are there other steps you take to reduce the risk that the user data can be intercepted or modified while on a network?
9. Does STB support physical or logical separation of management traffic and device traffic?

Annexure 1

A: Standards that are under consideration for development of ITSARs for STB devices (List is of informative nature)

Comments / suggestions may be given on applicability of each of the detailed security provisions/clauses given in below mentioned standards.

1. ETSI TS 102 824 V2.1 - Digital Video Broadcasting (DVB); Remote Management and Firmware Update System for DVB IPTV Services
2. CI Plus LLP: "CI Plus Specification. Content Security Extensions to the Common Interface v1.4.3"
3. ETSI TS 102 825-5: "Digital Video Broadcasting (DVB); Content Protection and Copy Management (DVB-CPCM); Part 5: CPCM Security Toolbox".
4. ETSI TR 102 825-6: "Digital Video Broadcasting (DVB); Content Protection and Copy Management (DVB-CPCM); Part 6: CPCM Security Test Vectors".
5. ETSI TS 102 006: "system software update in DVB systems"

Annexure 2

Nomination Proforma

Committee Name: ITSAR of STB

A) Principal Member

General Interest / Expertise : ______________________________

Shri/Smt/Dr./Prof. : ______________________________

Designation : ______________________________

Name of Organisation : ______________________________

Address in full for Correspondence : ______________________________
____
____

City : ______________________________

Mobile Number : ______________________________

email id : ______________________________

A) Alternate Member

General Interest/ Expertise : ______________________________

Shri/Smt/Dr./Prof. : ______________________________

Designation : ______________________________

Name of Organisation : ______________________________

Address in full for Correspondence : ______________________________
____
____

City : ______________________________

Mobile Number : ______________________________

email id : ______________________________