|  |  |
| --- | --- |
| INTERNATIONAL TELECOMMUNICATION UNION | **IPTV-GSI** |
| **TELECOMMUNICATIONSTANDARDIZATION SECTOR**STUDY PERIOD 2009-2012 | **IPTV-GSI-C-474** |
| **English only****Original: English** |
| **Question(s):** | 13/16 | Singapore, 20-27 September 2010 |
| **CONTRIBUTION** |
| **Source:** | Cisco Systems |
| **Title:** | Proposals for revised text of H.IPTV-AM.0 regarding the impact of user permission levels |

1. Abstract

This contribution proposes modified content for H.IPTV-AM.0 “IPTV application event handling: Overall aspects of audience measurement for IPTV services”. It proposes to modify and add text concerning the impact of user permission levels.

1. Proposals
2. Clause 6.2 AM0 introduces user permission profiles and two levels of security impact based upon permitted data collected. It should include the situation when no permission is given, and if a subscriber profile is given. The impact on non-measurement parts of the AM system should be included. Therefore it is proposed to replace the current clause 6.2 with the following expanded content.
3. Table 6 includes references to specific permission levels. Since the number and meaning of user permission levels are for definition by the measurement service provider, and configuration pending Cisco’s configuration proposal. This proposal is to modify the row containing specific permission levels.

**Content for Proposal 1 –**

## 6.2 The impact of permission levels on the AM system

The number and meaning of user permission levels are for definition by the measurement service provider. This recommendation provides mechanisms to support policies associated with permission levels. It also provides examples and implementation guidance. The following table relates the measurements, the implications for the AM system, the potential for a user’s data profile to threaten privacy, and services for six example permission levels.

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
|  | **Permission Level 0 (default)** | **Permission Level 1** | **Permission Level 2** | **Permission Level 3** | **Permission Level 4** | **Permission Level 5** |
| End-user permission  | Not required | required | required | required | required | required |
| Permitted measured data  | None | Viewing events and context, indistinguish-able user, no user profile | Viewing events and context, distinguishable user, no user profile | Viewing events and context, distinguishable user, anonymous profile | Viewing events and context, distinguishable user, with subscriber profile | Viewing events and context, identifiable user, with user profile |
| Example data | No data is measured | Program “A” was watched. | Program “A” was watched by anonymous user #12683304 | Program “A” was watched by anonymous user #12683304 who is male in named town  | Program “A” was watched on mobile type “X” contracted to subscriber “John Smith” with email js@sp.com | Program “A” was watched on mobile type “X” being used by “Mary Smith” with email ms@sp.com |
| Other impact on AM system \* | Prevent or filter out measurements | Correlation among users’ devices not possible | Correlation among users’ devices possible | Correlation among users’ devices possible | Subscriber profile requires special security handling | User profile requires special security handling |
| Privacy infringement potential  | None | Measured data does not influence privacy profile | Measured data plus additional data may influence privacy profile | Measured data plus additional data may influence privacy profile | Measured data may influence privacy profile | Measured data may influence privacy profile |
| Additional SP services supportable \*\* | Plain subscription | Content rating and engagement reporting | (Better) targeted advertisement and content recommendation | - | IPTV engagement driven communications | IPTV user engagement driven personalized communications |

Table 1 – Example permission levels, their impact on the AM system, privacy infringement potential and services supportable

\* Note that correlation is possible for levels 3, 4 and 5. Subscriber profile requires special security handling for level 5.

\*\* Note that the quality of the example additional services supportable in levels 2 and 3 improve further in levels 3, 4 and 5. Level 4 services become more personalised in level 5.

Viewing (or application) events and context are further discussed in clause 6.5 and throughout this recommendation.

In permission level 1, no data is collected which allows for distinguishing among users. In permission level 2, an assigned identifier keeps the user’s identity anonymous and supports distinguishing among users. In permission level 3, only information elements of the subscriber’s or user’s profile which are non-personally-identifying are permitted, thus supporting distinguishing among users with additional anonymous profile information. In permission level 4, a proxy profile for the actual user is used, which in this case is that of the subscriber. In addition to being distinguishable, the subscriber’s non-anonymous profile contains subscriber identifiable information elements. In permission level 5, in addition to supporting distinguishing among users, the user’s non-anonymous profile contains user identifiable information elements. [ITU-T H.750] identifies metadata elements for user profiles.

**Content for Proposal 2 –** Modify the row

**From:**

|  |  |  |  |
| --- | --- | --- | --- |
| **Element** | **Description** | **Support** | **Notes or Value Domain** |
| user permission availability | The information indicate that the privilege level of user information can be collected  | C | Level 1: “prohibit all”, defaultLevel 2: “anonymous”Level 3: “non-anonymous” |

**To:**

|  |  |  |  |
| --- | --- | --- | --- |
| **Element** | **Description** | **Support** | **Notes or Value Domain** |
| user permission level | Indicates the user information which is permitted to be collected  | C | See configuration of PmesId with permitted metadata elements set (proposed clause 16.1.2) |

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_