|  |  |  |
| --- | --- | --- |
| ITU logo | **International telecommunication union****Telecommunication Standardization Bureau** | CCITT/ITU-T 60th Anniversary logo |
|  | Geneva, 26 May 2016 |
| Ref: | **Addendum 1 toTSB Collective letter 12/11** | - To Administrations of Member States of the Union; - To ITU‑T Sector Members;- To ITU‑T SG11 Associates; and - To ITU Academia |
| Tel: | +41 22 730 5858 |
| Fax: | +41 22 730 5853 |
| E-mail: | tsbsg11@itu.int  |  |
| Subject: | **ITU-T Workshops on "SS7 Security" (29 June 2016) and "Combating Counterfeit Using Conformance and Interoperability Solutions" (28 June 2016) during the ITU-T Study Group 11 meeting (27 June – 6 July 2016)** |

Dear Sir/Madam,

This addendum is issued to provide additional information about relevant events organized at ITU headquarters during the Study Group 11 meeting, Geneva, 27 June – 6 July 2016.

I wish to draw your attention to the following events:

**1 ITU-T Workshop on "**[**SS7 Security**](http://www.itu.int/en/ITU-T/Workshops-and-Seminars/201606/Pages/default.aspx)**", 29 June 2016 (0900-1230)**

**Introduction**

Signaling System No. 7 (SS7) is a set of telephony signaling protocols developed by ITU-T since 1970s, which is used to set up and tear down most of the world's telephone calls.

SS7 standards are widely applied in public switched telephone networks (PSTN), which are well-known as ITU-T Q.700-series Recommendations. The Intelligent Networks standardized by ITU are also related to SS7 (ITU-T Q.1200-Q.1699). With the growth of mobile telecommunications, ETSI has developed the MAP and CAP protocols, which are also based on SS7 and are suitable for public land mobile networks (PLMN), e.g. GSM networks. In addition, a series of RFCs called SIGTRAN was published by IETF, which makes it possible to use SS7 over IP networks.

SS7 was designed to be managed by operators with the understanding that anyone connected to an SS7 network was considered trustable. With the current network environment, including interconnection over the Internet, SS7-based networks become vulnerable and can be attacked. The media have reported vulnerabilities and security issues related to SS7 that allow tracking a user’s location and voice interception. This has also been confirmed by some operators.

ITU-T SG11 is currently researching SS7 security issues and this event wishes to brainstorm possible actions to enhance the security mechanisms of SS7.

**Objectives**

The workshop aims to:

• share information on SS7 security issues;

• analyze the current SS7 standards and identify which ones have been impacted;

• discuss how to improve SS7 standards in terms of security;

• discuss the proposals to enhance the security of SS7-based networks for the benefit of users and operators;

• discuss cooperation with other SDOs and organizations on SS7 security issues.

**Target Audience**

Both ITU members and non-members are invited. In particular, the participation of operators, vendors, security experts, research institutions and academia, standards bodies and other such similar organizations is welcome.

**List of SS7 standards (not exhaustive)**

ITU-T Recommendations

− ITU-T Q.700-series (MTP, SCCP, TCAP, TUP, ISUP)

− ITU-T Q.1200-Q.1699 (Intelligent Networks)

− ITU-T Q.1912.5 (Interworking between SIP-I and ISUP)

ETSI/3GPP specifications

− 3GPP TS 09.02 (Mobile Application Part, MAP)

− 3GPP TS 09.78, 3GPP TS 29.078 (CAMEL Application Part, CAP)

IETF RFCs

− RFC 4960, Stream Control Transmission Protocol (SCTP)

− RFC 5133, ISDN User Adaptation (IUA)

− RFC 4165, Message Transfer Part 2 (MTP) User Peer-to-Peer Adaptation Layer (M2PA)

− RFC 3331, Message Transfer Part 2 User Adaptation Layer (M2UA)

− RFC 4666, Message Transfer Part 3 User Adaptation Layer (M3UA).

− RFC 3868, Signalling Connection Control Part (SCCP) User Adaptation (SUA)

− RFC 3807, V5 User Adaptation (V5UA)

− RFC 4129, DPNSS/DASS2 User Adaptation (DUA)

**Website:** <http://www.itu.int/en/ITU-T/Workshops-and-Seminars/201606/Pages/default.aspx>

**2 ITU Workshop on "**[**Combating Counterfeit Using Conformance and Interoperability Solutions**](http://www.itu.int/en/ITU-T/Workshops-and-Seminars/20160628/Pages/default.aspx)**", 28 June 2016 (1400-1800)**

**Introduction**

[Resolution 188](http://www.itu.int/pub/S-CONF-ACTF-2014) (Busan, 2014) of the ITU Plenipotentiary Conference on “Combating counterfeit telecommunication/information and communication technology devices” resolves to instruct the Directors of the three Bureaux to assist Member States in addressing their concerns with respect to counterfeit telecommunication/ICT devices through information sharing at the regional or global level, including conformity assessment systems.

Also, the ITU workshop on "[Combating counterfeit and substandard ICT devices"](http://www.itu.int/en/ITU-T/C-I/Pages/WSHP_counterfeit.aspx) in November 2014 identified the scope of problems and the negative impact of counterfeiting, including lost taxes, royalties and other revenues; decreased sales, prices and operations; erosion of brand value, goodwill and reputation; reduced incentive to innovate and invest; lower employment and economic growth rates; network disruptions and interoperability challenges resulting in poor quality of service delivery and reception; and risks to health, safety and environment.

Going forward, there is the need for actions to be taken to combat ICT product counterfeiting. Consequently, [ITU-T SG11 Question 8 (Q8)](http://www.itu.int/en/ITU-T/studygroups/2013-2016/11/Pages/q8.aspx) is currently leading the studies to determine every possible technical solution to combat counterfeit ICT devices. Q8 has published a [technical report on counterfeit ICT devices](http://www.itu.int/pub/T-TUT-CCICT) and a number of new work items have been established, including draft new Recommendation “[Framework for Solutions to Combat Counterfeit ICT Devices](http://web.itu.int/ITU-T/workprog/wp_item.aspx?isn=10502)”.

Also, within the ITU and around the world, there have been debates as to whether or not conformance and interoperability programmes could be one of the technical solutions to combat counterfeit ICT devices.

**Objectives**

The aims of this workshop are as follows:

* To create awareness of the studies currently on-going in ITU-T SG11 Q8 and particularly to foster development of the technical Recommendation “[Framework for Solutions to Combat Counterfeit ICT Devices](http://web.itu.int/ITU-T/workprog/wp_item.aspx?isn=10502)”;
* To determine whether or not conformance and interoperability programmes can assist to combat counterfeit ICT devices;
* To understand new trends and mechanisms in ICT counterfeiting, tempering and/or duplication of unique device identifiers;
* To understand mechanisms to secure the supply chain management (from manufacturing, importation, distribution and marketing) to ensure traceability, security, privacy and trust of people, products and networks;
* To continue raising awareness of the problem of counterfeiting of ICT devices and the dangers they pose; and
* To solicit views, proposals and ideas from ITU experts and experts around the world for further studies during the next study period.

**Target Audience**

Both ITU members and non-members are invited. In particular, the participation of vendors and manufacturers, research institutions and academia, laboratories, regulators, operators, NGOs, customs authorities and security agencies, standards and conformity assessment bodies and other such similar organizations are welcomed.

**Website:** <http://www.itu.int/en/ITU-T/Workshops-and-Seminars/20160628/Pages/default.aspx>

I wish you enjoyable and productive meetings.

Yours faithfully,

Chaesub Lee
Director of the Telecommunication
Standardization Bureau