|  |  |  |
| --- | --- | --- |
| itu_logo | **الاتحـاد الدولـي للاتصـالات****مكتب تقييس الاتصالات** |  |

|  |  |  |
| --- | --- | --- |
|  |  | جنيف، 26 مايو 2016 |
| المرجع: | **الإضافة 1 للرسالة الجماعيةTSB Collective letter 12/11** | إلى:- إدارات الدول الأعضاء في الات‍حاد؛- أعضاء قطاع تقييس الاتصالات في الات‍حاد؛- ال‍منتسبين إلى قطاع تقييس الاتصالات ال‍مشاركين في أعمال ل‍جنة الدراسات 11؛- الهيئات الأكادي‍مية ال‍منضمة إلى الات‍حاد |
| الهاتف: | +41 22 730 5858 |
| الفاكس: | +41 22 730 5853 |
| البريد الإلكتروني: | tsbsg11@itu.int |
|  |  |  |
| الموضوع: | **ورشتا عمل قطاع تقييس الاتصالات بشأن "أمن نظام التشوير رقم 7" (29 يونيو 2016) وبشأن "مكافحة التزييف باستخدام حلول المطابقة وقابلية التشغيل البيني" (28 يونيو 2016) خلال اجتماع لجنة الدراسات 11 لقطاع تقييس الاتصالات (27 يونيو – 6 يوليو 2016)** |

حضرات السادة والسيدات،

ت‍حية طيبة وبعد،

تم إصدار هذه الإضافة لتوفير مزيد من المعلومات بشأن الأحداث ذات الصلة التي ستُنظم في مقر الاتحاد خلال اجتماع لجنة الدراسات 11 لقطاع تقييس الاتصالات في جنيف، 27 يونيو - 6 يوليو 2016.

وأودّ أن أسترعي انتباهكم إلى الحدثيْن التاليين:

# 1 ورشة عمل قطاع تقييس الاتصالات بشأن "[أمن نظام التشوير رقم 7](http://www.itu.int/en/ITU-T/Workshops-and-Seminars/201606/Pages/default.aspx)"، 29 يونيو 2016 (الساعة 1230-0900)

مقدمة

نظام التشوير رقم 7 (SS7) هو مجموعة من بروتوكولات التشوير الخاصة بالمهاتفة التي يطورها قطاع تقييس الاتصالات منذ سبعينات القرن الماضي، وهي تُستخدم لإقامة معظم النداءات الهاتفية في العالم وإنهائها.

وتُطبق معايير نظام التشوير رقم 7 على نحو واسع في الشبكات الهاتفية العمومية التبديلية (PSTN)، وهي مشهورة باسم سلسلة التوصيات ITU‑T Q.700. وتتعلق أيضاً الشبكات الذكية التي يتولى الاتحاد تقييسها بالنظام SS7 (التوصيات ITU‑T Q.1699‑Q.1200). ومع نمو الاتصالات المتنقلة، قام المعهد الأوروبي لمعايير الاتصالات (ETSI) بتطوير البروتوكولين MAP وCAP اللذين يستندان أيضاً إلى النظام SS7 ويلائمان الشبكات المتنقلة البرية العمومية (PLMN) مثل شبكات النظام العالمي للاتصالات المتنقلة. وبالإضافة إلى ذلك، نشر فريق مهام هندسة الإنترنت (IETF) سلسلة من طلبات الحصول على تعليقات تدعى SIGTRAN وتسمح باستخدام النظام SS7 عبر شبكات بروتوكول الإنترنت.

وصُمم النظام SS7 لكي يقوم المشغلون بإدارته على أساس أن أي شخص يُوصّل بشبكة للنظام SS7 يعتبر موثوقاً. ومع بيئة الشبكات الحالية بما في ذلك التوصيل البيني عبر الإنترنت، أصبحت الشبكات القائمة على النظام SS7 ضعيفة ويمكن أن تتعرض للهجوم. وقد أبلغت وسائل الإعلام عن نقاط ضعف ومسائل أمنية ذات صلة بالنظام SS7 تسمح بتتبع موقع المستعمل واعتراض الصوت. وقد أكد بعض المشغلين هذا الأمر.

وتقوم لجنة الدراسات 11 لقطاع تقييس الاتصالات حالياً ببحث المسائل الأمنية للنظام SS7 ويرجى من هذا الحدث طرح أفكار بشأن الإجراءات التي يمكن اتخاذها لتعزيز الآليات الأمنية للنظام SS7.

الأهداف

تهدف ورشة العمل إلى ما يلي:

• تبادل المعلومات بشأن المسائل الأمنية للنظام SS7؛

• تحليل المعايير الحالية للنظام SS7 وتحديد المعايير التي تأثرت منها؛

• مناقشة كيفية تحسين معايير النظام SS7 من حيث الأمن؛

• مناقشة المقترحات المقدمة لتعزيز أمن الشبكات القائمة على النظام SS7 لفائدة المستعملين والمشغلين؛

• مناقشة كيفية التعاون مع منظمات تطوير المعايير والمنظمات الأخرى بشأن المسائل الأمنية للنظام SS7.

الجمهور المستهدف

الدعوة موجهة إلى الأعضاء وغير الأعضاء في الاتحاد على السواء. ويرحَّب خصوصاً بمشاركة المشغلين والبائعين وخبراء الأمن والمؤسسات البحثية والهيئات الأكاديمية وهيئات وضع المعايير وغير ذلك من المنظمات المماثلة.

قائمة بمعايير النظام SS7 (ليست حصرية)

توصيات قطاع تقييس الاتصالات

- توصيات السلسلة ITU‑T Q.700 (بروتوكول نقل الرسائل (MTP)، النظام الفرعي للتحكم بتوصيلات التشوير (SCCP)، جزء تطبيق مقدرات المعاملات (TCAP)، جزء المستعمل في الخدمات الهاتفية (TUP)، جزء المستعمل في خدمة الشبكة الرقمية المتكاملة (ISUP))

- التوصيات ITU‑T Q.1699‑Q.1200 (الشبكات الذكية)

- التوصية ITU‑T Q.1912.5 (التشغيل البيني بين SIP-I وISUP)

مواصفات المعهد الأوروبي لمعايير الاتصالات/مشروع شراكة الجيل الثالث

- المعيار 3GPP TS 09.02 (جزء التطبيق المتنقل، MAP)

- المعيار 3GPP TS 09.78، 3GPP TS 29.078 (جزء التطبيق CAMEL، CAP)

طلبات الحصول على تعليقات الصادرة عن فريق مهام هندسة الإنترنت

- RFC 4960، بروتوكول إرسال التحكم في قطار البتات (SCTP)

- RFC 5133، تكييف بيئة مستعمل الشبكة ISDN (IUA)

- RFC 4165، طبقة تكييف بيئة المستعمل من ند إلى ند (M2PA) للمستوى 2 من جزء نقل الرسائل (MTP)

- RFC 3331، طبقة تكييف بيئة المستعمل للمستوى 2 من جزء نقل الرسائل (M2UA)

- RFC 4666، طبقة تكييف بيئة المستعمل للمستوى 3 من جزء نقل الرسائل (M3UA)

- RFC 3868، تكييف بيئة المستعمل (SUA) لجزء التحكم بتوصيلات التشوير (SCCP)

- RFC 3807، تكييف بيئة مستعمل V5 (V5UA)

- RFC 4129، تكييف بيئة مستعمل DPNSS/DASS2 (DUA)

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

# 2 ورشة عمل الاتحاد بشأن "[مكافحة التزييف باستخدام حلول المطابقة وقابلية التشغيل البيني](http://www.itu.int/en/ITU-T/Workshops-and-Seminars/20160628/Pages/default.aspx)"، 28 يونيو 2016 (الساعة 1800-1400)

**مقدمة**

ينص [القرار 188](http://www.itu.int/pub/S-CONF-ACTF-2014) (بوسان، 2014) لمؤتمر المندوبين المفوضين للاتحاد بشأن "مكافحة أجهزة الاتصالات/تكنولوجيا المعلومات والاتصالات الزائفة" على تكليف مديري المكاتب الثلاثة بمساعدة الدول الأعضاء في معالجة شواغلها إزاء أجهزة الاتصالات/ تكنولوجيا المعلومات والاتصالات الزائفة عن طريق تبادل المعلومات على الصعيدين الإقليمي أو العالمي، بما في ذلك أنظمة تقييم المطابقة.

كما حددت أيضاً ورشة العمل التي نظمها الاتحاد في نوفمبر 2014 بشأن "[مكافحة أجهزة تكنولوجيا المعلومات والاتصالات الزائفة والمخالِفة للمعايير](http://www.itu.int/en/ITU-T/C-I/Pages/WSHP_counterfeit.aspx)"، نطاق المشاكل والآثار السلبية للتزييف بما فيها خسارة الضرائب والعوائد وغيرها من الإيرادات؛ وانخفاض المبيعات والأسعار والعمليات؛ وتضاؤل قيمة العلامة التجارية والنوايا الحسنة والسمعة؛ وانخفاض الحافز للابتكار والاستثمار؛ وانخفاض معدلات التوظيف والنمو الاقتصادي؛ وتعرض الشبكات للانقطاعات والتحديات المتعلقة بقابلية التشغيل البيني الناتجة عن تدني جودة الخدمات المقدمة واستقبالها؛ والمخاطر على الصحة والسلامة والبيئة.

وفي المستقبل ستكون هناك حاجة إلى اتخاذ إجراءات لمكافحة تزييف منتجات تكنولوجيا المعلومات والاتصالات. ولذلك تقود حالياً [لجنة الدراسات 11 لقطاع تقييس الاتصالات في إطار المسألة 8 (Q.8)](http://www.itu.int/en/ITU-T/studygroups/2013-2016/11/Pages/q8.aspx) دراسات لتحديد جميع الحلول التقنية الممكنة لمكافحة أجهزة تكنولوجيا المعلومات والاتصالات الزائفة. ونشر الفريق المعني بالمسألة 8 [تقريراً تقنياً عن أجهزة تكنولوجيا المعلومات والاتصالات الزائفة](http://www.itu.int/pub/T-TUT-CCICT)، ووُضع عدداً من بنود العمل الجديدة، بما في ذلك مشروع توصية جديدة بعنوان "[إطار لحلول مكافحة أجهزة تكنولوجيا المعلومات والاتصالات الزائفة](http://web.itu.int/ITU-T/workprog/wp_item.aspx?isn=10502)".

وبالإضافة إلى ذلك، جرت داخل الاتحاد وفي جميع أرجاء العالم مناقشات بشأن تحديد ما إذا كان من الممكن لبرامج المطابقة وقابلية التشغيل البيني أن تكون أحد الحلول التقنية لمكافحة أجهزة تكنولوجيا المعلومات والاتصالات الزائفة.

الأهداف

ترمي ورشة العمل إلى ما يلي:

• التوعية بالدراسات الجارية حالياً في لجنة الدراسات 11 لقطاع تقييس الاتصالات في إطار المسألة 8، وخصوصاً تعزيز تطوير التوصية التقنية "[إطار لحلول مكافحة أجهزة تكنولوجيا المعلومات والاتصالات الزائفة](http://web.itu.int/ITU-T/workprog/wp_item.aspx?isn=10502)"؛

• تحديد ما إذا كان من الممكن لبرامج المطابقة وقابلية التشغيل البيني أن تساعد على مكافحة أجهزة تكنولوجيا المعلومات والاتصالات الزائفة؛

• فهم الاتجاهات والآليات الجديدة في تزييف أجهزة تكنولوجيا المعلومات والاتصالات والتلاعب بمعرّفات الهوية الفريدة للأجهزة و/أو استنساخها؛

• فهم آليات تأمين إدارة سلسلة التوريد (بدءاً من التصنيع ثم الاستيراد ووصولاً إلى التوزيع والتسويق) لضمان تتبع وأمن وخصوصية وثقة الأشخاص والمنتجات والشبكات؛

• مواصلة التوعية بمشكلة تزييف أجهزة تكنولوجيا المعلومات والاتصالات وأخطارها؛

• التماس آراء ومقترحات وأفكار من الخبراء في الاتحاد وفي جميع أنحاء العالم من أجل إجراء مزيد من الدراسات خلال فترة الدراسة المقبلة.

الجمهور المستهدف

الدعوة موجهة إلى الأعضاء وغير الأعضاء في الاتحاد على السواء. ويرحَّب خصوصاً بمشاركة البائعين والمصنِّعين والمؤسسات البحثية والهيئات الأكاديمية والمختبرات والهيئات التنظيمية والمشغلين والمنظمات غير الحكومية والسلطات الجمركية والوكالات الأمنية وهيئات وضع المعايير وتقييم المطابقة وغير ذلك من المنظمات المماثلة.

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

أت‍منى لكم حدثين مثمرين وم‍متعين.

وتفضلوا بقبول فائق التقدير والاحترام.

تشيساب لي
مدير مكتب تقييس الاتصالات