الاتحـــــــــــاد الدولـــــــــــي للاتصـــــــــــالات

ITU-T

قطاع تقييس الاتصالات
في الاتحاد الدولي للاتصالات

X.1248

(2017/09)

السلسلة X: شبكات البيانات والاتصالات بين الأنظمة المفتوحة ومسائل الأمن

أمن الفضاء السيبراني – مكافحة الرسائل الاقتحامية

المتطلبات التقنية لمكافحة اقتحام المراسلة اللحظية

التوصية ITU-T X.1248

الاتحاد الدولي للاتصالات

توصيات السلسلة X الصادرة عن قطاع تقييس الاتصالات

شبكات البيانات والاتصالات بين الأنظمة المفتوحة ومسائل الأمن

الشبكات العمومية للبيانات	X.199-X.1
التوصيل البيني للأنظمة المفتوحة	X.299-X.200
التشغيل البيني للشبكات	X.399-X.300
أنظمة معالجة الرسائل	X.499-X.400
الدليل	X.599-X.500
التشغيل البيني لأنظمة التوصيل OSI ومظاهر النظام	X.699-X.600
إدارة التوصيل البيني للأنظمة المفتوحة (OSI)	X.799-X.700
الأمن	X.849-X.800
تطبيقات التوصيل البيني للأنظمة المفتوحة (OSI)	X.899-X.850
المعالجة الموزعة المفتوحة	X.999-X.900
آمن المعلومات والشبكات	
الجوانب العامة للأمن	X.1029-X.1000
أمن الشبكة	X.1049-X.1030
إدارة الأمن	X.1069-X.1050
الخصائص البيومترية	X.1099-X.1080
تطبيقات وخدمات آمنة (1)	
أمن البث المتعدد	X.1109-X.1100
أمن الشبكة المحلية	X.1119-X.1110
أمن الخدمات المتنقلة	X.1139-X.1120
أمن الويب	X.1149-X.1140
بروتوكولات الأمن (1)	X.1159-X.1150
الأمن بين جهتين نظيرتين	X.1169-X.1160
أمن معرفات الهوية عبر الشبكات	X.1179-X.1170
أمن التلفزيون القائم على بروتوكول الإنترنت	X.1199-X.1180
آمن الفضاء السيبراني	
الأمن السيبراني	X.1229-X.1200
مكافحة الرسائل الاقتحامية	**X.1249-X.1230**
إدارة الهوية	X.1279-X.1250
تطبيقات وخدمات آمنة (2)	
اتصالات الطوارئ	X.1309-X.1300
أمن شبكات المحاسيس واسعة الانتشار	X.1319-X.1310
أمن شبكة الكهرباء الذكية	X.1339-X.1330
البريد المعتمد	X.1349-X.1340
أمن إنترنت الأشياء (IoT)	X.1369-X.1360
أمن أنظمة النقل الذكية (ITS)	X.1389-X.1370
أمن سجل الحسابات الموزع	X.1429-X.1400
البروتوكول الأمني (2)	X.1459-X.1450
تبادل معلومات الأمن السيبراني	
نظرة عامة عن الأمن السيبراني	X.1519-X.1500
تبادل مواطن الضعف/الحالة	X.1539-X.1520
تبادل الأحداث/الأحداث العارضة/المعلومات الحدسية	X.1549-X.1540
تبادل السياسات	X.1559-X.1550
طلب المعلومات الحدسية والمعلومات الأخرى	X.1569-X.1560
تعرف الهوية والاكتشاف	X.1579-X.1570
التبادل المضمون	X.1589-X.1580
آمن الحوسبة السحابية	
نظرة عامة على أمن الحوسبة السحابية	X.1601-X.1600
تصميم أمن الحوسبة السحابية	X.1639-X.1602
أفضل الممارسات ومبادئ توجيهية بشأن أمن الحوسبة السحابية	X.1659-X.1640
تنفيذ أمن الحوسبة السحابية	X.1679-X.1660
أمن أشكال أخرى للحوسبة السحابية	X.1699-X.1680

لمزيد من التفاصيل يرجى الرجوع إلى قائمة التوصيات الصادرة عن قطاع تقييس الاتصالات.

التوصية ITU-T X.1248

المتطلبات التقنية لمكافحة اقتحام المراسلة اللحظية

ملخص

تحدد التوصية ITU-T X.1248 خصائص اقتحام المراسلة اللحظية (SPIM) وتوصف المتطلبات التقنية لمكافحته. ومع تزايد المراسلة اللحظية (IM) في شيوعها، أصبح انتشار الاقتحام SPIM مشكلة متزايدة الخطورة. وتمكن خصائص المراسلة اللحظية، مثل اعتمادها على بروتوكول الإنترنت واستعمالها المجاني على نطاق واسع من السماح للاقتحام SPIM من الانتشار بشكل كبير وبصورة خارج السيطرة. وإذا لم تعالج مشكلات الاقتحام SPIM بعناية، يمكن أن تؤثر بالسلب على استخدام خدمة المراسلة اللحظية ذاتها.

التسلسل التاريخي

الطبعة	التوصية	تاريخ الموافقة	لجنة الدراسات	معرف الهوية الفريد*
1.0	ITU-T X.1248	2017-09-06	17	11.1002/1000/13262

مصطلحات أساسية

اقتحام المراسلة اللحظية (SPIM).

* للنفاذ إلى توصية، ترجى كتابة العنوان http://handle.itu.int/ في حقل العنوان في متصفح الويب لديكم، متبوعاً بمعرف التوصية الفريد. ومثال ذلك، http://handle.itu.int/11.1002/1000/11830-en.

تمهيد

الاتحاد الدولي للاتصالات وكالة متخصصة للأمم المتحدة في ميدان الاتصالات وتكنولوجيات المعلومات والاتصالات (ICT). وقطاع تقييس الاتصالات (ITU-T) هو هيئة دائمة في الاتحاد الدولي للاتصالات. وهو مسؤول عن دراسة المسائل التقنية والمسائل المتعلقة بالتشغيل والتعريفة، وإصدار التوصيات بشأنها بغرض تقييس الاتصالات على الصعيد العالمي.

وتحدد الجمعية العالمية لتقييس الاتصالات (WTSA) التي تجتمع مرة كل أربع سنوات المواضيع التي يجب أن تدرسها لجان الدراسات التابعة لقطاع تقييس الاتصالات وأن تُصدر توصيات بشأنها.

وتتم الموافقة على هذه التوصيات وفقاً للإجراء الموضح في القرار 1 الصادر عن الجمعية العالمية لتقييس الاتصالات.

وفي بعض مجالات تكنولوجيا المعلومات التي تقع ضمن اختصاص قطاع تقييس الاتصالات، تُعد المعايير اللازمة على أساس التعاون مع المنظمة الدولية للتوحيد القياسي (ISO) واللجنة الكهرتقنية الدولية (IEC).

ملاحظة

تستخدم كلمة "الإدارة" في هذه التوصية لتدل بصورة موجزة سواء على إدارة اتصالات أو على وكالة تشغيل معترف بها.

والتقيد بهذه التوصية اختياري. غير أنها قد تضم بعض الأحكام الإلزامية (بهدف تأمين قابلية التشغيل البيني والتطبيق مثلاً). ويعتبر التقيّد بهذه التوصية حاصلاً عندما يتم التقيّد بجميع هذه الأحكام الإلزامية. ويستخدم فعل "يجب" وصيغ ملزمة أخرى مثل فعل "ينبغي" وصيغها النافية للتعبير عن متطلبات معينة، ولا يعني استعمال هذه الصيغ أن التقيّد بهذه التوصية إلزامي.

حقوق الملكية الفكرية

يسترعي الاتحاد الانتباه إلى أن تطبيق هذه التوصية أو تنفيذها قد يستلزم استعمال حق من حقوق الملكية الفكرية. ولا يتخذ الاتحاد أي موقف من القرائن المتعلقة بحقوق الملكية الفكرية أو صلاحيتها أو نطاق تطبيقها سواء طالب بها عضو من أعضاء الاتحاد أو طرف آخر لا تشمله عملية إعداد التوصيات.

وعند الموافقة على هذه التوصية، لم يكن الاتحاد قد تلقى إخطاراً بملكية فكرية تحميها براءات الاختراع يمكن المطالبة بها لتنفيذ هذه التوصية. ومع ذلك، ونظراً إلى أن هذه المعلومات قد لا تكون هي الأحدث، يوصى المسؤولون عن تنفيذ هذه التوصية بالاطلاع على قاعدة البيانات الخاصة ببراءات الاختراع في مكتب تقييس الاتصالات (TSB) في الموقع http://www.itu.int/ITU-T/ipr/.

جدول المحتويات

الصفحة

مقدمة

مع التطور السريع للإنترنت والإنترنت المتنقلة، تطورت المراسلة اللحظية (IM) من وسيلة دردشة بسيطة إلى منصة معلومات متكاملة تضم الاتصالات والمعلومات والترفيه والبحث والتجارة الإلكترونية والتعاون في الأعمال التجارية وخدمات عملاء الشركات ككل. ونظراً إلى انخفاض أسعارها وسهولة استعمالها، يتحول المزيد والمزيد من الأشخاص إلى المراسلة اللحظية وهو ما يؤثر بشدة على مجالات الاتصالات التقليدية. ويقوم مشغلو الاتصالات حالياً وبشكل متزايد بتوفير خدمات المراسلة اللحظية؛ ولكن في الوقت نفسه أصبحت المراسلة اللحظية عرضة بشكل خطير لنشر الرسائل الاقتحامية على خدمات الصوت وخدمة الرسائل القصيرة (SMS). ومشغلو الاتصالات حول العالم على علم بالاقتحام SPIM و/أو تأثروا به بدرجات متفاوتة. والاقتحام SPIM لا يستنزف موارد الشبكة فحسب، ولكنه يتسبب أيضاً في خسارة المستعملين للوقت والإنتاجية. وإلى جانب ذلك، يستخدم الاقتحام SPIM من أجل التدليس ونشر الفيروسات والديدان وبرمجيات التجسس وغيرها من أشكال البرمجيات الضارة، بل يمكنها أن تحمل ربما معلومات ضارة مسيئة للمستعملين. لذا، يحد الاقتحام SPIM من رضاء المستعملين عند استعمال المراسلة اللحظية وأصبح هذا الأمر عاملاً مهماً يقف عائقاً أمام استعمال المراسلة اللحظية.

وبرغم تنفيذ الكثير من التدابير المضادة للاقتحام في أنظمة المراسلة اللحظية، لا تزال هناك مواطن ضعف كثيرة في هذه الأنظمة يمكن أن تتسبب في الاقتحام SPIM، مثل: معدلات التسجيل غير المحدودة والافتقار إلى التحقق عند استلام الرسائل وآليات الإرسال الشبكي غير المؤمنة وعدم وجود ضوابط لمعدلات إرسال الرسائل بالنسبة إلى المستعملين ومواطن الضعف التي لا مفر منها في أنظمة المراسلة اللحظية.

وتوصف هذه التوصية المتطلبات التقنية لمكافحة الاقتحام SPIM في ضوء وظائف نظام المراسلة اللحظية من أجل وقف وسائل إنتاج ونشر رسائل الاقتحام SPIM. فعلى سبيل المثال، من المهم فرض تصميم آلية تسجيل لمنع عمليات التسجيل الضخمة الأوتوماتية وأن يزود نظام المراسلة اللحظية المستعملين بوظيفة للاختيار بين استلام أو حجب جميع الرسائل من كيانات مرخصة/غير مرخصة وتقييد معدلات إرسال المستعملين في حال تجاوزهم عتبة معقولة.

التوصية ITU-T X.1248

المتطلبات التقنية لمكافحة اقتحام المراسلة اللحظية

1 مجال التطبيق

تعرف هذه التوصية أنواع وخصائص اقتحام المراسلة اللحظية (SPIM). وللتخفيف من حدة إنتاج ونشر رسائل الاقتحام SPIM، توصف هذه التوصية المتطلبات التقنية لمكافحة الاقتحام SPIM، تشمل عميل المراسلة اللحظية ومخدم المراسلة اللحظية. وتركز هذه التوصية بشكل رئيسي على التدابير المضادة للاقتحام SPIM في طبقة نظام المراسلة اللحظية ويمكن تطبيقها على مشغلي خدمات المراسلة اللحظية.

2 المراجع

لا يوجد.

3 التعاريف

1.3 مصطلحات معرَّفة في مواضع أخرى

تستعمل هذه التوصية المصطلحات التالية المعرفة في مواضع أخرى:

1.1.3 المراسلة اللحظية (IM) [b-IETF RFC 3428]: تبادل محتوى بين مجموعة من المشاركين في وقت قريب من الوقت الفعلي. وعادةً يكون المحتوى رسائل نصية قصيرة، وإن لم تكن مقصورة على هذا الشكل.

2.1.3 الاقتحام (spam) [b-ITU-T X.1240]: يتوقف معنى كلمة "اقتحام" على النظرة المحلية للخصوصية وعلى ما يمثله الاقتحام من المنظور الوطني التقني والاقتصادي والاجتماعي والعملي. ويتطور معنى الكلمة ويتسع خصوصاً مع تطور أنواع التكنولوجيا وتوفيرها فرصاً جديدة لإساءة استخدام الاتصالات الإلكترونية. وعلى الرغم من عدم وجود أي تعريف متفق عليه عالمياً للاقتحام، يُستعمل هذا المصطلح عموماً لوصف الرسائل الإلكترونية غير المطلوبة التي ترسَل بالجملة عبر البريد الإلكتروني أو بواسطة خدمة المراسلة المتنقلة لأغراض الترويج التجاري لمنتجات أو خدمات ما.

3.1.3 اقتحام المراسلة اللحظية (SPIM) [b-ITU-T X.1244]: اقتحام يستهدف مستعملي خدمة المراسلة اللحظية.

4.1.3 المقتحِم (spimmer) [b-ITU-T X.1244]: مُرسِل رسائل اقتحام المراسلة اللحظية.

2.3 مصطلحات معرفة في هذه التوصية.

لا يوجد.

4 المختصرات والأسماء المختصرة

تستخدم هذه التوصية الاختصارات والأسماء المختصرة التالية:

ID الهوية *(Identity)*

IM المراسلة اللحظية *(Instant Messaging)*

IP بروتوكول الإنترنت *(Internet Protocol)*

SMS خدمة الرسائل القصيرة *(Short Message Service)*

SPIM اقتحام المراسلة اللحظية *(Spam over Instant Messaging)*

5 الاصطلاحات

لا يوجد.

6 خصائص رسائل الاقتحام SPIM وسيناريوهات إنتاجها

تشير رسائل الاقتحام SPIM إلى رسالة لحظية يستلمها مستعمل ما ويُرى أنها غير مطلوبة أو تسبب الإزعاج لهذا المستعمل. من هنا، تتسم رسائل الاقتحام SPIM بالخصائص التالية:

- تحدث عادةً في الوقت الفعلي. ففي الحالة التي يكون فيها المرسل والمستلم على الخط، تستعمل الرسالة SPIM في نفس توقيت إرسالها تقريباً. حتى عندما لا يكون المستلم على الخط وقتها، فإن الرسالة SPIM يمكن استلامها بمجرد توصيل المستلم؛
- ترسل غالباً في مجموعات كبيرة، وبالتالي، ترسل أعداد ضخمة من الرسائل ذات المحتوى ذاته في نفس الوقت؛
- المقتحم هو مصطلح يستعمل لتعريف مرسل الرسائل SPIM غير المرخص له إلى مستلمي رسائل المراسلة اللحظية. ومع ذلك، يمكن في بعض الأوقات انتهاك حساب أحد الأصدقاء وتوجيهه لإرسال رسائل SPIM نتيجةً لإصابته بشفرة ضارة أو نتيجةً لكشف معلومات الحساب وكلمة السر. والرسائل SPIM التي ترسل عبر أصدقاء تكون أكثر خداعاً، خاصةً إذا تضمنت روابط إلى مواقع إلكترونية ضارة أو ملفات قابلة للتنفيذ يقوم معظم المستلمين بالنقر عليها وبالتالي يزيد احتمال إصابة أنظمتهم بالشفرة الضارة؛
- لا يمكن تتبع الرسائل SPIM بسهولة نظراً إلى أنه يمكن إنشاء الحسابات بصورة اعتباطية وعادةً ما تكون غير قابلة للتتبع لهوية حقيقية.

ويتعلق إنتاج الرسائل SPIM بشكل وثيق بوظائف نظام المراسلة اللحظية (راجع التذييل I)، وفيما يلي السيناريوهات التي يمكن أن تنتج رسائل SPIM:

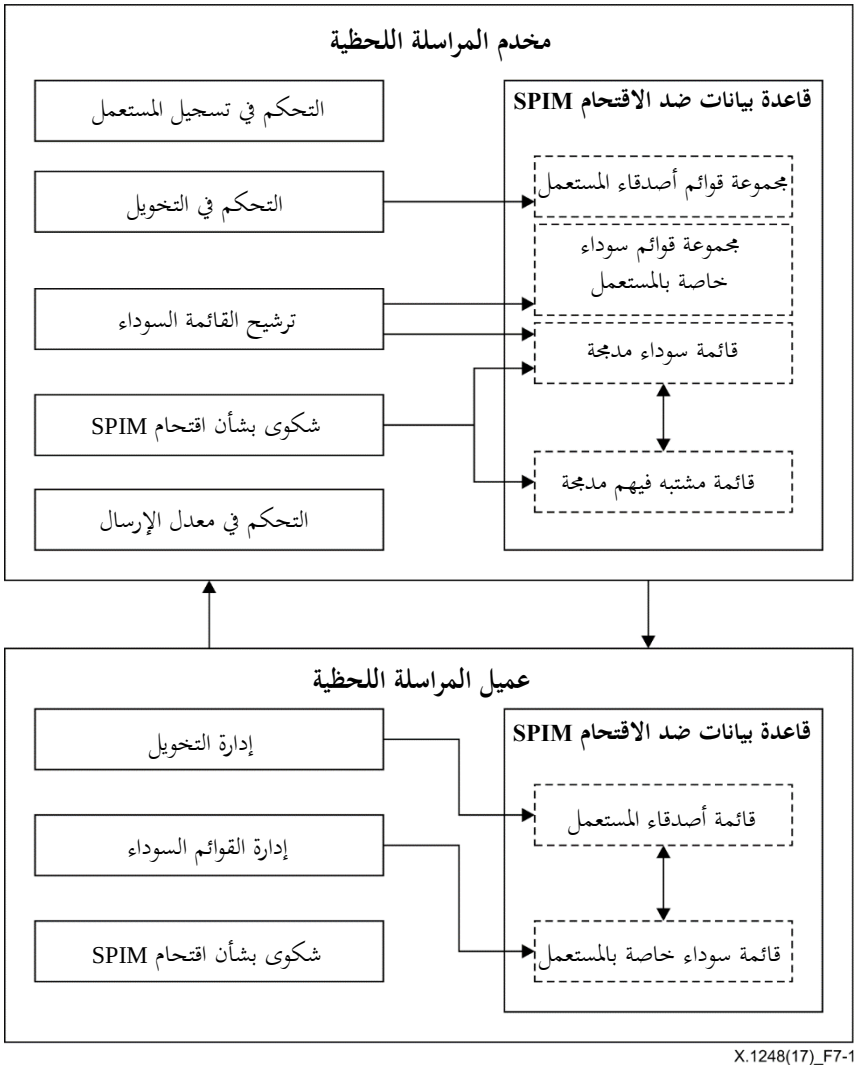
- يمكن للمقتحمين استعمال برمجية للتسجيل الأوتوماتي لتسجيل عدد ضخم من الحسابات واستعمالها في نشر الرسائل SPIM؛
- يمكن للمستعملين ذوي النوايا السيئة استعمال حسابات زائفة للمراسلة اللحظية واستعمالها في إرسال الرسائل SPIM؛
- إذا حصل مهاجم ضار على وسيلة للتحكم في حساب مستعمل شرعي بدون ترخيص، يمكنه تعديل معلومات المستعمل مثل كلمة السر أو معلومات الاستيقان الأخرى، لاستخدام هذا الحساب (غالباً لمدة طويلة) في إرسال الرسائل SPIM؛
- في حالة تعديل معلمة استلام أي من عملاء المراسلة اللحظية بدون ترخيص، يمكن استقبال الرسائل SPIM بدون أي قيود؛
- يمكن التلاعب في الرسائل اللحظية أثناء إرسالها. يمكن دمج الإعلانات أو الشفرات الضارة ضمن أي رسالة لحظية وتحويلها إلى رسالة SPIM؛
- نتيجة للافتقار إلى آليات التحقق، يمكن أن يكون للمقتحم الحرية في إضافة أصدقاء وإرسال رسائل SPIM إليهم.

ولمنع الرسائل SPIM، من الضروري دراسة خصائصها بشكل كامل والسيناريوهات التي تؤدي إليها وذلك من أجل اتخاذ تدابير وقائية شاملة.

7 معمارية وظيفية للمراسلة اللحظية لمكافحة الاقتحام SPIM

1.7 نظرة عامة

يوضح الشكل 7-1 المعمارية الوظيفية للمراسلة اللحظية لمكافحة الاقتحام SPIM



الشكل 7-1 – المعمارية الوظيفية للمراسلة اللحظية لمكافحة الاقتحام SPIM

تضم هذه المعمارية وظائف لمكافحة الاقتحام SPIM، بما في ذلك مراشيح القوائم السوداء وضوابط تسجيل المستعمل والشكاوى بشأن الاقتحام SPIM. والأكثر أهمية هو أن هذه المعمارية تدعم الترشيح على أساس تقييد معدل إرسال الرسائل اللحظية والتحكم في الترخيص لمرسل الرسائل اللحظية.

ويصف التذييل I، بتفصيل أكبر، وظائف عميل ومخدم المراسلة اللحظية ودور مرسل الرسائل اللحظية ومستلمها والمقتحم.

2.7 وظائف المكونات

1.2.7 مخدم المراسلة اللحظية

تشمل وظيفة مكون مخدم المراسلة اللحظية العناصر الستة التالية:

1) التحكم في تسجيل المستعمل

يلزم استعمال أساليب تحقق يدوية مثل شفرات التحقق وعمليات التحقق عبر البريد الإلكتروني وشفرات التحقق بخدمة الرسائل القصيرة، وذلك لمنع المستعملين من التسجيل الأوتوماتي. ويمنع ذلك المقتحمين الذين لديهم عدد ضخم من الحسابات المسجلة أوتوماتياً من إرسال الرسائل SPIM.

2) التحكم في التخويل

يتعين تقديم طلب من المستعمل لإضافة صديق التخويل علاقة الصديق بالمستعمل على أساس تعليقات عميل المراسلة اللحظية.

3) ترشيح القائمة السوداء

يجب أن يرشح مخدم المراسلة اللحظية الرسائل اللحظية على أساس قائمة سوداء مدمجة ومجموعة من القوائم السوداء الخاصة بالمستعمل.

4) الشكاوى بشأن الرسائل SPIM

يجب قبول شكاوى المستعملين بخصوص الحسابات التي ترسل رسائل SPIM وتحديد ما إذا كان يتعين إضافة هذه الحسابات إلى القائمة السوداء المدمجة للمشتبه فيهم أو إلى القائمة السوداء المدمجة. ويتعين التواصل مع أنظمة خارجية للبت في الشكاوى المتعلقة بالرسائل SPIM واستيراد القوائم السوداء المدمجة وتصديرها.

5) التحكم في معدل الإرسال

يتعين التحكم في عدد الرسائل اللحظية المرسلة من نفس الحساب في غضون فترة زمنية معينة. وينبغي نبذ الرسائل اللحظية التي تتجاوز هذه العتبة.

6) قاعدة البيانات المضادة للرسائل SPIM

- مجموعة قوائم أصدقاء المستعمل: تتضمن قوائم أصدقاء جميع المستعملين التي يديرها مخدم المراسلة اللحظية. ويتعين مزامنة مجموعة قوائم أصدقاء المستعملين في المراسلة اللحظية مع قوائم أصدقاء المستعملين في عملاء المراسلة اللحظية.
- مجموعة القوائم السوداء الخاصة بالمستعمل: تتضمن القوائم السوداء الخاصة بالمستعمل لجميع المستعملين التي يديرها مخدم المراسلة اللحظية. ويتعين مزامنة هذه القوائم الموجودة في مخدم المراسلة اللحظية مع نظيرتها في عملاء المراسلة اللحظية.
- القائمة السوداء المدمجة: تتضمن الحسابات الموجودة في الشكاوى المرفوعة من المستعملين والحسابات التي اكتشفها مخدم المراسلة اللحظية. فعلى سبيل المثال، إذا تجاوز مستعمل المراسلة اللحظية المعدل المحدد بعتبة معينة من الرسائل المرسلة، يضيف مخدم المراسلة اللحظية معرف هوية المرسل ويضيفه إلى القائمة السوداء المدمجة. وتتضمن القائمة السوداء المدمجة أيضاً الحسابات المستوردة من أنظمة أخرى مثل مخدمات المراسلة اللحظية الأخرى.
- قائمة المشتبه فيهم المدمجة: يتعين وضع قائمة بجميع الحسابات المشتبه فيها التي يديرها مخدم المراسلة اللحظية. ويمكن وضع هذه القائمة من خلال شكاوى المستعملين واستيرادها من أنظمة أخرى، وما إلى ذلك.

2.2.7 عميل المراسلة اللحظية

تتضمن وظائف مكون عميل المراسلة اللحظية العناصر الأربعة التالية:

1) إدارة التخويل

ينبغي وجود مكونين رئيسيين، التحكم في رؤية هوية المراسلة IM وإدارة الطلبات، من الكيانات غير المخولة. بالنسبة إلى المكون الأول من الضروري أن يحدد أي مستعمل ما إذا كان ينبغي لمستعمل غير مخول رؤية معلوماته (مثل هوية المراسلة IM والاسم الدارج والموقع). ولإدارة الطلبات من الكيانات غير المخولة، يتعين أن يكون المستعمل قادراً على اختيار سياسة مناسبة لمعالجة هذه الطلبات. وينبغي لأي مستعمل أن يكون قادراً على أن يوافق ويطلب إجابة دقيقة على سؤال شخصي أو حتى حجب جميع الطلبات. وعلاوةً على ذلك، ينبغي للمستعمل أن يملك القدرة على تحديد الأصدقاء الموثوق بهم وإدارة قائمة أصدقائه على عميل المراسلة IM.

2) إدارة القوائم السوداء

ينبغي للمستعملين أن يملكوا القدرة على إدارة قوائمهم السوداء بأنفسهم وينبغي حجب جميع الرسائل المرسلة من حسابات مدرجة في القوائم السوداء الخاصة بكل مستعمل. وينبغي أن يتسنى للمستعمل الإضافة أو الحذف في القائمة السوداء الخاصة به أو حتى تبادلها.

3) الشكاوى بشأن اقتحام SPIM

ينبغي وجود وظيفة في عميل المراسلة IM لتقديم الشكاوى عن الحسابات التي ترسل رسائل SPIM. وقد تكون الحسابات المشكو منها بيانات اتصال في قائمة أصدقاء المستعمل أو أعضاء في إحدى مجموعات المراسلة IM أو حتى أحد الحسابات غير المخولة التي ترسل طلبات للتخويل.

4) قاعدة بيانات ضد الاقتحام SPIM

- قائمة أصدقاء المستعمل: يلزم تخزين قائمة بالأصدقاء الموافَق عليهم من المستعمل.
- قائمة سوداء خاصة بالمستعمل: تحدد من قبل المستعملين وتتضمن الحسابات التي يرغب المستعمل في حجب الرسائل الواردة منها.

يجب أن يتسنى تحميل قاعدة البيانات الموجودة في عميل المراسلة IM أوتوماتياً في مخدم المراسلة IM.

8 إجراءات العمل

1.8 إجراء العمل الخاص بالتحكم في معدل إرسال الرسائل

ينبغي أن تضبط في مخدم المراسلة IM العتبة التي تحدد العدد الأقصى من الرسائل المسموح بإرسالها من حساب في المراسلة IM، وذلك في غضون مدة زمنية معينة.

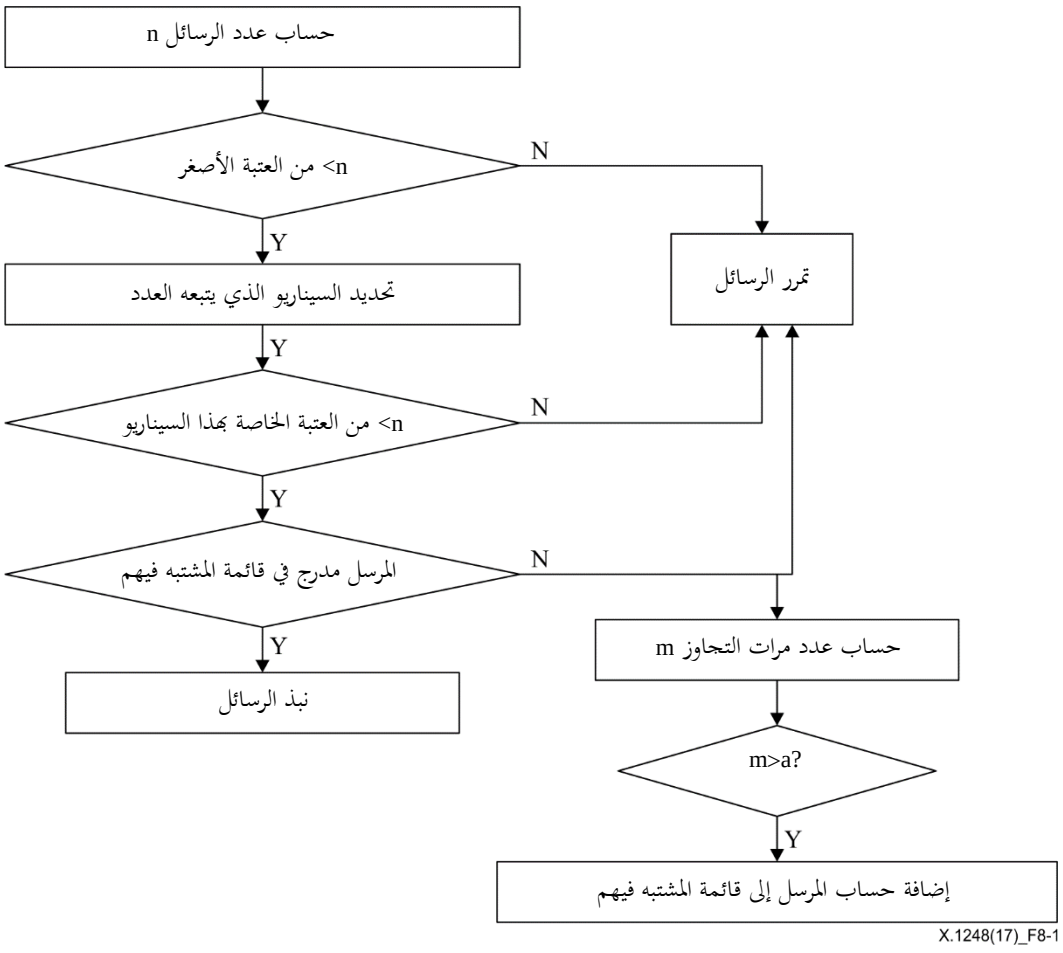
وتدرس العتبة أو تحسب باستعمال عدد ضخم من عينات رسائل المستعمل، وذلك باستعمال تكنولوجيات مثل التعلم الإلكتروني أو التعلم العميق وما إلى ذلك. وينبغي للعتبة أن تضبط السيناريوهات المختلفة، بما في ذلك، على سبيل الذكر وليس الحصر:

- الرسائل اللحظية المرسلة إلى مجموعة ويكون المرسل عضواً في المجموعة؛
- الرسائل اللحظية المرسلة إلى مجموعة ولا يكون المرسل عضواً في المجموعة؛
- الرسائل اللحظية المرسلة إلى واحد أو أكثر من أصدقاء المرسل؛
- الرسائل اللحظية المرسلة إلى أشخاص غير أصدقاء للمرسل.

وعندما يستلم مخدم المراسلة IM رسائل مرسلة من حساب محدد، ينفذ المخدم التحكم في معدل الإرسال عبر العملية التالية، وعلى النحو الموضح في الشكل 8-1:

- حساب عدد الرسائل المرسلة من الحساب في غضون مدة زمنية معينة؛
- مقارنة عدد الرسائل المرسلة (n) بالعتبة الدنيا المحددة لجميع السيناريوهات. وإذا تجاوز العدد n العتبة الدنيا، يحدد مخدم المراسلة IM السيناريو الذي ينتمي إليه هذا العدد وما إذا كان العدد n يتجاوز العتبة الخاصة بهذا السيناريو. وفي حالة عدم تجاوز العتبة، يمرر المخدم الرسائل؛
- إذا تجاوز عدد الرسائل n العتبة المحددة، يتحقق المخدم IM مما إذا كان الحساب مدرجاً في قائمة المشتبه فيهم المدمجة. إذا كان الحساب مدرجاً في هذه القائمة، يقوم المخدم IM بنبذ الرسائل، وإلا يمرر الرسائل ولكن مع حساب عدد مرات التجاوز (m). وإذا كان هذا الرقم m أكبر من رقم معين (*a*)، يضيف المخدم IM الحساب إلى قائمة المشتبه فيهم.

وتوضح في الشكل 8-1 عملية تنفيذ التحكم في معدل إرسال الرسائل:



الشكل 8-1 – عملية تنفيذ التحكم في معدل إرسال الرسائل

2.8 إجراء عمل القوائم السوداء

تعتبر أنظمة المراسلة IM مستقلة نسبياً، لذا يتعين أن يضع موردو خدمات المراسلة IM القوائم السوداء الخاصة بهم من أجل مخدماتهم IM. وإلى جانب ذلك، فإنه لتحقيق المصلحة للمستعملين، يتعين توفير القوائم السوداء الخاصة بالمستعملين لدى عملاء المراسلة IM.

وتجري عملية التفاعل بالنسبة إلى جميع أنواع القوائم السوداء في أي نظام IM كالتالي:

- يحرر المستعمل القائمة السوداء الخاصة به لدى عميل المراسلة IM. يراقب المخدم IM القائمة السوداء الخاصة بالمستعمل في الوقت الفعلي ويحدِّث مجموعة القوائم السوداء الخاصة بالمستعملين عند تغيرها؛
- يتتبع المخدم IM عدد المرات التي يضاف فيها نفس الحساب إلى القوائم السوداء الخاصة بالمستعملين. وإذا تجاوز العدد عتبة معينة، يضيف المخدم IM هذا الحساب إلى القائمة السوداء المدمجة؛
- يضيف المخدم IM الحساب المشار إليه في أي شكوى من أي عميل إلى القائمة السوداء المدمجة للمشتبه فيهم إذا لم يكن الحساب في القائمة السوداء المدمجة للمشتبه فيهم أو في القائمة السوداء المدمجة. ويحسب المخدم IM عدد المرات التي تسجل فيها شكوى بالنسبة إلى الحساب؛ فإذا تجاوز العدد عتبة معينة، يضيف المخدم IM هذا الحساب إلى القائمة السوداء المدمجة.

وتجري عملية ترشيح الرسائل على أساس القوائم السوداء على النحو التالي:

- عندما يستلم المخدم IM رسالة، يتحقق المخدم مما إذا كان حساب المرسل مدرج في القائمة السوداء المدمجة؛ وفي هذه الحالة، يقوم المخدم IM بنبذ الرسالة؛
- إذا لم يكن حساب المرسل ضمن القائمة السوداء المدمجة، يمكن للمخدم IM التحقق أيضاً مما إذا كان حساب المرسل ضمن القائمة السوداء الخاصة بالمستعمل مستلم الرسالة، وفي هذه الحالة، يقوم المخدم IM بنبذ الرسالة. وخلاف ذلك يقوم المخدم IM بتمرير الرسالة.

3.8 إجراءات إدارة التخويل

يوصى بأن يكون لدى عميل المراسلة IM وظيفة تسمح للمستعملين بتحديد نوع ما يستلمونه من رسائل، وينبغي أن يكون للمخدم IM القدرة على ترشيح الرسائل غير المطلوبة طبقاً لما يحدده المستعمل وذلك لمنع المرسلين غير المخولين (مثل غير الأصدقاء، الأعضاء في مجموعة ما من غير الأصدقاء، أصدقاء في أنظمة IM أخرى، بيانات اتصال هاتفية) من إرسال رسائل غير مطلوبة. وتشمل السيناريوهات التي تخول المرسلين، على سبيل الذكر وليس الحصر، الخطوات الخمس التالية:

1) ضبط عميل المراسلة IM بحيث "لا يستلم إلا الرسائل المرسلة من الأصدقاء". وعند استلام المخدم IM رسالة مرسلة من المستعمل B إلى المستعمل A، يتحقق المخدم مما إذا كان المستعمل B ضمن قائمة أصدقاء المستعمل A. وإذا لم يكن كذلك، يقوم المخدم بنبذ الرسالة.

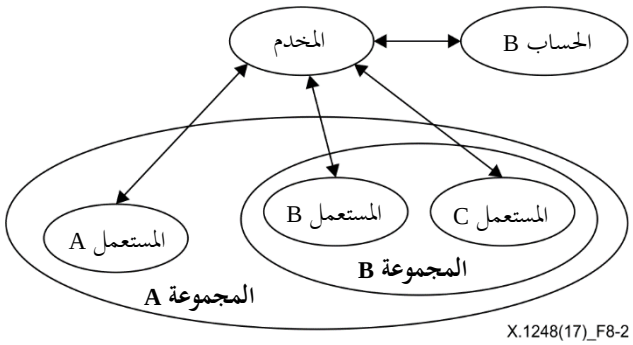
2) ضبط عميل المراسلة IM بحيث "يستلم الرسائل من مجموعة منضم إليها العميل صراحةً". عند استلام المخدم IM رسالة مرسلة من المجموعة B إلى المستعمل A، يتحقق المخدم مما إذا كان المستعمل A عضواً في المجموعة B. فإذا لم يكن كذلك، يقوم المخدم بنبذ الرسالة. وإضافةً إلى ذلك، عندما يستلم المخدم IM دعوة مرسلة من عضو في المجموعة B إلى المستعمل A، ينبغي أن يسمح المستعمل A قبل أن يضيف المخدم IM المستعمل A إلى المجموعة B.

3) ضبط عميل المراسلة IM بحيث "يستلم الرسائل من عضو في مجموعة يكون العميل صديق فيها". عندما يستلم المخدم IM رسالة مرسلة من المستعمل B العضو في المجموعة A إلى المستعمل A، يتحقق المخدم مما إذا كان المستعمل B ضمن قائمة أصدقاء المستعمل A. فإذا لم يكن كذلك، يقوم المخدم بنبذ الرسالة.

4) ضبط عميل المراسلة IM بحيث "يستلم الرسائل المرسلة من حسابات خاصة بأنظمة IM أخرى أو بيانات اتصال هاتفية فقط بعد أن تضاف هذه الحسابات أو البيانات صراحةً كأصدقاء". عندما يستلم المخدم IM رسالة مرسلة من حساب B منتسب إلى المستعمل A، يتحقق المخدم مما إذا كان الحساب B ضمن قائمة أصدقاء المستعمل A. وإذا لم يكن كذلك، يقوم المخدم بنبذ الرسالة. وكذلك، عندما يستلم المخدم IM طلباً لإضافة صديق من حساب B إلى قائمة أصدقاء المستعمل A، ينبغي أن يسمح المستعمل A قبل أن يضيف المخدم IM الحساب B إلى قائمة أصدقاء المستعمل A.

5) ضبط عميل المراسلة IM بحيث "يقيد إقامة توصيل من نقطة إلى نقطة على الأصدقاء فقط". عند استلام المخدم IM طلباً من المستعمل B لإقامة توصيل من نقطة إلى نقطة مع المستعمل A، يتحقق المخدم مما إذا كان المستعمل B ضمن قائمة أصدقاء المستعمل A. وفي هذه الحالة، يمرر المخدم طلب المستعمل B إلى المستعمل A ويساعد المستعملين A وB على إقامة توصيل من نقطة إلى نقطة. وإذا لم يكن كذلك، يقوم المخدم بنبذ طلب المستعمل B.

ويوضح الشكل 8-2 العلاقة بين المستعمل A وB والمجموعتين A وB والحساب B.



الشكل 8-2 – العلاقة بين المستعملين والمجموعات

4.8 إجراءات إدارة تسجيل المستعملين

لمنع تسجيل الحسابات أوتوماتياً، ينبغي للأنظمة IM أن تنفذ واحداً أو أكثر من تدابير التحقق اليدوية، مثل شفرة التحقق والتحقق بالبريد الإلكتروني وشفرة التحقق بالرسائل SMS.

وعندما يقوم مستعمل ما بتقديم معلومات التسجيل (مثل اسم المستعمل وكلمة السر ورقم الهاتف المحمول وعنوان البريد الإلكتروني) على عميل المراسلة IM أو على صفحة الويب الخاصة بتسجيل مستعملي المراسلة IM، يرسل المخدم IM تأكيد تسجيل ثانيةً إلى المستعمل، مثل شفرة أو شفرة تحقق برسالة SMS أو رسالة بريد إلكتروني لتأكيد التسجيل.

وبمجرد إرسال المستعمل تأكيد التسجيل بدوره إلى المخدم IM، يتحقق المخدم IM من تأكيد التسجيل المقدم من المستعمل. وإذا كان التحقق سليماً، يعيد المخدم رسالة نجاح للتسجيل إلى المستعمل ويحفظ معلومات تسجيل المستعمل في قاعدة البيانات. وإذا لم يكن كذلك، يعيد رسالة بفشل التسجيل.

ينبغي أن يتواصل النظام IM مع بوابة للخدمة SMS أو ينشر مخدم بريدي لتوفير وظيفة لإرسال شفرة تحقق SMS أو بريد إلكتروني لتأكيد التسجيل إلى المستعمل.

5.8 الإجراءات المتعلقة بالشكاوى من الرسائل SPIM

ينبغي دعم إجراءين للإبلاغ عن شكاوى بخصوص الرسائل SPIM، وهما:

1) الشكوى من خلال عميل المراسلة IM. وفي هذه الطريقة، توضح فيما يلي عملية معالجة الشكوى:

يقوم مستعملو المراسلة IM بوسم حساب الرسائل SPIM لدى عميل المراسلة IM بعد استلام الرسالة SPIM؛ وترسل الشكوى إلى المخدم IM. وينبغي للمخدم IM أن تكون له عتبة شكاوي محددة سلفاً. وعند استلام شكوى من مستعمل، يقوم المخدم IM أولاً بالتحقق مما إذا كان الحساب مدرجاً بالفعل ضمن القائمة السوداء المدمجة للمشتبه فيهم أو ضمن القائمة السوداء المدمجة. وإذا لم يكن الوضع كذلك، يضيف المخدم IM الحساب إلى قائمة المشتبه فيهم المدمجة ويحسب عدد المرات التي وردت فيها شكوى من الحساب. فإذا تجاوز هذا العدد العتبة المحددة سلفاً، يضيف المخدم IM الحساب إلى القائمة السوداء المدمجة. وإذا كان الحساب مدرجاً بالفعل في القائمة السوداء المدمجة للمشتبه فيهم، يقوم المخدم IM بتجميع عدد مرات الشكوى من الحساب. فإذا تجاوزت هذه القيمة العتبة المحددة سلفاً خلال فترة زمنية معينة، يضيف

المخدم IM هذا الحساب إلى القائمة السوداء المدمجة، ولا يقوم المخدم IM بأي إجراء. ويقوم المخدم IM بعد ذلك بنبذ الرسائل التي ترسل من هذا الحساب بعد ذلك.

2) الشكوى عبر نظام خارجي لمعالجة شكاوى الرسائل SPIM. وفي هذه الطريقة توضح فيما يلي عملية معالجة الشكوى:

يقدم مستعملو المراسلة IM شكوى إلى نظام خارجي لمعالجة شكاوى الرسائل SPIM بعد استلام الرسالة SPIM. ويتولى هذا النظام الخارجي مسؤولية تحليل شكوى المستعمل ويقرر ما إذا كان يضيف الحساب المشكو منه ضمن القائمة السوداء. ويتواصل المخدم IM مع نظام خارجي لمعالجة شكاوى الرسائل SPIM ويستورد القائمة السوداء ويصدرها من السطح البيني للتواصل. ويجب أن يقوم المخدم IM بنبذ الرسائل المرسلة من حسابات مدرجة في القائمة السوداء.

6.8 إجراء ترشيح الرسائل SPIM

عندما يستلم المخدم IM رسائل لحظية، يقوم بتنفيذ عملية ترشيح للرسائل SPIM على أساس القائمة السوداء المدمجة ومجموعة القوائم السوداء الخاصة بالمستعملين؛ ويرد شرح هذه العملية في الفقرة 2.8.

وإذا لم يكن الحساب مرسل المراسلة IM ضمن القائمة السوداء المدمجة ومجموعة القوائم السوداء الخاصة بالمستعملين، يقوم المخدم IM بعد ذلك بتنفيذ عملية ترشيح للرسائل SPIM على أساس التحكم في التخويل ويبحث ما إذا كان المرسل يملك التخويل بإرسال رسائل إلى المستلم (الذي يقوم المستلم بضبطه). وإذا لم يكن الأمر كذلك، تنبذ الرسالة. ويرد شرح لسيناريو التخويل في الفقرة 3.8.

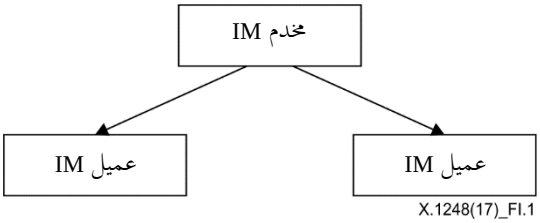
وإذا كان المرسل يملك التخويل، يقوم المخدم IM بعد ذلك بتنفيذ عملية ترشيح للرسائل SPIM على أساس حد معدل إرسال الرسائل؛ ويرد شرح لهذه العملية في الفقرة 1.8.

التذييل I

الأدوار والوظائف في نظام المراسلة اللحظية

(لا يشكل هذا التذييل جزءاً أساسياً من هذه التوصية)

يعرض في الشكل I-1 النموذج الأساسي لنظام المراسلة اللحظية.



الشكل I.1 – النموذج الأساسي لنظام المراسلة اللحظية

يتضمن النموذج الأساسي لنظام المراسلة اللحظية مخدم مراسلة لحظية والعديد من عملاء المراسلة اللحظية المتجانسين. ويستعمل المخدم IM لاستقبال وتمرير الرسائل اللحظية المرسلة من العملاء IM. وللعميل IM دوران: مرسل IM ومستلم IM. ويقوم المرسل IM بتمرير الرسائل اللحظية إلى المخدم IM لتوصيلها والذي يحاول بدوره توصيل الرسائل إلى المستلمين IM المتقابلين. وإذا قام مرسل IM بإرسال رسالة SPIM، فإنه ينظر إليه كمقتحم.

ويجب أن تستكمل وظائف النظام IM من خلال المخدم IM والعملاء IM والتفاعل بينهما.

وتشمل الوظائف الرئيسية للمخدم IM ما يلي:

- إدارة المستعملين، مثل تسجيل المستعملين وتسجيل دخول وخروج المستعملين وتحرير حسابات المستعملين؛
- إدارة الرسائل اللحظية، مثل إرسال الرسائل واستلامها ونقلها؛
- إدارة الأصدقاء، مثل البحث عن الأصدقاء وإدارة قائمة الأصدقاء؛
- إدارة النظام، مثل تشكيل المعلمات وتحديث النظام، بدء/إعادة/وقف تشغيل النظام.

وتشمل الوظائف الرئيسية للعميل IM ما يلي:

- إدارة المستعملين، مثل تسجيل المستعملين وتسجيل دخول وخروج المستعملين؛
- إدارة الرسائل اللحظية، مثل إرسال الرسائل واستلامها؛
- إدارة الأصدقاء، مثل إضافة أصدقاء، حذف أصدقاء، البحث عن أصدقاء؛
- إدارة العميل، مثل تشكيل المعلمات، وتحديث العميل، وبدء/إعادة/وقف تشغيل العميل.

بيبليوغرافيا

[b-ITU-T X.1231] Recommendation ITU-T X.1231 (2008), *Technical strategies for countering spam*.

[b-ITU-T X.1240] Recommendation ITU-T X.1240 (2008), *Technologies involved in countering e-mail spam*.

[b- ITU-T X.1244] Recommendation ITU-T X.1244 (2008), *Overall aspects of countering spam in IP-based multimedia applications*.

[b-IETF RFC 2778] IETF RFC 2778 (2000), *A Model for Presence and Instant Messaging*.

[b-IETF RFC 3428] IETF RFC 3428 (2002), *Session Initiation Protocol (SIP) Extension for Instant Messaging*.

سلاسل التوصيات الصادرة عن قطاع تقييس الاتصالات

السلسلة A	تنظيم العمل في قطاع تقييس الاتصالات
السلسلة D	مبادئ التعريفة والمحاسبة والقضايا الاقتصادية والسياساتية المتصلة بالاتصالات/تكنولوجيا المعلومات والاتصالات على الصعيد الدولي
السلسلة E	التشغيل العام للشبكة والخدمة الهاتفية وتشغيل الخدمات والعوامل البشرية
السلسلة F	خدمات الاتصالات غير الهاتفية
السلسلة G	أنظمة الإرسال ووسائطه والأنظمة والشبكات الرقمية
السلسلة H	الأنظمة السمعية المرئية والأنظمة متعددة الوسائط
السلسلة I	الشبكة الرقمية متكاملة الخدمات
السلسلة J	الشبكات الكبلية وإرسال إشارات تلفزيونية وبرامج صوتية وإشارات أخرى متعددة الوسائط
السلسلة K	الحماية من التداخلات
السلسلة L	البيئة وتكنولوجيا المعلومات والاتصالات، وتغير المناخ، والمخلفات الإلكترونية، وكفاءة استخدام الطاقة، وإنشاء الكبلات وغيرها من عناصر المنشآت الخارجية وتركيبها وحمايتها
السلسلة M	إدارة الاتصالات بما في ذلك شبكة إدارة الاتصالات وصيانة الشبكات
السلسلة N	الصيانة: الدارات الدولية لإرسال البرامج الإذاعية الصوتية والتلفزيونية
السلسلة O	مواصفات تجهيزات القياس
السلسلة P	نوعية الإرسال الهاتفي والمنشآت الهاتفية وشبكات الخطوط المحلية
السلسلة Q	التبديل والتشوير، والقياسات والاختبارات المرتبطة بهما
السلسلة R	الإرسال البرقي
السلسلة S	التجهيزات المطرافية للخدمات البرقية
السلسلة T	المطاريف الخاصة بالخدمات التليماتية
السلسلة U	التبديل البرقي
السلسلة V	اتصالات البيانات على الشبكة الهاتفية
السلسلة X	**شبكات البيانات والاتصالات بين الأنظمة المفتوحة ومسائل الأمن**
السلسلة Y	البنية التحتية العالمية للمعلومات، والجوانب الخاصة ببروتوكول الإنترنت وشبكات الجيل التالي وإنترنت الأشياء والمدن الذكية
السلسلة Z	اللغات والجوانب العامة للبرمجيات في أنظمة الاتصالات

طُبعت في سويسرا
جنيف، 2018