

# X.1247

## التعديل 1

(2022/05)

# ITU-T

قطاع تقييس الاتصالات  
في الاتحاد الدولي للاتصالات

السلسلة X: شبكات البيانات، والاتصالات  
بين الأنظمة المفتوحة ومسائل الأمن  
أمن الفضاء السيبراني - مكافحة الرسائل الاقتحامية

## الإطار التقني لمكافحة الرسائل الاقتحامية المتنقلة التعديل 1

التوصية ITU-T X.1247 (2016) - التعديل 1



توصيات السلسلة X الصادرة عن قطاع تقييس الاتصالات  
شبكات البيانات والاتصالات بين الأنظمة المفتوحة ومسائل الأمن

X.199-X.1	الشبكات العمومية للبيانات
X.299-X.200	التوصيل البيني للأنظمة المفتوحة
X.399-X.300	التشغيل البيني للشبكات
X.499-X.400	أنظمة معالجة الرسائل
X.599-X.500	الدليل
X.699-X.600	التشغيل البيني لأنظمة التوصيل OSI ومظاهر النظام
X.799-X.700	إدارة التوصيل البيني للأنظمة المفتوحة (OSI)
X.849-X.800	الأمن
X.899-X.850	تطبيقات التوصيل البيني للأنظمة المفتوحة (OSI)
X.999-X.900	المعالجة الموزعة المفتوحة
X.1029-X.1000	أمن المعلومات والشبكات
X.1049-X.1030	الجوانب العامة للأمن
X.1069-X.1050	أمن الشبكة
X.1099-X.1080	إدارة الأمن
X.1109-X.1100	الخصائص البيومترية
X.1119-X.1110	تطبيقات وخدمات آمنة (1)
X.1139-X.1120	أمن البث المتعدد
X.1149-X.1140	أمن الشبكة المحلية
X.1159-X.1150	أمن الخدمات المتنقلة
X.1169-X.1160	أمن الويب (1)
X.1179-X.1170	أمن التطبيقات
X.1199-X.1180	الأمن بين جهتين نظيرتين
X.1229-X.1200	أمن معرفات الهوية عبر الشبكات
<b>X.1249-X.1230</b>	<b>مكافحة الرسائل الاحتمالية</b>
X.1279-X.1250	أمن التلفزيون القائم على بروتوكول الإنترنت
X.1309-X.1300	أمن الفضاء السيبراني
X.1319-X.1310	إدارة الهوية
X.1339-X.1330	تطبيقات وخدمات آمنة (2)
X.1349-X.1340	اتصالات الطوارئ
X.1369-X.1350	أمن شبكات المحاسيس واسعة الانتشار
X.1399-X.1370	أمن الشبكة الكهربائية الذكية
X.1429-X.1400	البريد المعتمد
X.1459-X.1450	أمن إنترنت الأشياء (IoT)
X.1489-X.1470	أمن نظام النقل الذكي (ITS)
X.1519-X.1500	أمن تكنولوجيا سجل الحسابات الموزع (DLT)
X.1539-X.1520	أمن التطبيق (2)
X.1549-X.1540	أمن الويب (2)
X.1559-X.1550	تبادل معلومات الأمن السيبراني
X.1569-X.1560	نظرة عامة عن الأمن السيبراني
X.1579-X.1570	تبادل مواطن الضعف/الحالة
X.1589-X.1580	تبادل الأحداث/الأحداث العارضة/المعلومات الحديثة
X.1599-X.1590	تبادل السياسات
X.1601-X.1600	طلب المعلومات الحديثة والمعلومات الأخرى
X.1639-X.1602	تعرف الهوية والاكتشاف
X.1659-X.1640	التبادل المضمون
X.1679-X.1660	الدفاع السيبراني
X.1699-X.1680	أمن الحوسبة السحابية
X.1701-X.1700	نظرة عامة على أمن الحوسبة السحابية
X.1709-X.1702	تصميم أمن الحوسبة السحابية
X.1711-X.1710	أفضل الممارسات ومبادئ توجيهية بشأن أمن الحوسبة السحابية
X.1719-X.1712	تنفيذ أمن الحوسبة السحابية
X.1729-X.1720	أمن أشكال أخرى للحوسبة السحابية
X.1759-X.1750	الاتصالات الكمومية
X.1789-X.1770	المصطلحات
X.1819-X.1800	مولد الأرقام العشوائية الكمومي
	إطار أمن شبكات توزيع المفاتيح الكمومية
	التصميم الأمني لشبكات توزيع المفاتيح الكمومية
	التقنيات الأمنية لشبكات توزيع المفاتيح الكمومية
	أمن البيانات
	أمن البيانات الضخمة
	حماية البيانات
	أمن الاتصالات المتنقلة الدولية-2020

## الإطار التقني لمكافحة الرسائل الاقتحامية المتنقلة

### التعديل 1

#### ملخص

تنتشر بصورة هائلة الرسائل الاقتحامية المتنقلة جنباً إلى جنب مع التطور السريع لخدمات الرسائل المتنقلة. ولسوء الحظ، لم يثبت أي إجراء بمفرده أنه الوصفة السحرية لعلاج الرسائل الاقتحامية المتنقلة. وبالتالي، من الضروري وضع إطار عملي لمكافحة الرسائل الاقتحامية المتنقلة. وتقدم التوصية ITU-T X.1247 عرضاً مجملًا لعمليات مكافحة الرسائل الاقتحامية المتنقلة وتقتصر إطاراً تقنياً لمخاربتها. ويحدد هذا الإطار وظائف الكيانات وإجراءات المعالجة. وإلى جانب ذلك، توفر هذه التوصية آليات لتقاسم المعلومات المتعلقة بمكافحة المراسلة الاقتحامية المتنقلة داخل الميدان الواحد لمكافحة الاقتحام وفيما بين هذه الميادين.

ويقدم التعديل 1 آلية التغذية الراجعة من العميل الذي يتلقى مكالمة اقتحامية محتملة (بالصوت أو عبر خدمة الرسائل القصيرة (SMS) أو خدمة رسائل الوسائط المتعددة (MMS)) إلى المشغل الخاص به. ويقدم المتطلبات التقنية لأنظمة إدارة الاتصالات و/أو خدمات دعم العملاء لتلقي إشعارات بالمكالمات أو الرسائل (الرسائل القصيرة/رسائل الوسائط المتعددة) الاقتحامية الواردة. وتُعرض سيناريوهات التواصل التفاعلي بين العملاء ومشغلي/مقدمي خدمات شبكات الاتصالات الهاتفية بشأن المكالمات الاقتحامية الواردة والتدابير التقنية اللازمة للحفاظ على هذا التواصل التفاعلي. ويتمثل هذا التفاعل في قيام متلقي المكالمات الاقتحامية، بعد الانتهاء من المكالمات مباشرةً، بالاتصال برقم مكافحة الرسائل الاقتحامية الذي يوفره مشغل الاتصالات مقدماً.

#### التسلسل التاريخي

الطبعة	التوصية	تاريخ الموافقة	لجنة الدراسات	معرف الهوية الفريد*
1.0	ITU-T X.1247	2016-03-23	17	<a href="http://handle.itu.int/11.1002/1000/12600">11.1002/1000/12600</a>
1.1	ITU-T X.1247 (2016) Amd. 1	2022-05-20	17	<a href="http://handle.itu.int/11.1002/1000/14989">11.1002/1000/14989</a>

#### مصطلحات أساسية

مكافحة الرسائل الاقتحامية، الرسائل الاقتحامية المتنقلة، إطار تقني.

\* للنفاد إلى توصية، يرجى 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 الأمم المتحدة المتخصصة 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 والتعريف، 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 الكهروتقنية الدولية (IEC).

## ملاحظة

تستخدم كلمة "الإدارة" في هذه التوصية لتدل بصورة موجزة سواء على إدارة اتصالات أو على وكالة تشغيل معترف بها. والتقييد بهذه التوصية اختياري. غير أنها قد تضم بعض الأحكام الإلزامية (بهدف تأمين قابلية التشغيل البيئي والتطبيق مثلاً). ويعتبر التقييد بهذه التوصية حاصلاً عندما يتم التقييد بجميع هذه الأحكام الإلزامية. ويستخدم فعل "يلزم" وصيغ ملزمة أخرى مثل فعل "يجب" وصيغها النافية للتعبير عن متطلبات معينة، ولا يعني استعمال هذه الصيغ أن التقييد بهذه التوصية إلزامي.

## حقوق الملكية الفكرية

يستعري 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 اختراع/حقوق لتأليف ونشر البرمجيات 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 قواعد البيانات المناسبة لدى قطاع تقييس الاتصالات المتاحة في الموقع الإلكتروني للقطاع:

<http://www.itu.int/ITU-T/ipr/>

© ITU 2022

جميع الحقوق محفوظة. لا يجوز استنساخ أي جزء من هذه المنشورة بأي وسيلة كانت إلا بإذن خطي مسبق من الاتحاد الدولي للاتصالات.

## جدول المحتويات

### الصفحة

1	..... نطاق التطبيق	1
1	..... المراجع	2
1	..... التعاريف	3
1	..... 1.3 المصطلحات المعرّفة في مواضع أخرى	
2	..... 2.3 المصطلحات المعرّفة في هذه التوصية	
3	..... المختصرات والأسماء المختصرة	4
4	..... الاصطلاحات	5
4	..... لمحة عامة عن مكافحة الرسائل الاقترامية المتنقلة	6
6	..... هيكل وظائف مكافحة الرسائل الاقترامية المتنقلة	7
6	..... 1.7 الهيكل العام	
7	..... 2.7 نموذج مرجعي	
8	..... 3.7 وظائف المكونات	
9	..... 8 تكنولوجيا مكافحة الرسائل الاقترامية المتنقلة	
9	..... 1.8 آليات الإفادة من المستعمل	
10	..... 2.8 المصيدة	
10	..... 3.8 أسلوب تعرف الهوية من قبل مشغل شبكة متنقلة	
11	..... 4.8 تعزيز إضافي	
11	..... 9 العلاقة بين ميادين مكافحة الرسائل الاقترامية	
13	..... 10 المعالجة الخاصة بمكافحة الرسائل الاقترامية المتنقلة	
16	..... الملحق A – التدابير التفاعلية والتقنية لمكافحة المكالمات الاقترامية	
16	..... 1.A سيناريو/خوارزمية/حالة استعمال التغذية الراجعة التفاعلية	
17	..... 2.A المتطلبات التقنية	
18	..... بيبلوغرافيا	

تتطور الرسائل المتنقلة على نحو سريع جداً، بما في ذلك خدمة الرسائل القصيرة وخدمة الرسائل متعددة الوسائط، ويرجع ذلك إلى رخص ثمنها، وسهولة استخدامها، ومرونتها العالية. إلا أن الرسائل الاقترامية المتنقلة تحدث اضطرابات تؤثر في الحياة اليومية للعملاء ولها جوانب سلبية كثيرة.

ومن الصعوبة بمكان التخفيف من وطأة الرسائل الاقترامية المتنقلة على نحو فعال باللجوء إلى حل واحد فقط. وعند استخدام عدد من تكنولوجيات مكافحة الرسائل الاقترامية المتنقلة معاً، فإن الضرر الناجم عن الرسائل الاقترامية المتنقلة يمكن خفضه بشكل كبير. علاوة على ذلك، وبالنظر إلى أن الرسائل الاقترامية المتنقلة تنتشر حول العالم على نطاق واسع، فإن التعاون فيما بين ميادين مكافحة الرسائل الاقترامية المتعددة ربما يسفر عن تكلفة أقل كثيراً وكفاءة أعلى. لذا، فإنه من الضروري إرساء إطار مفتوح يستوعب حلولاً متنوعة ويدعم آليات التعاون. والإطار متواءم مع معظم تكنولوجيات مكافحة الرسائل الاقترامية وليس قاصراً على تفاصيل تقنية بعينها. وعلى الإجراءات المنضوية تحت هذا الإطار أن تطلب موافقة صريحة من المستعمل النهائي للجهاز المتنقل كما عليها أن تتواءم مع اللوائح والقوانين الوطنية.

## الإطار التقني لمكافحة الرسائل الاقترامية المتنقلة

### التعديل 1

ملاحظة صياغية: هذا منشور نص كامل. والتنقيحات المطروحة بهذا التعديل مبنية بعلامات المراجعة بالنسبة إلى التوصية ITU-T X.1247 (2016).

#### 1 نطاق التطبيق

تقدم هذه التوصية إطاراً تقنياً لمكافحة الرسائل الاقترامية المتنقلة. وفي هذا الإطار، تتحدد وظائف الكيانات وإجراءات المعالجة. وعلى الإجراءات المنضوية تحت هذا الإطار أن تطلب موافقة صريحة من المستعمل النهائي للجهاز المتنقل كما عليها أن تتماشى مع اللوائح والقوانين الوطنية. وإلى جانب ذلك، توفر هذه التوصية آليات لتقاسم المعلومات المتعلقة بمكافحة الرسائل الاقترامية المتنقلة داخل الميدان الواحد وفيما بين هذه الميادين.

وتنطبق هذه التوصية على خدمة الرسائل القصيرة (SMS) وخدمة الرسائل متعددة الوسائط (MMS).

#### 2 المراجع

تتضمن التوصيات التالية لقطاع تقييس الاتصالات وغيرها من المراجع أحكاماً تشكل من خلال الإشارة إليها في هذا النص جزءاً أساسياً من هذه التوصية. وقد كانت جميع الطباعات المذكورة سارية الصلاحية في وقت النشر. ولما كانت جميع التوصيات والمراجع الأخرى تخضع إلى المراجعة، يرجى من جميع المستعملين لهذه التوصية السعي إلى تطبيق أحدث طبعة للتوصيات والمراجع الأخرى الواردة أدناه. وتُنشر بانتظام قائمة توصيات قطاع تقييس الاتصالات السارية الصلاحية. والإشارة إلى وثيقة ما في هذه التوصية لا يضيفي على الوثيقة في حد ذاتها صفة التوصية.

[لا يوجد](#) [ITU-T X.1246] التوصية ITU-T X.1246 (2015)، التكنولوجيات المشاركة في مكافحة الرسائل الاقترامية الصوتية في منظمات الاتصالات.

#### 3 التعاريف

##### 1.3 المصطلحات المعروفة في مواضع أخرى

تستعمل هذه التوصية المصطلحات التالية المعرفة في مواضع أخرى:

**1.1.3 رقم مكافحة الرسائل الاقترامية (anti-spam number) [ITU-T X.1246]:** رقم هاتفي خاص يُحدد مسبقاً من جانب مقدم الخدمة المنزلية/الخاصة/مشغل الاتصالات (يمكن أن يكون هذا الرقم فريداً في البلد أو فردياً لكل مشغل)، يقوم من خلاله المستعمل بالإبلاغ عن تلقي مكالمات اقترامية إلى رقم هاتفه مباشرة قبل الاتصال برقم مكافحة الاقترام هذا. والإخطار هو واقع الاتصال برقم مكافحة الرسائل الاقترامية؛ وينبغي ألا يقدم المستعمل أي معلومات.

**2.1.3 تقرير المستعمل التفاعلي (interactive user report) [ITU-T X.1246]:** شكوى من مشترك يتلقى مكالمات إلى المطرف الهاتفي تحتوي على رسالة اقترامية أو تعتبر اقتراماً. وبشكل عام، يعد الإبلاغ بمثابة مكالمات (واقع الاتصال) إلى رقم مكافحة الرسائل الاقترامية أو إعادة توجيه مكالمات اقترامية مشبوهة مع رسالة إلى رقم مكافحة الرسائل الاقترامية.

**13.1.3 الرسائل الاقترامية لخدمة الرسائل القصيرة (SMS spam) [b-ITU-T X.1242]:** الرسالة الاقترامية التي ترسل عبر خدمة الرسائل القصيرة.

**24.1.3 الاقترام (spam) [b-ITU-T X.1240]:** يتوقف معنى كلمة "اقترام" على النظرة المحلية للخصوصية وعلى ما يمثله الاقترام من المنظور الوطني التكنولوجي 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 للاقترام، يُستعمل هذا المصطلح عموماً لوصف الرسائل الإلكترونية غير المطلوبة التي ترسل بالجملة عبر البريد الإلكتروني أو بواسطة خدمة المراسلة المتنقلة لأغراض الترويج التجاري للمنتجات أو الخدمات.

**5.1.3 مكالمة اقترامية (spam-call) [ITU-T X.1246]:** مكالمة هاتفية تتضمن رسالة صوتية أو نصية أو وسائط متعددة غير مرغوب فيها، الغرض منها، كقاعدة عامة، تسويق منتجات أو خدمات تجارية.

**36.1.3 المقتحم (spammer) [b-ITU-T X.1240]:** كيان أو شخص يُعدّ رسائل اقترامية ويرسلها.

**7.1.3 مكالمة اقترامية مشبوهة (suspicious spam call) [ITU-T X.1246]:** مكالمة هاتفية غير محددة يُشتبه في أنها غير مرغوب فيها.

## 2.3 المصطلحات المعروفة في هذه التوصية

تعرف هذه التوصية المصطلحات التالية:

**1.2.3 ميدان مكافحة الرسائل الاقترامية:** نظام مستقل يتضمن وظيفة لإدارة مكافحة الرسائل الاقترامية، ووظيفة لمراقبة مكافحتها، ووظيفة لمعالجة مكافحتها، وعمليات خدمة الرسائل المتنقلة.

ملاحظة - الوظائف في ميدان مكافحة الرسائل الاقترامية تخضع للإدارة الموحدة للمشغل.

**2.2.3 كيان ترشيح مكافحة الرسائل الاقترامية:** جهاز أو نظام يطبق تدابير مكافحة الرسائل الاقترامية لترشيح رسائل متنقلة طبقاً لقواعد ترشيح. ويستطيع منع الرسائل الاقترامية، أو يصنف الرسائل كمشبوهة، أو يرسلها إلى المستلم.

**3.2.3 وظائف إدارة مكافحة الرسائل الاقترامية:** مجموعة من الوظائف التي تطبق لإدارة ميدان مكافحة الرسائل الاقترامية والإشراف عليه، بما في ذلك التواصل مع ميادين مكافحة الرسائل الاقترامية الأخرى لتقاسم المعلومات بشأنها، وتوليد قواعد ترشيح جديدة ناتجة عن تحليل الرسائل الاقترامية وتوصيلها لوظائف المعالجة.

**4.2.3 وظائف مراقبة مكافحة الرسائل الاقترامية:** مجموعة من الوظائف التي تطبق لمراقبة ميدان معالجة مكافحة الرسائل الاقترامية وتحليل نتيجة ترشيحها، بما في ذلك التحقق من سلامة الرسالة الاقترامية المشبوهة التي وقعت في المصيدة، وتحليل بيانات الرسائل الاقترامية، وتوليد إحصائيات خاصة بها ونتائج تحليلها.

**5.2.3 وظائف معالجة مكافحة الرسائل الاقترامية:** مجموعة من الوظائف التي تطبق لمعالجة الرسائل المتنقلة مع قواعد الترشيح وسياساتها العامة. فهي تعالج الرسائل من خلال منع الرسائل الاقترامية، وإرسالها مع وسم خاص أو إرسال الرسائل إلى المستلم.

**6.2.3 سلمي خاطئ:** رسالة اقترامية متنقلة صنّفها نظام الترشيح خطأً بأنها غير اقترامية.

**7.2.3 إيجابي خاطئ:** رسالة صنّفها نظام الترشيح خطأً بأنها اقترامية.

**8.2.3 قواعد الترشيح:** مجموعة من القواعد الخاصة بخوارزميات مكافحة تنتشر بواسطة كيان ترشيح مكافحة الرسائل الاقترامية، مثل القوائم السوداء/القوائم البيضاء، وعتبات التشابه وعتبات إحصائية. وقد تتضمن قواعد الترشيح أيضاً قواعد ترشيح حددها المستعمل.

- 9.2.3** عميل خدمة الرسائل المتنقلة: المشترك في خدمة رسائل متنقلة.
- 10.2.3** الرسائل الاقتحامية المتنقلة: اتصالات إلكترونية غير مطلوبة من خلال خدمات الرسائل المتنقلة، تتكون عادة من رسالة اقتحامية لخدمة الرسائل القصيرة (SMS)، ورسالة اقتحامية لخدمة رسائل متعددة الوسائط (MMS).
- 11.2.3** رسالة اقتحامية لخدمة رسائل متعددة الوسائط (MMS): رسالة اقتحامية مرسله عبر خدمة الرسائل متعددة الوسائط.
- 12.2.3** خدمة الإبلاغ: خدمة توفر جمع وإجمال الإبلاغ عن الرسائل الاقتحامية للمشارك بموجب إذن المستعمل، واللوائح والقوانين الوطنية.
- 13.2.3** تقرير تحليل الرسائل الاقتحامية: تقدم النتيجة المحللة أداء نظام الترشيح. وينبغي أن تتضمن معدل ترشيح إيجابي/سلبي خاطئ، وخصائص الرسائل الاقتحامية، واتجاهاتها وغير ذلك من التحليلات.
- 14.2.3** إحصائيات الرسائل الاقتحامية: تمثل بيانات الرسائل الاقتحامية المجملة مدى الاقتحام بموجب شروط تقييد معينة، مثل الفاصل الزمني في ميدان ما لمكافحة الرسائل الاقتحامية. وينبغي للبيانات أن تشمل كمية الرسائل الاقتحامية داخل الميدان، والصادرة والواردة من الميادين، ونسبة الأنواع المختلفة من الاقتحام، وقائمة المفتاحين، وغير ذلك من البيانات الإحصائية الخاصة بالرسائل الاقتحامية.
- 15.2.3** الرسالة الاقتحامية المشبوهة: الرسالة المتنقلة غير المحددة التي يشبهه في كونها اقتحامية.
- 16.2.3** تقرير المستعمل: شكوى من مشترك استلم رسائل اقتحامية متنقلة. وعموماً، ربما يشتمل التقرير على وقت الرسائل الاقتحامية، ورقم الشبكة ISDN/PSTN الدولي لمشارك متنقل، وما إلى ذلك. ويشتمل هذا التقرير على معلومات عن الرسالة التي وسمت خطأً بأنها اقتحامية متنقلة، أو لم توسم مع أنه كان ينبغي وسمها باقتحامية، وبعبارة أخرى إيجابي خاطئ، سلبي خاطئ.

#### 4 المختصرات والأسماء المختصرة

تستعمل هذه التوصية المختصرات والأسماء المختصرة التالية:

AO	منشأة بتطبيق (Application Originated)
AMgmt	وظيفة إدارة مكافحة الرسائل الاقتحامية المتنقلة (Anti-spam Mobile messaging Management Function)
Amon	وظيفة مراقبة مكافحة الرسائل الاقتحامية المتنقلة (Anti-spam Mobile Messaging Monitoring Function)
Apr	وظيفة معالجة مكافحة الرسائل الاقتحامية المتنقلة (Anti-spam Mobile Messaging Processing Function)
Caller ID	تعرف هوية المتصل (Caller Identification)
CDR	سجل تفاصيل المكالمات (Call Detail Record)
CDR <sub>n</sub>	سجل تفاصيل المكالمات الأولية (initial Call Detail Record)
CDR <sub>n+1</sub>	سجل تفاصيل المكالمات التفاعلية من المستعمل إلى المشغل الخاص به (interactive Call Detail Record back from the user to its operator)
CLI	تعرف هوية الخط الطالب (Calling Line Identification)
CLI <sub>n</sub>	تعرف هوية خط طالب النداء الأولي إلى المستعمل (Calling Line Identification of initial caller to the user)
CLI <sub>n+1</sub>	تعرف هوية خط الطالب للمستعمل، عند إجراء مكالمات تغذية راجعة إلى رقم مكافحة الرسائل الاقتحامية (Calling Line Identification of the user, when it makes feedback call to an anti-spam number)

GPRS	الخدمة العامة للاتصالات الراديوية بأسلوب الرزم (General Packet Radio Service)
HPLMN	شبكة متنقلة برية عمومية محلية (Home Public Land Mobile Network)
HTTP	بروتوكول نقل نصوص ترابطية (HyperText Transfer Protocol)
ISDN	شبكة رقمية متكاملة الخدمات (Integrated Services Digital Network)
MAP	جزء خاص بالتطبيق المتنقل (Mobile Application Part)
MMS	خدمة الرسائل متعددة الوسائط (Multimedia Message Service)
MMSC	مركز خدمة الرسائل متعددة الوسائط (Multimedia Message Service Centre)
MNO	مشغل شبكة متنقلة (Mobile Network Operator)
MO	صادر عن نظام متنقل (Mobile Oriented)
MSC	مركز تبديل متنقل (Mobile Switching Centre)
MSISDN	رقم الشبكة ISDN/PSTN الدولي لمستخدم متنقل (Mobile Subscriber International ISDN/PSTN Number)
MT	موجه إلى نظام متنقل (Mobile Terminated)
PSTN	شبكة هاتفية عمومية تبديلية (Public Switched Telephone Network)
QoS	جودة الخدمة (Quality of Service)
SMPP	رسالة قصيرة بين الأقران (Short Message Peer-to-Peer)
SMS	خدمة الرسائل القصيرة (Short Message Service)
SMSC	مركز خدمة الرسائل القصيرة (Short Message Service Centre)
UICC	بطاقة الدوائر المتكاملة العالمية (Universal Integrated Circuit Card)
VPLMN	شبكة متنقلة برية عمومية مُزارة (Visited Public Land Mobile Network)
WAP	بروتوكول التطبيقات اللاسلكية (Wireless Application Protocol)

## 5 الاصطلاحات

لا يوجد.

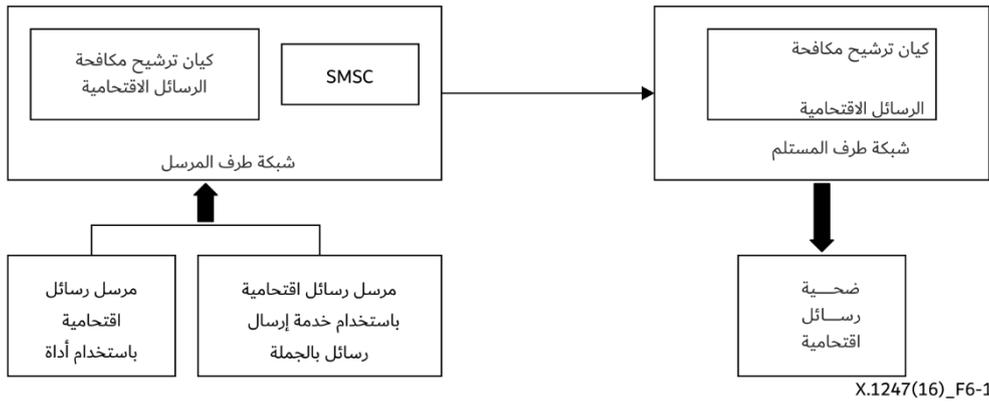
## 6 ملحة عامة عن مكافحة الرسائل الاقترامية المتنقلة

كما هو موضح في الشكل 6-1، يمكن أن تنشأ الرسالة الاقترامية في خدمة الرسائل القصيرة غالباً بطريقتين. تتمثل إحدى هاتين الطريقتين في أن المقتحم يستخدم أدوات اقتحام لإرسال رسائل بالجملة من خلال إرسال رسائل قصيرة عادية بطريقة من نقطة إلى نقطة، مع الكثير من بطاقات الدوائر المتكاملة العالمية المكتسبة (UICC) أو المكررة. والطريقة الأخرى تتمثل في أن المقتحمين يستغلون خدمات إرسال الرسائل بالجملة المطروحة من مقدمي الخدمة من خلال استخدام واجهات بوابة الرسائل القصيرة التابعة للمشغل. وحيث إن المشغلين ليس لديهم آليات إشراف إدارية وتقنية فعالة على واجهة بوابة الرسائل القصيرة، فإنه من السهولة يمكن استغلالها من قبل المقتحمين.

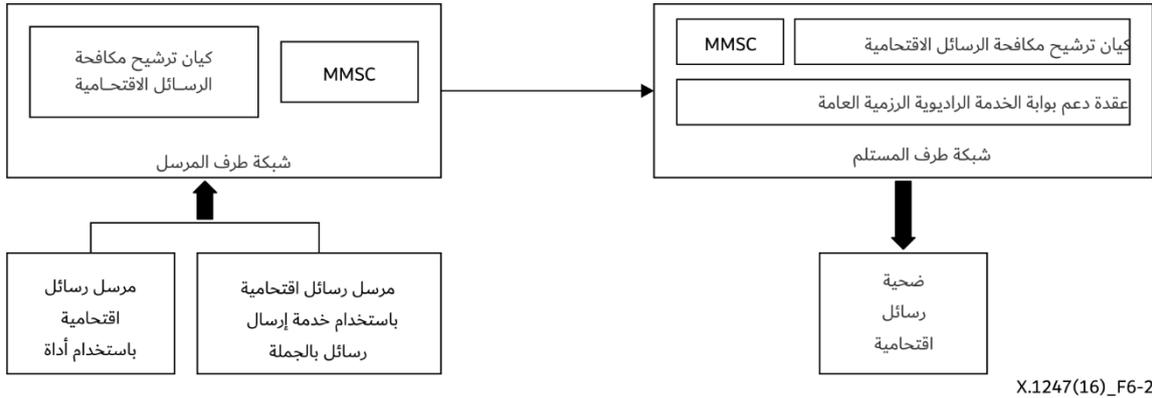
وطبقاً لآليات إعادة تسيير الرسائل، ثمة إجراءين أمام المقتحمين لإنشاء رسالة اقتحامية في خدمة الرسائل القصيرة، أحدهما يُعرف بالإجراء الصادر عن نظام متنقل أو التطبيقي المنشأ (MO/AO) والثاني بالإجراء الموجه إلى نظام متنقل (MT). في الإجراء MO تُرسل الرسالة الاقتحامية المتولدة من أدوات الاقتحام إلى مركز خدمة الرسائل القصيرة من خلال كيانات مرتبطة بشبكة المرسل. أما في الإجراء AO، فإن الرسالة القصيرة المدسوسة في الرسالة الاقتحامية من خلال بوابة الرسائل القصيرة التابعة للمشغل يتم إعادة تسييرها إلى مركز خدمة الرسائل القصيرة (SMSC). وبعد ذلك، يقوم مركز خدمة الرسائل القصيرة باستقصاء مركز خدمة التبديل المتنقل (MSC) الخاصة بالمستلم ثم يقوم بإعادة تسيير الرسالة إلى مركز خدمة التبديل هذا. وفي النهاية، يتم إعادة تسيير الرسالة إلى المستلم من خلال الشبكة الزائرة الخاصة بمركز التبديل المتنقل، وهو ما يطلق عليه اسم الإجراء الموجه إلى نظام متنقل.

ويأذن من المشترك واللوائح الإدارية، فإن مشغلي الشبكات المتنقلة (MNO) لهم السلطة في التخفيف من وطأة الرسائل الاقتحامية من خلال كيانات الترشيح. وينبغي أن تقتيد عملية مكافحة الرسائل الاقتحامية بمواد القوانين المطبقة بحيطه بُغية تحاشي انتهاك خصوصية المشتركين.

ومن المقبول به على نطاق واسع نشر كيانات ترشيح مكافحة الرسائل الاقتحامية إما بطريقة MO/AO أو بطريقة MT، أو بالطريقتين معاً. وفيما يخص ترشيح الرسائل الاقتحامية في الطريقة MO، تجمع كيانات الترشيح رسال قصيرة من مركز خدمة الرسائل القصيرة. ويلزم أيضاً توفر الاتصال بين مركز التبديل المتنقل (MSC) وكيان ترشيح الرسائل الاقتحامية بُغية تحقيق كفاءة الترشيح في شبكة المستلم.



الشكل 1-6 - الرسائل الاقتحامية في خدمة الرسائل القصيرة في شبكة متنقلة



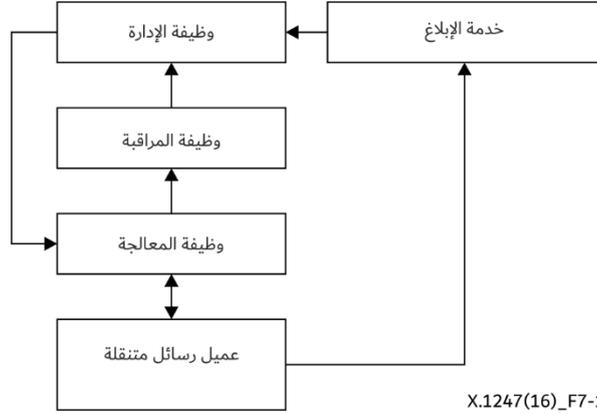
الشكل 2-6 - الرسائل الاقتحامية في خدمة الرسائل متعددة الوسائط في شبكة متنقلة

كما هو موضح في الشكل 6-2، فإن الإجراء المتعلق برسائل خدمة الرسائل متعددة الوسائط (MMS) مشابه لإجراء خدمة الرسائل القصيرة باستثناء الاستعاضة عن مركز التبديل المتنقل (MSC) بعقدة دعم بوابة الخدمة الراديوية الرزمية العامة (GGSN)، والاستعاضة عن مركز خدمة الرسائل القصيرة (SMSC) بمركز خدمة الرسائل متعددة الوسائط (MMSC). وسيتم إعادة تسيير الرسائل متعددة الوسائط إلى مركز خدمة الرسائل متعددة الوسائط الخاصة بشبكة المستلم والتي يقوم بعدها مركز خدمة الرسائل القصيرة بإرسال رسالة قصيرة إلى المستلم. وبعدها يقوم المستلم بتنزيل رسالة متعددة الوسائط من مركز خدمة الرسائل متعددة الوسائط. ولهذا السبب، يمكن نشر كيانات الترشيح الخاصة بمكافحة الرسائل الاحتمالية لخدمة الرسائل متعددة الوسائط يمكن نشرها بجوار مراكز خدمة الرسائل متعددة الوسائط، الأمر الذي يعني أنه إذا نُشرت كيانات الترشيح في جانب المرسل أو المستلم فإن هذا الأمر لن يحدث أي فرق.

## 7 هيكل وظائف مكافحة الرسائل الاحتمالية المتنقلة

يتضمن هيكل وظائف مكافحة الرسائل الاحتمالية المتنقلة وظيفة إدارة مكافحة الرسائل الاحتمالية المتنقلة (AMgmt)، ووظيفة مراقبة مكافحة الرسائل الاحتمالية المتنقلة (AMon)، ووظيفة معالجة مكافحة الرسائل الاحتمالية المتنقلة (APr) وعملاء المراسلة المتنقلة. وتحدد هذه الوظائف ميدان مكافحة الرسائل الاحتمالية المتنقلة. ويوصى بوجود ترابط بين مختلف ميادين مكافحة الرسائل الاحتمالية المتنقلة، إذ يمكنها أن تنسق فيما بينها طبقاً للسياسات العامة والقواعد التي تحددها الاتفاقيات ذات الصلة. وبوسع هذه الوظائف أن تتواصل فيما بينها من خلال بروتوكولات المراسلة القائمة وترد خصائصها على النحو التالي.

### 1.7 الهيكل العام



X.1247(16)\_F7-1

### الشكل 1-7-1- الهيكل العام

تتسلم وظيفة الإدارة (AMgmt) إحصائية بشأن الرسائل الاحتمالية من وظيفة المراقبة (AMon) فتحدّث الإدارة قواعد الترشيح في ميدانها. وتتشارك وظيفة الإدارة (AMgmt) أيضاً المعلومات بشأن الرسائل الاحتمالية مع خدمة الإبلاغ وغيرها من وظائف الإدارة.

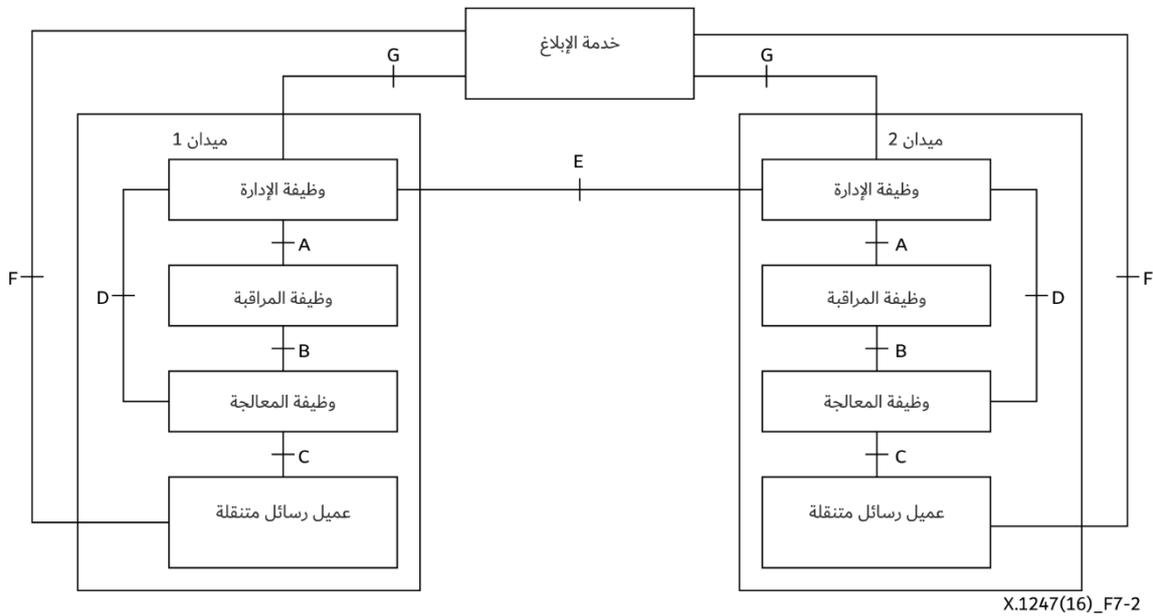
وتتسلم وظيفة المراقبة (AMon) من وظيفة المعالجة (APr) الرسائل الاحتمالية المتنقلة المشبوهة التي وقعت في حبال المصيدة أو حبال مثيلاتها، ثم تتحقق من كونها احتمالية أم لا. كما تبلغ وظيفة المراقبة (AMon) بشأن تحليل الرسالة الاحتمالية وإحصائياتها للإدارة (AMgmt) وذلك بعد إجمالها وتحليل بياناتها.

وتطبق وظيفة المعالجة (APr) القواعد على الرسائل المتنقلة، ثم تختار إما أن ترسلها مع وسمها بأنها اقتحامية، أو تمنعها كلية طبقاً لمختلف السياسات ونتائج الترشيح بموجب إذن من المستعمل. وتتسلم وظيفة المعالجة (APr) قواعد الترشيح من الإدارة والإفادات الواردة من المستعملين من عملاء خدمة الرسائل المتنقلة. ويوصى بنشر بعض المنصات مثل المصيدة على وظيفة المعالجة (APr) من أجل تجميع الرسائل الاقتحامية المشبوهة.

ويسهم عميل خدمة الرسائل المتنقلة في عملية مكافحة الرسائل الاقتحامية المتنقلة من خلال إرسال ما يعرف بإفادات المستعمل إلى وظيفة المعالجة (APr) تفيد بأن الرسالة المتنقلة المستلمة الموسومة بأنها اقتحامية غير صحيحة ويُعلم خدمة الإبلاغ.

والهدف من خدمة الإبلاغ هو جمع وإجمال التقارير بشأن الرسائل الاقتحامية من المشترك بموجب إذن من المستعمل واللوائح والقوانين الوطنية. وهي تساعد في تقاسم بيانات التقارير المقدمة من المستعمل بين ميادين مكافحة الرسائل الاقتحامية. ويمكن تشغيل خدمة الإبلاغ من خلال البيروقراطية التنظيمية أو شركات الأمن أو مشغلي الشبكات المتنقلة (MNO)، إلخ. وتُمكن الاتفاقيات فيما بين الميادين ميادين مكافحة الرسائل الاقتحامية المتنقلة من تقاسم معلومات مفصلة بشأن الرسائل الاقتحامية.

## 2.7 نموذج مرجعي



الشكل 7-2- نموذج مرجعي

الواجهة A هي واجهة منطقية بين وظيفة الإدارة (AMgmt) ووظيفة المراقبة (AMon). وتستخدم لنقل تقارير تحليلات الاقتحام وإحصائيات الاقتحام.

والواجهة B هي واجهة منطقية بين وظيفة المراقبة (AMon) ووظيفة المعالجة (APr). وتستخدم لنقل الرسالة الاقتحامية المشبوهة التي وقعت في حبال المصيدة وإفادة المستعمل بعدم صحة الرسالة المتنقلة المستلمة الموسومة بأنها اقتحامية من عميل خدمة الرسائل المتنقلة.

والواجهة C هي واجهة منطقية بين وظيفة المعالجة (APr) وعميل في خدمة الرسائل المتنقلة. ويستخدمها العميل لإعلام وظيفة المعالجة (APr) باستلام رسالة وسمها مشغل الشبكة المتنقلة (MNO) خطأً بأنها اقتحامية. وعلاوة على ذلك، تُستخدم الواجهة C أيضاً لإرسال رسائل من وظيفة المعالجة (APr) إلى عميل خدمة الرسائل المتنقلة. وطبقاً لأنواع المختلفة من عملاء خدمة الرسائل المتنقلة، ينبغي دعم بروتوكولات متنوعة في الواجهة C، مثل بروتوكول الجزء الخاص بالتطبيق المتنقل (MAP) وبروتوكول التطبيقات اللاسلكية (WAP) وبروتوكول نقل النصوص الترابطية (HTTP) وبروتوكول الرسائل القصيرة بين الأقران (SMPP).

والواجهة D هي واجهة منطقية بين وظيفة الإدارة (AMgmt) ووظيفة المعالجة (APr). وتستخدم في نقل قواعد الترشيح. والواجهة E هي واجهة منطقية بين وظائف الإدارة (AMgmt) مع الميادين الأخرى. وتستخدم في تبادل بيانات الرسائل الافتتاحية بين مختلف ميادين مكافحة الرسائل الافتتاحية المتنقلة.

والواجهة F هي واجهة منطقية بين عميل خدمة الرسائل المتنقلة وخدمة الإبلاغ. ويستخدمها عميل خدمة الرسائل المتنقلة لإرسال تقرير المستعمل لخدمة الإبلاغ مع موافقة صريحة من المستعمل. وينبغي دعم بروتوكولات متنوعة في الواجهة F مثل بروتوكول الجزء الخاص بالتطبيق المتنقل (MAP) وبروتوكول التطبيقات اللاسلكية (WAP) وبروتوكول نقل النصوص الترابطية (HTTP) وبروتوكول الرسائل القصيرة بين الأقران (SMPP).

والواجهة G هي واجهة منطقية بين وظيفة الإدارة (AMgmt) وخدمة الإبلاغ. وتستخدم في نقل معلومات الإبلاغ عن الرسائل الافتتاحية من خدمات الإبلاغ إلى وظيفة الإدارة (AMgmt).

وفي هذا النموذج المرجعي تكون الواجهات من A إلى D واجهات داخل الميادين، والواجهات من E إلى G واجهات بين الميادين.

### 3.7 وظائف المكونات

#### 1.3.7 عملاء خدمة الرسائل المتنقلة

تشمل وظائف عملاء خدمة الرسائل المتنقلة:

- تقديم آليات لمساعدة المستعملين على إرسال تقارير المستعملين إلى خدمة الإبلاغ.
- تقديم آليات لمساعدة المستعملين على إعلام وظيفة المعالجة (APr) باستلام رسائل وسمت خطأ بأنها افتتاحية.
- ترشيح الرسائل بقواعد ترشيح محددة باستخدام تطبيقات الأمان.

#### 2.3.7 وظيفة المعالجة (APr)

تشمل وظائف المعالجة:

- تطبيق قواعد مكافحة الرسائل الافتتاحية الواردة من وظيفة الإدارة (AMgmt) ثم تختار إما أن ترسلها، أو ترسلها مع وسمها بأنها افتتاحية، أو تمنعها كلية طبقاً لمختلف السياسات ونتائج الترشيح.
- استلام إفادات المستعمل من عميل خدمة الرسائل المتنقلة الذي يدعي أن الرسالة المتنقلة المستلمة، الموسومة بأنها افتتاحية ليست كذلك بالفعل.
- جمع الرسائل الافتتاحية المشبوهة من خلال المصائد أو غيرها من المنصات المشابهة.
- توصيل إفادة المستعمل فضلاً عن الرسالة الافتتاحية المشبوهة الواقعة في المصيدة إلى وظيفة المراقبة (AMon).

#### 3.3.7 وظيفة المراقبة AMon

تشمل وظائف المراقبة:

- إجمال الرسائل الافتتاحية المشبوهة المجموعة بمصيدة وظيفة المعالجة ومعلومات تقرير المستعمل الواردة من خدمة الإبلاغ.
- التثبت من الرسالة الافتتاحية المشبوهة الواردة من وظيفة المعالجة.
- تحليل بيانات الرسائل الافتتاحية المجمعة للتنقيب عن خصائص اقتحام جديد.
- إرسال تقارير بشأن إحصائيات الرسائل الافتتاحية وتحليلها إلى وظيفة الإدارة.

### 4.3.7 وظيفة الإدارة AMgmt

تشمل وظائف الإدارة:

- استقبال إحصائيات الرسائل الاقتحامية وتقرير التحليل من وظيفة المراقبة.
- تحليل البيانات المبلّغة من إدارة المراقبة لتوليد قواعد الترشيح.
- إرسال قواعد الترشيح إلى إدارة المعالجة، علماً بأن قواعد الترشيح ستطبق على عملاء خدمة الرسائل المتنقلة.
- التواصل مع وظائف الإدارات الأخرى لتبادل وتقاسم بيانات الرسائل الاقتحامية، مثل كميتها ومصادرها وخصائصها، وقائمة بالمقترحين الجدد، إلخ.
- استلام معلومات عن تقرير المستعمل من خدمة الإبلاغ، بما في ذلك المقترحين الأكثر إساءة، وإحصائيات الرسائل الاقتحامية واتجاهاتها. وقد تكون معلومات تقرير المستعمل مخصصة وتشمل بعض البيانات المعالجة من تقرير المستعمل طبقاً لاتفاق مع خدمة الإبلاغ في إطار ما تسمح به اللوائح والقوانين الوطنية.
- توفير القدرة على وضع قواعد ترشيح خاصة بالمستعمل مقدمة للمشارك، وإرسال القواعد إلى وظيفة المعالجة بعد التثبيت من صلاحيتها.

### 5.3.7 خدمة الإبلاغ

تشمل وظائف خدمة الإبلاغ:

- جمع تقارير المستعمل والتثبيت من كونها اقتحامية.
- تخزين الرسائل الاقتحامية وتحليلها لتوليد خصائص الرسائل الاقتحامية باستخدام البصمة بدلاً من المحتوى لتجنب انتهاك الخصوصية.
- تقديم بيانات تقرير المستعمل لتمكين مشغل الشبكة المتنقلة من القدرة على فهم مدى الرسائل الاقتحامية، الصادرة من شبكاتهم والواردة إليها من مشغلين آخرين، لاستخدام هذه الرؤية لاستهداف إجراءات الإنفاذ ضد الرسائل الاقتحامية فقط، دونما التأثير على المستعمل أو المحتوى.

## 8 تكنولوجيا مكافحة الرسائل الاقتحامية المتنقلة

تنطبق التكنولوجيات المقدمة في هذه الفقرة على هيكل مكافحة الرسائل الاقتحامية المذكور أعلاه وتقدم مثلاً. وينبغي أن تستعمل كل هذه التدابير بحرص للتماشي مع اللوائح والقوانين الوطنية المطبقة وبإذن من المستعمل. والقصد هو تحاشي انتهاك خصوصية المشترك.

### 1.8 آليات الإفادة من المستعمل

تمكن آليات الإفادة من المستعمل المشتركين من إبلاغ نظام الترشيح بأرائهم بشأن نتيجة ترشيح الرسائل الاقتحامية. ويوصى بتنفيذ خدمة الإبلاغ وإفادة المستعمل لتحسين نتيجة الترشيح الخاصة بمشغل الشبكة المتنقلة.

وخدمة الإبلاغ هي نظام لجمع تقارير المستعمل بشأن استلام رسائل اقتحامية، وقد تكون الخدمة منشأة من جانب الحكومة، أو المشغلين، إلخ. ومن الممكن أن تكون خدمة الإبلاغ خطأً ساخناً، أو موقعاً شبكياً، أو مركز رسائل قصيرة للإبلاغ عن الرسائل الاقتحامية؛ وبهذا يكون بمقدور مشغل الشبكة المتنقلة أن يجمع الرسائل الاقتحامية القصيرة ويعدل على أساسها قواعد الترشيح. وعموماً، فإن تسجيل شكوى مبلّغة بشأن رسائل اقتحامية قصيرة ينبغي أن يشمل جزئيات الرسالة الاقتحامية، ووقت الاستلام، وكذلك رقم الشبكة ISDN الدولي لمشارك متنقل والخاص بمرسل الرسالة، إلخ. وطبقاً للسياسات المختلفة، وفي حالة موافقة المستعمل، فإن المشغل لا يكتفي بالمنع فحسب بل يعرض أيضاً على مستلم الرسالة الاقتحامية النفاذ إلى الحجر، وهذا يعني أن هذه الرسائل من الممكن أن ترسل موسومة، أو تسجل في موقع محدد. ويسمح ذلك للمستلم برؤية هذه "الرسائل الاقتحامية المحتملة"، والتي وسمت

بأنها مشبوهة، ويمنحهم فرصة لتقديم إفادة إذا ما رأى المستعمل أن رسالة بعينها قد سمت خطأً أو "إيجابي خاطئ". ولا يمكن التعويل على كل إفادات المستعمل بمفردها. فقد يرتكب المستلم أخطاءً أو يكون لديه أسباب أخرى للإبلاغ عن رسالة ما بأنها اقتحامية. وتحتاج معلومات تعرف الرسائل الاقتحامية إلى التثبت منها يدوياً قبل استخدامها لتوليد البصمة أو قواعد الترشيح. ويمكن استحداث نظام تصنيف ثقة خاص بالمبلِّغ للثبوت أو توماتياً بشأن الإفادة الصحيحة مقابل الخاطئة أو الخبيثة.

## 2.8 المصيدة

مصيدة الرقم الهاتفي هي حساب ينشأ "كفخ" بغرض كشف أو تشتيت أو مجاهدة الاستخدام غير المسموح به للرسائل المتنقلة. ويشتمل عادةً على حساب يستخدم أو ينشأ ليكتشفه المقتحمون، بما في ذلك أرقام هواتف غير نشطة وحتى غير موجودة. وبهذه الطريقة فإن أي رسالة تختلف عما هو متوقع يمكن أن تعامل باعتبارها رسالة اقتحامية مشبوهة وقد يكون من المناسب تحليل المحتوى. ويخضع رقم الهاتف لإعادة تخصيص سريع كما تكتب أرقام الهواتف مراراً بشكل خاطئ، بحيث تستقبل المصيدة الهاتفية الكثير من الرسائل العارضة وغير الاقتحامية. والتحقق من هذه الرسائل الاقتحامية المشبوهة أمر ضروري لترشيح تلك البيانات غير المطلوبة قبل تحليل الرسائل الاقتحامية المشبوهة لمعرفة خصائصها.

وتعاني آلية إفادة المستعمل من التأخير الذي يتراوح من دقائق إلى أيام قبل أن يرفع المستلم تقريراً بشأن تلقيه رسالة غير مرغوبة. وعلى النقيض من ذلك، فإن فخاخ المصيدة قد تكشف رسائل غير مرغوبة بمجرد وصولها.

## 3.8 أسلوب تعرف الهوية من قبل مشغل شبكة متنقلة

باستثناء إفادة المستعمل والمصيدة، يستطيع مشغل الشبكة المتنقلة اتخاذ تدابير أخرى لتعرف الرسالة الاقتحامية قبل إرسالها للمستلم. وبسياسات مختلفة، تُمنع هذه الرسائل أو ترسل مع علامة خاصة بوصفها مشبوهة. وقد تعتمد أساليب التعرف تلك على خصائص الرسائل الاقتحامية أو نمط الإرسال.

- قائمة سوداء/قائمة بيضاء برقم الشبكة (ISDN/PSTN) للمرسل المشترك في الشبكة المتنقلة:

ورقم الشبكة ISDN الدولي لمشارك متنقل هي المعلومات الأساسية لتمييز رسالة من مشترك أو مقتحم. وتلجأ القوائم السوداء/القوائم البيضاء إلى استخدام رقم الشبكة ISDN الدولي للمرسل المتنقل لاتخاذ قرار بشأن تعليق أو قبول الرسائل. ويستطيع مشغلو الشبكات المتنقلة منع المقتحم المعروف أو الجديد، بينما يستطيع المشتركون تحديد القوائم البيضاء/القوائم السوداء الخاصة بهم لمنع أو قبول الرسائل من مرسلين محددين.

- التعرف الغائم:

يستخدم المقتحمون بعض أعمال التشويش بغية الهروب من عمليات ترشيح الرسائل الاقتحامية. على سبيل المثال، تدرج بعض الرموز الخاصة مثل "!", "h" إلخ إدراجاً تعسفياً في نص الرسائل. وتستبدل الحروف برموز مشابهاة، على سبيل المثال كلمة مثل كلمة "porn" ربما تُكتب هكذا "p0rn". والصور يجري تضخيمها أو تدويرها. والتعرف الغائم مسؤول عن التعرف على هذا التحايل وترشيحه حيثما كان مسموحاً.

- تكرار الإرسال:

لنشر الرسالة الاقتحامية على وجه السرعة، قد يرسل المقتحمون الرسائل إلى عدد كبير من المستلمين في وقت زمني قصير. ويرسل المقتحمون رسائلهم بسرعة أعلى بكثير مما هو معتاد، وبذا فإن الفاصل الزمني بين رسالتين يكون أقصر. وعندما يتجاوز معدل تكرار الإرسال من مستعمل ما عتبة الإرسال، يحدد المستعمل بوصفه مفتحماً مشبوهاً إلى حد كبير.

- معدل النجاح في إرسال الرسائل:

ترسل الرسائل الاقتحامية إلى مستلم مجهول، ولهذا السبب يختار المقتحم المستلم بشكل عشوائي. ولذا فمن الشائع أن تكون بعض الأرقام المطلوبة غير موجودة بالمرّة. ومعدل النجاح في إرسال الرسائل الاقتحامية أقل بشكل ملحوظ مما هو عليه في الرسائل المتنقلة العادية.

• سجل نداءات المرسل:

سجل نداءات المرسل يمكنه أن يساعد المشغل في تحليل نمط الإرسال ويجب أن يشمل السجل على الأقل رقم هاتف المرسل، ورقم هاتف المستلم، ووقت الإرسال. فإذا ما أرسلت الرسالة إلى مشتركين أكثر، وكانت ذات معدل منخفض من الاستجابة أو الرد، فإن الشكوك تثار حول كون المرسل مقترحاً. ونادراً ما يستخدم المقترحون الخدمات الأخرى (مثل المكالمات الصوتية) التي يقدمها المشغل بخلاف خدمة الرسائل.

#### 4.8 تعزيز إضافي

• تهيئة قواعد خاصة بالمستعمل:

إن آلية تهيئة قواعد بالمستعمل تمكن المستلمين من التعرف وإبلاغ نظام الترشيح بنوع الرسائل التي لا يرغب المستلم في تلقيها. وترشيح الرسائل طبقاً لقواعد خاصة بالمستعمل يمكن أن ينجزه مشغل الشبكة المتنقلة أو باستخدام برنامج مركب في معدات المستلم.

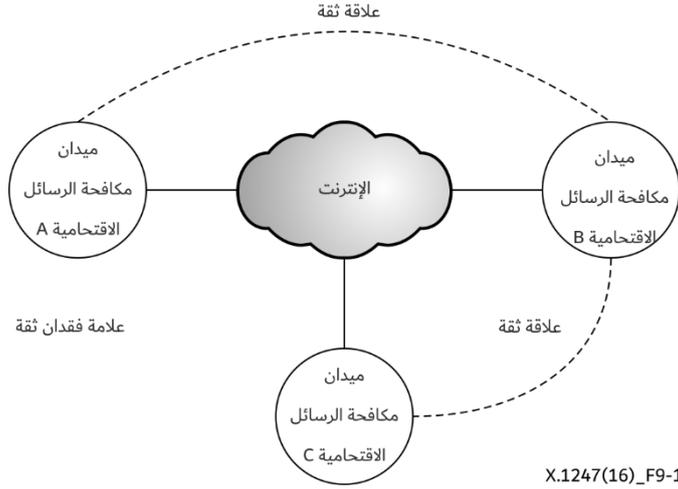
• التسيير العائد إلى الشبكة المتنقلة البرية العمومية المحلية (HPLMN) الخاصة بالمستلم:

قد يطبق المشغلون عمليات مختلفة لمكافحة الرسائل الاحتمالية بالنسبة لأولئك العملاء المتجولين خارج الشبكة المتنقلة البرية العمومية المحلية (HPLMN). وعملية إعادة التسيير إلى الشبكة HPLMN أمر اختياري، لذا فقد يحدث أن يتسلم مستلم التجوال رسالة بدون ترشيح للرسائل الاحتمالية. وهكذا فإن الرسائل المرسله لعملاء التجوال لا بد أن تخضع لإعادة تسيير إلى كيانات الترشيح الخاصة بمكافحة الرسائل الاحتمالية في الشبكة (HPLMN) بدلاً من الاعتماد على الشبكة المزارة. وقبل الوصول إلى شبكة متنقلة برية عمومية مزارة (VPLMN)، تحتاج الشبكة HPLMN الخاصة بالمستلم إلى استلام وترشيح الرسائل بتدابير مكافحة الرسائل الاحتمالية ذات الصلة.

### 9 العلاقة بين ميادين مكافحة الرسائل الاحتمالية

يتميز أداء تدابير مكافحة الرسائل الاحتمالية في ميدان وحيد لمكافحة الرسائل الاحتمالية بأنه محدود تقنياً واقتصادياً. وثمة حاجة للاتصال والعمل فيما بين مشغلي الشبكات المتنقلة، كما أن آليات التعاون بين ميادينهم لمكافحة الرسائل الاحتمالية أمر حيوي. إذ تستطيع آليات التعاون المساعدة في تحسين الكفاءة وتعزيز أداء نظم مكافحة الرسائل الاحتمالية.

وثمة نوعين من العلاقة بين ميادين مكافحة الرسائل الاحتمالية، وهما علاقة الثقة وعلاقة فقدان الثقة (الشكل 9-1). وينبغي أن تكون العلاقة الافتراضية بين ميادين مكافحة الرسائل الاحتمالية علاقة فقدان الثقة، إذ يتم ترشيح كل الرسائل من الأقران غير الموثوقين. وبموجب الاتفاقيات التعاونية يمكن بناء علاقة الثقة بين ميادين مكافحة الرسائل الاحتمالية التابعة للأقران؛ ولأجل هذه العلاقة، ربما يختار المشغلون ألا يرشحوا رسائلهم الواردة من أقران موثوقين استناداً إلى سياساتهم العامة وقواعد الترشيح.



### الشكل 9-1- علاقة الثقة وعلاقة فقدان الثقة

وعلاقة الثقة غير متعدية. فعلى سبيل المثال، إذا كان الميدان ألف يثق بالميدان باء، والميدان باء يثق بالميدان جيم، فإن الميدان ألف ربما لن يثق بالميدان جيم إلا إذا تفاوضا مباشرة وأقاما علاقة ثقة. وعلاقة الثقة هي علاقة ثنائية الاتجاه، ما يعني أن الأقران الذين يثقون ببعضهم البعض يعاملون بعضهم على قدم المساواة.

وبعد إرساء علاقة الثقة، يوصى بآليات التنسيق التالية.

- تقاسم بيانات الرسائل الاحتمالية:

يجري تقاسم بيانات الرسائل الاحتمالية من خلال ربط وظائف الإدارة. وقد تشمل المعلومات القوائم السوداء، والكلمات المفتاحية، والتقارير، وخصائص الرسائل الاحتمالية الجديدة. والقصد من هذه المعلومات سيتم التشاور بشأنه خلال عملية إرساء علاقة الثقة. وينبغي أن يُمنح اقتسام بيانات الرسائل الاحتمالية الموافقة صراحةً من المستعمل النهائي للجهاز المتنقل ويجب أن يتواءم مع اللوائح والقوانين الوطنية.

- الاستيقان من مصدر الرسالة:

تعتبر الرسالة الواردة من قرين موثوق به متحقق منها إذا كان مصدر الرسالة مصدق عليه.

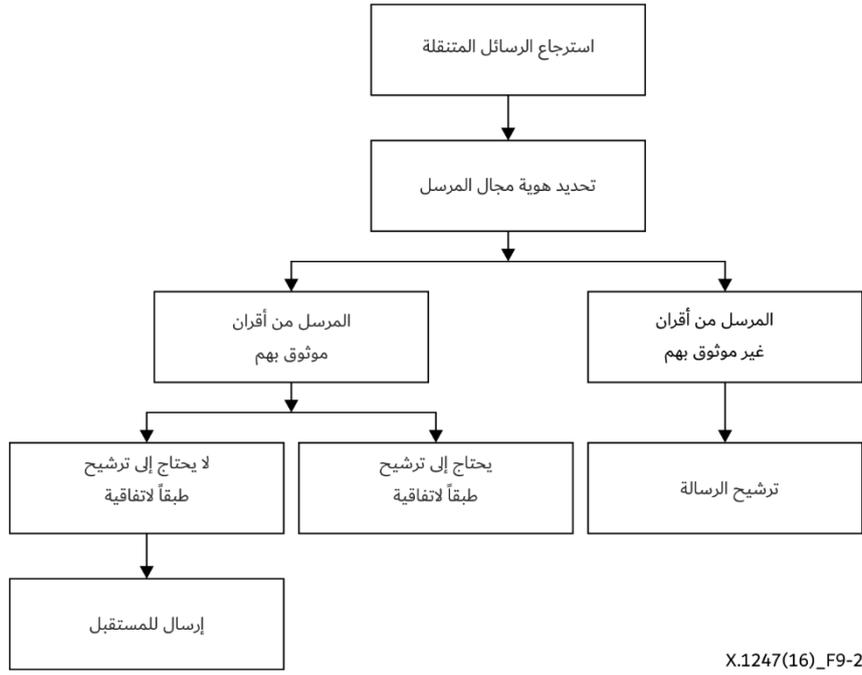
- الاستغناء عن الترشيح:

الرسائل الواردة من ميدان موثوق به يمكن أن ترسل مباشرة إلى المستلم وبذا نتحاشى تكرار معالجة الرسالة.

- تقرير شكوى المستعمل والإفادة عن رسالة احتمالية مشبوهة:

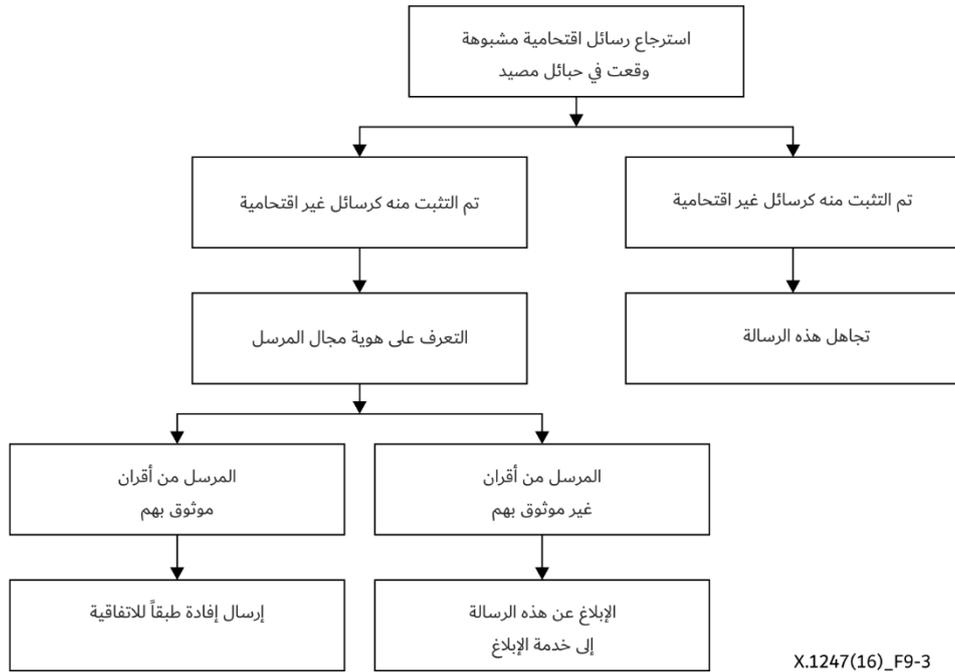
لو وصلت تقارير الرسائل الاحتمالية والرسائل المشبوهة على رسائل من أقران موثوق بهم، فإنه يجب إرسالها للقرين الموثوق به من أجل تحسين قواعد الترشيح لديه بموجب اللوائح المطبقة والقوانين الوطنية.

وتلبية لآليات التنسيق المختلفة، ينبغي على وظيفتي المعالجة والمراقبة تنفيذ إجراءات مختلفة عند التعامل مع الرسائل المتنقلة. وسوف تقرر وظيفة المعالجة ما إذا كانت سترشح الرسالة أم لا. وطبقاً للاتفاق، ستقوم وظيفة المراقبة بإعادة توجيه/منع الرسالة، أو إرسال إفادة إلى القرين الموثوق. ويصف الشكلان 9-2 و 9-3 سياق العمليات في وظيفتي المعالجة والمراقبة.



X.1247(16)\_F9-2

الشكل 9-2- سياق التعامل مع الرسائل المتنقلة في وظيفة المعالجة

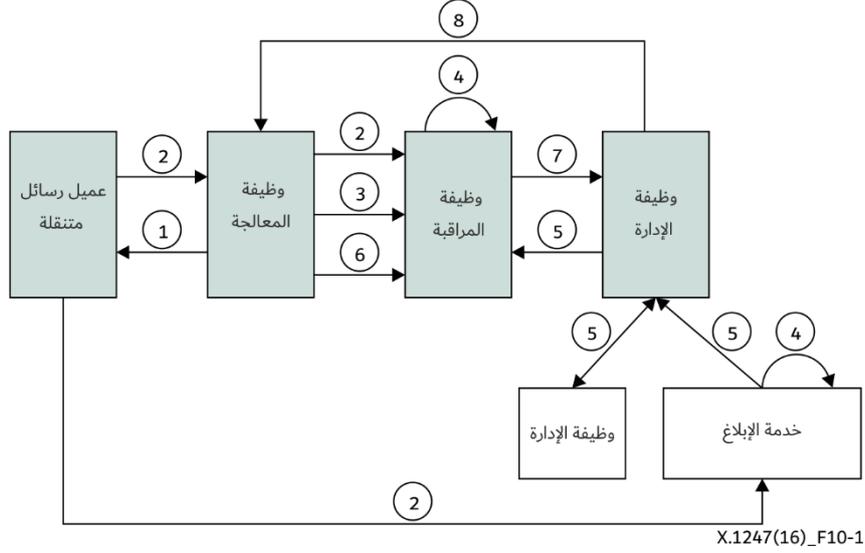


X.1247(16)\_F9-3

الشكل 9-3- سياق التعامل مع الرسائل المتنقلة في وظيفة المراقبة

## 10 المعالجة الخاصة بمكافحة الرسائل الاقتمانية المتنقلة

في المعالجة الخاصة بمكافحة الرسائل الاقتمانية المتنقلة، يجب تقديم آلية تكييفية لاستيعاب الرسائل الاقتمانية الجديدة الناشئة باستمرار وتنويعاتها الجديدة. وعموماً، يمكن اعتبار أن عملية مكافحة الرسائل الاقتمانية تشكل من ثمانية إجراءات كما هو موضح في الشكل 10-1. وتشكل هذه الإجراءات نظاماً تكييفياً يسهم في تعظيم أداء النظام.



الشكل 10-1- إجراءات المعالجة الخاصة بمكافحة الرسائل الاحتمالية

### الإجراء 1: ترشيح الرسالة

استناداً إلى السياسات العامة وقواعد الترشيح، تقوم وظيفة المعالجة بشكل خاص بوسم أو ترشيح الرسائل الاحتمالية قبل أن ترسلها إلى المستلم. وقواعد الترشيح هذه يمكن أن يسنها المشغل أو تكون حسب تخصيص المستعمل.

### الإجراء 2: إرسال المستعمل للإفادة

يرسل عميل خدمة الرسائل المتنقلة شكوى المستعمل لخدمة الإبلاغ للإبلاغ بشأن الرسائل الاحتمالية غير المرشحة، فضلاً عن إفادات المستعمل إلى وظيفة المراقبة للإعراب عن استلام رسائل موسومة خطأ بأنها احتمالية. وهذا سوف يساعد المشغلين في تحسين قواعد الترشيح لديهم.

### الإجراء 3: إعادة توجيه الرسالة الاحتمالية المشبوهة

سوف ترسل وظيفة المعالجة الرسالة الاحتمالية المشبوهة التي جمعتها المصدرة إلى وظيفة المراقبة للثبوت منها.

### الإجراء 4: الثبوت من الرسالة الاحتمالية

تعالج وظيفة المراقبة الرسالة الاحتمالية المشبوهة من خلال الثبوت وخدمات الإبلاغ التي تتعامل مع تقارير المستعمل بشأن الاحتمال. وهذا الإجراء معقد ويستند إلى تدخل يدوي، يتمشى مع اللوائح المطبقة والقوانين الوطنية. وينبغي للثبوت أن يستخدم البصمة أو البيانات المجزأة للاقتحام بدلاً من استخدام محتوى الرسالة. وقد تكون بعض المعلومات مفيدة لاتخاذ هذا الحكم، مثل سمعة المقتحمين والمبلغين والتي تعطي تصنيف ثقة للمستعمل المتقدم بالإبلاغ.

### الإجراء 5: تقاسم المعلومات

تبادل وظيفة الإدارة البيانات مع الأقران الموثوق بهم، كما تقوم باستلام تحليلات الاقتحام المخصصة من خدمة الإبلاغ. واتساقاً مع توافق الآراء في التفاوض، قد تتضمن البيانات إحصائيات خاصة بتقرير المستعمل، وقائمة المقتحمين، والإفادة عن الشكوى، والخصائص الجديدة للرسائل الاحتمالية. وينبغي معالجة بيانات الرسائل الاحتمالية تلك بعناية للتأكد من أنه ليس هناك محتوى خاص بالمستعمل.

## الإجراء 6: مراقبة أداء النظام

تعتبر وظيفة المراقبة مسؤولة أيضاً عن مراقبة الأداء الخاص بنظام ترشيح الرسائل الاقتحامية. وتجمع وظيفة المراقبة البيانات من وظيفة المعالجة لتوليد تقارير الأداء وتحليلها. وقد يحتوي تقرير الأداء على أرقام بشأن الأداء في الوقت الفعلي ونسبة الرسائل الاقتحامية والمعدل السلبي الخاطئ، إلخ.

## الإجراء 7: تحليل الرسائل الاقتحامية

يتم تجميع وتخزين بيانات الرسائل الاقتحامية المؤكدة الواردة من خدمة الإبلاغ والأقران الموثوقين ووظيفة المراقبة، مع مراعاة اللوائح والقوانين المحلية. وقد تقوم وظيفة المراقبة بشكل دوري بتحليل هذه البيانات وتنقيتها للكشف عن الأنماط والخصائص الجديدة للرسائل الاقتحامية. وسوف يساعد هذا في تحسين قواعد الترشيح وأداء النظام. وأخيراً سوف يستخدم لتوليد إحصائيات الرسائل الاقتحامية وتقارير تحليل الرسائل الاقتحامية التي سوف تنقل إلى وظيفة الإدارة.

## الإجراء 8: ضبط تدابير المجابهة

طبقاً لإحصائيات الرسائل الاقتحامية وتقرير التحليل الواردة من وظيفة المراقبة، تقوم وظيفة الإدارة بتقييم أداء مكافحة الرسائل الاقتحامية الخاص بنظام ترشيح هذه الرسائل بهدف تقديم تحسينات محتملة. واستناداً إلى نتيجة التقييم، قد يتم تعديل التدابير والسياسات وتغيير آليات التعاون مع الميادين الأخرى. وسيتم تنفيذ التدابير ذات الصلة مثل إنشاء أو إنهاء علاقة ثقة وتوزيع سياسات وقواعد ترشيح جديدة على وظائف المعالجة.

## الملحق A

### التدابير التفاعلية والتقنية لمكافحة المكالمات الاقترامية

(يشكل هذا الملحق جزءاً أساسياً من هذه التوصية.)

#### ملخص

يقدم هذا الملحق لمحة عامة عن العمليات الرامية إلى مكافحة المكالمات الاقترامية ويقترح أساساً تقنياً لمكافحة مثل هذه المكالمات استناداً إلى المكالمات الموجهة إلى الأرقام (لا سيما الأرقام التي يوزعها مشغل الاتصالات) بعد تلقي مكالمة اقترامية واردة مباشرة. وفي هذا الإطار، يتعين أن يكون للمشغل (أو المشغلين) رقم خاص (أو أرقام خاصة) لمكافحة الرسائل الاقترامية ومختلف مستويات وظائف معالجة سجل تفاصيل المكالمة لهذه الأرقام. وبالإضافة إلى ذلك، يوفر هذا الملحق آليات لتبادل المعلومات من أجل مكافحة الرسائل الاقترامية في إطار التفاعل بين المشغلين.

ويوفر هذا الملحق الأساس التقني لمكافحة الرسائل الاقترامية عندما يقوم المشترك بإخطار المشغل بواسطة مكالمة قصيرة إلى رقم مكافحة الرسائل الاقترامية بعد تلقي المكالمة الاقترامية مباشرة. وينطبق هذا الملحق على خدمة المكالمات الصوتية وخدمة الرسائل القصيرة (SMS) وخدمة الرسائل متعددة الوسائط (MMS).

#### سيناريو خدمة الإبلاغ التفاعلية للتفاعل بين المشترك ومشغل الاتصالات/مقدم الخدمة من أجل مكافحة المكالمات الاقترامية إلى المطاريف الهاتفية

تعرف التوصية ITU-T X.1247 بمفهوم آليات التغذية الراجعة للمستعمل وتقرير المستعمل المستخدمة في معالجة الرسائل الاقترامية. وتعرف التوصية [ITU-T X.1246] بآليات تفاعلية مختلفة للتحقق من الرسائل الاقترامية ومعالجتها.

وتكتمل آلية تفاعلية موصوفة هنا الإجراءات الحالية الواردة في متن هذه التوصية [ITU-T X.1246] والتوصية (ITU-T X.1247) وتوسّعها. ويتمثل التفاعل المقترح بين المشترك/متلقي المكالمة الاقترامية مع مشغل الاتصالات/مقدم الخدمة في قيام المشترك بمكالمة قصيرة إلى رقم محدد لمكافحة الرسائل الاقترامية لدى مشغل الاتصالات/مقدم الخدمة أو إعادة توجيه الرسالة الاقترامية المستلمة إلى هذا الرقم.

#### 1.A سيناريو/خوارزمية/حالة استعمال التغذية الراجعة التفاعلية

يشمل سيناريو استخدام طلب رقم مكافحة الرسائل الاقترامية من أجل تحديد مكالمة اقترامية باستخدام المعالجة الأوتوماتية للتفاصيل CDR/CLI، الخطوات التالية:

- 1 يستلم المتلقي/العميل/المشترك مكالمة واردة، يحددها على أنها مكالمة اقترامية أو مكالمة مشبوهة (رسائل صوتية اقترامية، رسائل اقترامية في خدمة الرسائل القصيرة أو رسائل اقترامية في خدمة الرسائل متعددة الوسائط).
- 2 تُخزن المعلومات CDR/CLI بشأن هذه المكالمة (وكذلك بشأن أي مكالمة أخرى) في نظام إدارة الاتصالات (أو في أي نظام آخر/أنظمة أخرى) الخاص بـمشغل الاتصالات. وتحتوي المعلومات CDR<sub>n</sub>/CLI<sub>n</sub> هذه على معرف هوية المتصل (المصدر المحتمل للمكالمة الاقترامية)، ومعرف هوية متلقي المكالمة (مستلم المكالمة الاقترامية) ووقت المكالمة.
- 3 بعد الانتهاء من هذه المكالمة مباشرة/بأسرع ما يمكن، يقوم المتلقي/العميل/المشترك بطلب رقم مكافحة الرسائل الاقترامية الخاص الذي يحدده مسبقاً مقدم الخدمة/مشغل الاتصالات الخاص به (وفقاً للوائح الوطنية، يمكن أن يكون هذا الرقم فريداً في البلد أو فردياً لكل مشغل)، أي أنه يجري مكالمة صادرة إلى رقم مكافحة الرسائل الاقترامية كإفادة تفاعلية للمستعمل.

- 4 تُخزن أيضاً المعلومات  $CDR_{n+1}/CLI_{n+1}$  المتعلقة بهذه المكالمات في نظام إدارة الاتصالات الخاص بالمشغل.
- 5 يقوم المشغل الذي يتلقى من المشترك مثل هذه المكالمات إلى رقم مكافحة الرسائل الاقتحامية بالتقاط جميع المعلومات التقنية  $CDR_{n+1}$  ( $CDR$  و  $CLI$  بدرجات متفاوتة من التفاصيل)، ويعثر تلقائياً على المكالمات ما قبل الأخيرة التي وردت إلى المشترك/المستلم لمكالمة اقتحامية محتملة، ويبدأ بجمع معلومات عن الطرف الطالب المحتمل المسؤول عن الرسالة الاقتحامية (وربما يتبادل هذه المعلومات مع مشغلين/منظمين).
- 6 إذا كانت المكالمات إلى رقم مكافحة الرسائل الاقتحامية فريدة و/أو خاطئة، قد لا تكون هناك حاجة إلى مزيد من الخطوات.
- 7 وإذا كان هناك عدة مكالمات موجهة إلى رقم مكافحة الرسائل الاقتحامية، من العديد من المتلقين للمكالمات الاقتحامية المحتملة، وحدد نظام المعالجة  $CDR$ ، في كل حالة، نفس الرقم طالب النداء أو المعلومات  $CLI_n$  لآخر مكالمة واردة إلى المشترك/المستعمل قبل مكالمته الموجهة إلى رقم مكافحة الرسائل الاقتحامية، سيزيد احتمال كشف المصدر الحقيقي للمكالمات الاقتحامية للمساعدة في العثور على المقتحمين.
- 8 من الممكن اختيارياً تحديد عتبات مختلفة لأنظمة المعالجة  $CDR$  للقضاء على الإنذارات الزائفة.

## 2.A المتطلبات التقنية

- 1.2.A يُتطلب أن يكون لدى مشغل الاتصالات/مقدم الخدمة رقم خاص لمكافحة الرسائل الاقتحامية لاستلام مكالمات التغذية الراجعة من الجهة المتلقية لهذه المكالمات.
- 2.2.A لمعالجة العدد الكبير من مكالمات التغذية الراجعة، يُتطلب أن يكون لمشغل الاتصالات/مقدم الخدمة إمكانية استقبال ومعالجة هذه المكالمات بشكل كامل بالاستناد إلى كل من تفاصيل  $CDR$  وتفاصيل  $CLI$  بدرجة أقل.
- 3.2.A يُتطلب أن يضمن نظام إدارة الاتصالات جودة البيانات الإحصائية لخدمة الإبلاغ.

## بييليوغرافيا

- [b-ITU-T X.1240] التوصية ITU-T X.1240 (2008)، التكنولوجيا المشاركة في مكافحة الرسائل الاقترامية المصاحبة للبريد الإلكتروني.
- [b-ITU-T X.1242] التوصية ITU-T X.1242 (2009)، نظام ترشيح الرسائل الاقترامية في خدمة الرسائل القصيرة استناداً إلى قواعد يحددها المستعمل.
- [b-M3AAWG report] التقرير M3AAWG، أفضل الممارسات لمقدمي الخدمات في خدمة الرسائل المتنقلة، تم تحديثه في أغسطس 2015.
- <https://www.m3aawg.org/sites/default/files/M3AAWG-Mobile-Messaging-Best-Practices-Service-Providers-2015-08.pdf>



## سلاسل التوصيات الصادرة عن قطاع تقييس الاتصالات

السلسلة A	تنظيم العمل في قطاع تقييس الاتصالات
السلسلة D	مبادئ التعريف 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	المطاريق 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 بروتوكول الإنترنت وشبكات الجيل التالي وإنترنت الأشياء والمدن الذكية
السلسلة Z	اللغات والجوانب العامة للبرمجيات في أنظمة الاتصالات