

X.1246

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 السبراني - مكافحة الرسائل الاقتحامية

التكنولوجيات المشاركة في مكافحة الرسائل
الاقتحامية الصوتية في منظمات الاتصالات
التعديل 1

التوصية ITU-T X.1246 (2015) - 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 الأمن (1)
X.1199-X.1180	الأمن بين جهتين نظيرتين
X.1229-X.1200	أمن معرفات الهوية عبر الشبكات
X.1249-X.1230	مكافحة الرسائل الاحتمالية
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

التكنولوجيا المشاركة في مكافحة الرسائل الاقترامية الصوتية في منظمات الاتصالات

التعديل 1

ملخص

الاتصالات الصوتية خدمة أساسية تقدمها شبكات الاتصالات. ومع تطور الاتصالات الصوتية، تزايدت أيضاً الرسائل الاقترامية الصوتية وما يترتب عليها من آثار سلبية متعددة على المستخدمين النهائيين ومشغلي الشبكات. وتشمل الرسائل الاقترامية الصوتية بصورة عامة محتوى يتراوح بين الإعلانات التجارية والمواد الإباحية المسيئة التي تؤدي إلى آثار سلبية مختلفة على المستخدمين النهائيين ومشغلي الشبكات. ويمكن أن تسبب الرسائل الاقترامية الصوتية في إغواء أو إزعاج أو مضايقة أو حتى تخويف المستخدمين فضلاً عن التأثير سلباً في موارد الشبكة. ولتفادي هذه التأثيرات السلبية وحماية حقوق المستعمل والحفاظ على استقرار الشبكة، قد يرغب المشغلون في زيادة جهودهم الرامية إلى مكافحة الرسائل الاقترامية الصوتية.

والغرض من التوصية ITU-T X.1246 هو استعراض الحلول التقنية لمكافحة الرسائل الاقترامية الصوتية دون اعتبار المخاطر التي تنطوي عليها حقيقة هوية الجهة المتطفلة. وتعطي هذه التوصية لمحة عامة عن الرسائل الاقترامية الصوتية وتلخص التكنولوجيا الحالية لمكافحة الرسائل الاقترامية التي يستخدمها المستعملون النهائيون وشبكات الاتصالات على السواء وكذلك آليات التعاون فيما بينهم. ويوصى أيضاً بحلول تقنية إضافية مقترحة استناداً إلى التكنولوجيا وآليات التعاون هذه المضادة للرسائل الاقترامية. ويقدم التعديل 1 آلية التغذية الراجعة من العميل الذي يتلقى مكالمات اقترامية 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) الاقترامية الواردة. وتُعرض سيناريوهات التواصل التفاعلي بين العملاء ومشغلي/مقدمي خدمات شبكات الاتصالات الهاتفية بشأن المكالمات الاقترامية الواردة والتدابير التقنية اللازمة للحفاظ على هذا التواصل التفاعلي. ويتمثل هذا التفاعل في قيام متلقي المكالمات الاقترامية، بعد الانتهاء من المكالمات مباشرةً، بالاتصال برقم مكافحة الرسائل الاقترامية الذي يوفره مشغل الاتصالات مقدماً.

التسلسل التاريخي

الطبعة	التوصية	تاريخ الموافقة	لجنة الدراسات	معرف الهوية الفريد*
1.0	ITU-T X.1246	2015-09-17	17	11.1002/1000/12448
1.1	ITU-T X.1246 (2015) Amd. 1	2022-05-20	17	11.1002/1000/14988

مصطلحات أساسية

الرسائل الاقترامية، الرسائل الاقترامية الصوتية.

* للنفذ 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

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 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	1	1	مجال التطبيق
1	2	2	المراجع
2	3	3	التعاريف
2	1.3	1.3	المصطلحات المعرّفة في وثائق أخرى
2	2.3	2.3	المصطلحات المعرّفة في هذه التوصية
3	4	4	المختصرات والأسماء المختصرة
4	5	5	الاصطلاحات
4	6	6	لمحة عامة عن الرسائل الاقتحامية الصوتية
4	1.6	1.6	سيناريوهات الاتصالات الصوتية
5	2.6	2.6	خصائص الرسائل الاقتحامية الصوتية
6	7	7	تكنولوجيات مكافحة الرسائل الاقتحامية الصوتية
6	1.7	1.7	الجوانب العامة
6	2.7	2.7	التكنولوجيات من جانب الشبكة
12	3.7	3.7	التكنولوجيات من جانب المستخدم
13	4.7	4.7	آلية التعاون
13	5.7	5.7	الحلول المقترحة
15			الملحق A - التدابير التفاعلية والتقنية لمكافحة المكالمات الاقتحامية
15	1.0A	1.0A	سيناريو/خوارزمية/حالة استعمال التغذية الراجعة التفاعلية
16	2.A	2.A	المتطلبات التقنية
17			التذييل I - تدابير شاملة بشأن مكافحة الرسائل الاقتحامية الصوتية
18			التذييل II - حل مقترح بشأن التحقق التفاعلي
19			التذييل III - اعتبارات السياسة العامة في مجال مكافحة الرسائل الاقتحامية الصوتية
19	1.III	1.III	المستخدمون
19	2.III	2.III	المشغلون
20	3.III	3.III	الجهات الإدارية والمنظمات التي تشكل طرفاً ثالثاً
21			بيبلوغرافيا

التكنولوجيات المشاركة في مكافحة الرسائل الاقترامية الصوتية في منظمات الاتصالات

التعديل 1

ملاحظة صياغية: هذا منشور نص كامل. والتنقيحات المطروحة بهذا التعديل مبينة بعلامات المراجعة بالنسبة إلى التوصية ITU-T X.1246 (2015).

1 مجال التطبيق

تقدم هذه التوصية لمحة عامة عن الرسائل الاقترامية الصوتية وتعرض التقنيات القائمة المستخدمة للمساعدة في مكافحة الرسائل الاقترامية الصوتية، بما في ذلك التكنولوجيات من جانب شبكة ومن جانب المستخدم وآلية التعاون بينهما. وبالإضافة إلى ذلك، تقترح هذه التوصية أيضاً حلاً إضافياً لعملية مكافحة الرسائل الاقترامية، مثل سجلات التشوير والتحقق التفاعلي وتدابير التحكم، وما إلى ذلك.

وتركز هذه التوصية حصراً على مكافحة الرسائل الاقترامية الصوتية الصادرة من حيز تبديل الدارات في شبكات الاتصالات مع مراعاة محددة لخصائص البنية التحتية للشبكة. أما تكنولوجيات مكافحة الرسائل الاقترامية الصوتية الصادرة من الحيز القائم على بروتوكول الإنترنت، فينبغي أن تحال إلى المراجع [ITU-T X.1244] و [b-ITU-T X.1245] و [b-IETF RFC 5039]. وأما التكنولوجيات التي تمنع انتحال هويات متصلين فهي تقع خارج مجال تطبيق هذه التوصية.

وتبني مراعاة الامتثال للقوانين والتشريعات ذات الصلة كافة قبل اعتماد أساليب مكافحة الرسائل الاقترامية الواردة في هذه التوصية.

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 الطبعات 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.

[ITU-T X.1240] التوصية ITU-T X.1240 (2008)، التكنولوجيات المشاركة في مكافحة الرسائل الاقترامية المصاحبة للبريد الإلكتروني.

[ITU-T X.1244] التوصية ITU-T X.1244 (2008)، الجوانب العامة لمكافحة الرسائل الاقترامية في تطبيقات الوسائط المتعددة القائمة على بروتوكول الإنترنت.

[ITU-T X.1247] التوصية ITU-T X.1247 (2016)، الإطار التقني لمكافحة الرسائل الاقترامية المتنقلة.

3 التعاريف

1.3 المصطلحات المعرّفة في وثائق أخرى

تستخدم هذه التوصية المصطلحات التالية المعرّفة في وثائق أخرى:

1.1.3 شبكة عاملة بتبديل الدارات [b-ITU-T M.60]: شبكة توفر توصيلات لاستخدام المستخدمين الحصري طوال مدة مكاملة أو خدمة من خلال التوصيل البيني لقنوات الإرسال أو دارات الاتصالات.

2.1.3 شبكة قائمة على بروتوكول الإنترنت [b-ITU-T E.370]: شبكة يُستخدم فيها بروتوكول الإنترنت كبروتوكول الطبقة 3 لدى المنظمة الدولية للتوحيد القياسي (ISO) (النموذج المرجعي للتوصيل البيني للأنظمة المفتوحة (OSI)).

3.1.3 المشغّل [b-ITU-T M.1400]: عبارة عن منظمة مسؤولة عن تحديد هوية موارد الاتصالات وإدارتها. ويجب أن يكون هذا المشغّل معترف به قانوناً من جانب إدارة الاتصالات الموجودة في البلد، أو الوفد المعني بذلك. وقد يُقصد بالمشغّل أحد الشركاء التجاريين أو لا يُقصد به ذلك.

4.1.3 خدمة الإبلاغ [ITU-T X.1247]: خدمة توفر جمع وإجمال الإبلاغ عن الرسائل الاقتحامية للمشارك بموجب إذن المستعمل، واللوائح والقوانين الوطنية.

5.1.3 خدمة الرسائل القصيرة (SMS) [b-ITU-T X.1231]: تشير خدمة الرسائل القصيرة إلى نوع من أنواع خدمات المراسلة التي تتيح للهواتف المتنقلة والهواتف الثابتة والكيانات الأخرى للرسائل القصيرة (SME) نقل واستلام رسائل نصية من خلال جهاز يدعى مركز الخدمة يقوم بتنفيذ الوظائف مثل عمليات الحفظ والتسليم.

6.1.3 اقتحام خدمة الرسائل القصيرة [b-ITU-T X.1242]: رسائل اقتحامية ترسل عبر خدمة الرسائل القصيرة.

7.1.3 الاقتحام (spam) [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 وتوفرها 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 ترسل بالجملة عبر البريد الإلكتروني أو بواسطة خدمة المراسلة المتنقلة لأغراض الترويج التجاري لمنتجات أو خدمات ما.

8.1.3 المقتحم (spammer) [ITU-T X.1240]: كيان أو شخص يُعدّ رسائل اقتحامية ويرسلها.

~~**4.1.3 صاحب الرسائل الاقتحامية [b-ITU-T X.1231]:** يشير صاحب الرسائل الاقتحامية إلى كيان أو شخص ينشئ رسائل طفيلية ويرسلها.~~

2.3 المصطلحات المعرّفة في هذه التوصية

تعرف هذه التوصية المصطلحات التالية:

1.2.3 رقم مكافحة الرسائل الاقتحامية: رقم هاتفي خاص يُحدد مسبقاً من جانب مقدم الخدمة المنزلية/الخاصة/مشغّل الاتصالات (يمكن أن يكون هذا الرقم فريداً في البلد أو فردياً لكل مشغّل)، يقوم من خلاله المستعمل بالإبلاغ عن تلقي مكاملة اقتحامية إلى رقم هاتفه مباشرة قبل الاتصال برقم مكافحة الاقتحام هذا. والإخطار هو واقع الاتصال برقم مكافحة الرسائل الاقتحامية؛ وينبغي ألا يقدم المستعمل أي معلومات.

2.2.3 مصيدة: برمجية (قد تكمن في مطراف) تحاكي مطرافاً أو مجموعة من المطاريف لكشف من يُشتبه بكونهم من أصحاب الرسائل الاقتحامية الصوتية، بل وللمساعدة في التحقق منهم. ويمكن أن تُستخدم مخرجات هذه الأنظمة في جمع الأدلة.

3.2.3 تقرير المستعمل التفاعلي: شكوى من مشترك يتلقى مكالمة إلى المطراف الهاتفية تحتوي على رسالة اقتحامية أو تعتبر اقتحاماً. وبشكل عام، يعد الإبلاغ بمناوبة مكالمة (واقع الاتصال) إلى رقم مكافحة الرسائل الاقتحامية أو إعادة توجيه مكالمة اقتحامية مشبوهة مع رسالة إلى رقم مكافحة الرسائل الاقتحامية.

43.2.3 جهة إدارية: جهة قد تتولى واحدة أو أكثر من مسؤوليات إدارة أو تدقيق أو توجيه أعمال مكافحة الرسائل الاقتحامية الصوتية.

5.2.3 مكالمة اقتحامية: مكالمة هاتفية تتضمن رسالة صوتية أو نصية أو وسائط متعددة غير مرغوب فيها، الغرض منها، كقاعدة عامة، تسويق منتجات أو خدمات تجارية.

6.2.3 مكالمة اقتحامية مشبوهة: مكالمة هاتفية غير محددة يُشتبه في أنها غير مرغوب فيها.

74.2.3 منظمة تشكل طرفاً ثالثاً: كيان يمكنه أن يقدم المشورة أو المساعدة أو التنسيق في أعمال مكافحة الرسائل الاقتحامية الصوتية.

81.2.3 الرسائل الاقتحامية الصوتية: مكالمات هاتفية مسجلة مسبقاً تُرسل تلقائياً على غير استئذان من المتلقي، وتهدف عادة إلى تسويق منتجات أو خدمات تجارية. ويتراوح محتوى الرسائل الاقتحامية الصوتية بين إعلان عن منتجات وبين مواد إباحية مسيئة. وقد تنوع الآثار الضارة للرسائل الاقتحامية الصوتية على المستخدمين والمشغلين.

4 المختصرات والأسماء المختصرة

تستعمل هذه التوصية المختصرات والأسماء المختصرة التالية:

Caller ID تعرف هوية المتصل (Caller Identification)

CAMEL تطبيقات على مقياس منطق الاتصالات المتنقلة المعزز (Customized Applications for Mobile Enhanced Logic)

CCLTP النقطة الزمنية لإجازة المكالمة (Call Clear Time Point)

CCOTP النقطة الزمنية لاستمرار المكالمة (Call Continued Time Point)

CDMA نفاذ متعدد بتقسيم شفري (Code Division Multiple Access)

CDR سجل تفاصيل المكالمة (Call Detail Record)

CDR_n سجل تفاصيل المكالمة الأولية (initial Call Detail Record)

CDR_{n+1} سجل تفاصيل المكالمة 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_n تعرف هوية خط طالب النداء الأولي إلى المستعمل (Calling Line Identification of initial caller to the user)

CLI_{n+1} تعرف هوية خط الطالب للمستعمل، عند إجراء مكالمة تغذية راجعة إلى رقم مكافحة الرسائل الاقتحامية (Calling Line Identification of the user, when it makes feedback call to an anti-spam number)

COSN رقم المشترك المنشئ للمكالمة (Call Originated Subscriber Number)

COTP النقطة الزمنية لإنشاء المكالمة (Call Originating Time Point)

CRBT نغمة رنين الاتصال المخصصة (Customized Ring Back Tone)

CS بتبديل الدارات (Circuit-Switched)

CTSN رقم المشترك الذي ينهي المكالمة (Call Terminated Subscriber Number)

DMP منصة إدارة الجهاز (Device Management Platform)

GMSC مركز التبديل المتنقل للبوابة (Gateway Mobile Switching Centre)

GSM نظام الاتصالات المتنقلة العالمي (Global System for Mobile communications)

HLR سجل المواقع الرئيسية (Home Location Register)

تحديد الهوية (Identification)	ID
نظام تبادل المعلومات (Information Sharing System)	ISIS
نظام فرعي متعدّد الوسائط قائم على بروتوكول الإنترنت (IP Multimedia Subsystem)	IMS
شبكة ذكية (Intelligent Network)	IN
بروتوكول تطبيق شبكة ذكية (Intelligent Network Application Protocol)	INAP
بروتوكول الإنترنت (Internet Protocol)	IP
رد صوتي تفاعلي (Interactive Voice Response)	IVR
خدمة الرسائل متعددة الوسائط (Multimedia Messaging Service)	MMS
مركز تبديل متنقل (Mobile Switching Centre)	MSC
منصة عبر الأثير (Over-the-Air Platform)	OTAP
الشبكة الهاتفية العمومية التبديلية (Public-Switched Telephone Network)	PSTN
جودة الخدمة (Quality of Service)	QoS
نقطة تحكم في الخدمة (Service Control Point)	SCP
وحدة هوية المشترك (Subscriber Identity Module)	SIM
النقطة الزمنية لإقامة وصلة التشوير (Signalling Link Establishment Time Point)	SLETP
النقطة الزمنية لفك وصلة التشوير (Signalling Link Release Time Point)	SLRTP
خدمة الرسائل القصيرة (Short Message Service)	SMS
نظام التشوير رقم 7 (Signalling System No.7)	SS7
نقطة نقل التشوير (Signalling Transfer Point)	STP
نظام الاتصالات المتنقلة الشامل (Universal Mobile Telecommunications System)	UMTS
سجل موقع الزائر (Visitor Location Register)	VLR
مخدّم البريد الصوتي (Voice Mail Server)	VMS
الاتصالات الصوتية عبر بروتوكول الإنترنت (Voice over Internet Protocol)	VoIP

5 الاصطلاحات

لا توجد.

6 ملحة عامة عن الرسائل الاقتحامية الصوتية

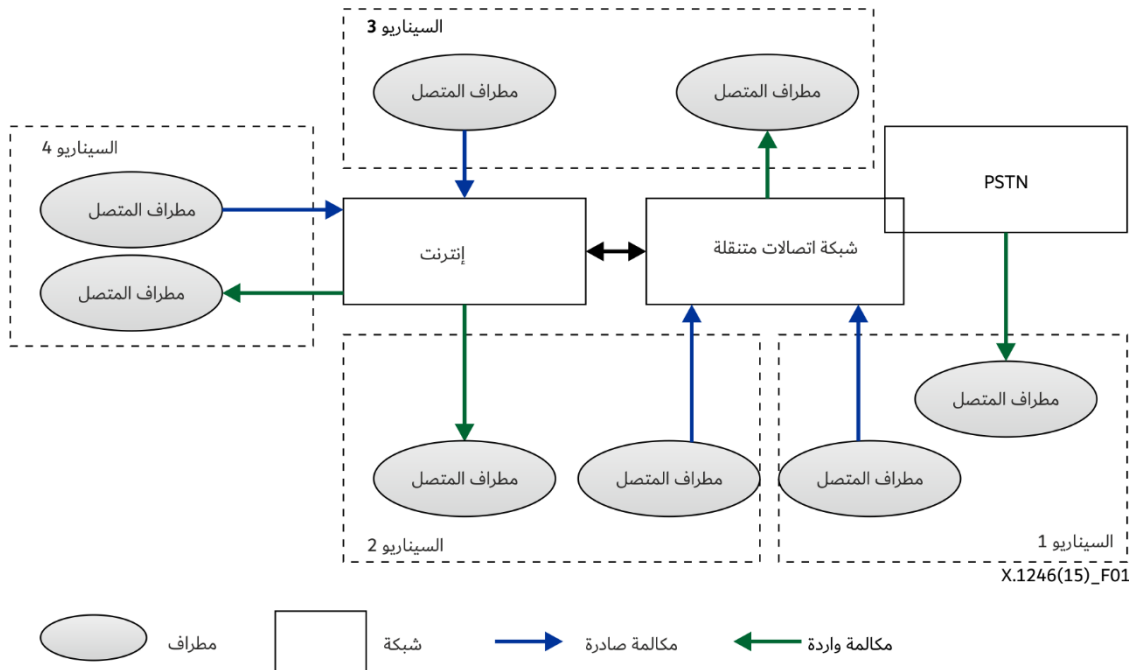
الرسائل الاقتحامية الصوتية هي مكالمات هاتفية مسجلة مسبقاً تُرسل تلقائياً على غير استئذان من المتلقي، وتهدف عادة إلى تسويق منتجات أو خدمات تجارية. ويتراوح محتوى الرسائل الاقتحامية الصوتية بين إعلان عن منتجات وبين مواد إباحية مسيئة. وتعدد الآثار الضارة للرسائل الاقتحامية الصوتية بأنواعها المختلفة على المستخدمين والمشغلين.

1.6 سيناريوهات الاتصالات الصوتية

الاتصالات الصوتية هي خدمة أساسية يقدمها مشغلو الاتصالات. وفي الأصل، كانت الاتصالات الصوتية تقوم على الشبكات العاملة بتبديل الدارات (CS). ومع تطور الإنترنت، توسعت الاتصالات الصوتية لتشمل الاتصالات الصوتية عبر بروتوكول الإنترنت (VoIP) على امتداد الشبكات القائمة على بروتوكول الإنترنت (IP).

ويُنظر أدناه في أربعة سيناريوهات للاتصالات الصوتية، تحدد التكنولوجيات المستخدمة كل منها:

- السيناريو 1: CS-CS: اتصالات صوتية تقليدية متنقلة/ثابتة بتبديل الدارات.
 - السيناريو 2: CS-IP: اتصالات صوتية تصدر عن مستخدم اتصالات متنقلة/ثابتة بتبديل الدارات وتنتهي عند مستخدم مهاتفة عاملة بروتوكول الإنترنت.
 - السيناريو 3: IP-CS: اتصالات صوتية تصدر عن مستخدم مهاتفة عاملة بروتوكول الإنترنت وتنتهي عند مستخدم اتصالات متنقلة/ثابتة بتبديل الدارات.
 - السيناريو 4: IP-IP: اتصالات صوتية بين مستخدم مهاتفة عاملة بروتوكول الإنترنت.
- وتظهر في الشكل 1 هذه السيناريوهات الأربعة للاتصالات الصوتية مع التكنولوجيات المرتبطة بها.



الشكل 1 - سيناريوهات اتصالات صوتية في شبكات الاتصالات

ملاحظة - قد يشمل مصطلح طرف المبين هنا في الشكل رقم 1، هواتف متنقلة وهواتف ثابتة وحواسيب محمولة وحواسيب شخصية، وما إلى ذلك، مما يمكنه من النفاذ إلى شبكات الاتصالات بتبديل الدارات/القائمة على بروتوكول الإنترنت. وبصفة عامة، فإن معظم المستخدمين يتقنون بمصدر الاتصالات الصوتية. ونتيجة لذلك، فإن أصحاب الرسائل الاقتحامية الصوتية على استعداد لاستخدام الاتصالات التقليدية بتبديل الدارات لإرسال الرسائل الاقتحامية الصوتية. بالإضافة إلى ذلك، ترد في التوصية [ITU-T X.1244] تكنولوجيات يوصى بها لمكافحة الرسائل الاقتحامية الصوتية التي تندرج في السيناريو 3 والسيناريو 4. ولذلك، ينحصر تركيز هذه التوصية على مكافحة الرسائل الاقتحامية الصوتية التي تندرج في السيناريو 1 (CS-CS) والسيناريو 2 (CS-IP).

2.6 خصائص الرسائل الاقتحامية الصوتية

يمكن أن يتراوح المحتوى الذي تنشره الرسائل الاقتحامية الصوتية بين الإعلان التجاري وبين مواد إباحية مسيئة؛ مما قد يتسبب في آثار ضارة على المستخدمين ومشغلي الشبكات:

- يمكن أن تتضمن الرسائل الاقتحامية الصوتية محتويات مملّة أو خادعة أو محتويات تنطوي على تهريب أو تهديد.
- يمكن أن يعاني المستخدمون والمشغلون من هدر الموارد.
- يمكن أن يحتاج المستخدمون والمشغلون إلى إنفاق بعض الوقت والمال والجهد في مكافحة الرسائل الطفيلية الصوتية.

وتصنف أشكال الرسائل الاقترامية الصوتية الأكثر رواجاً في نمطين دون الاقتصار عليهما:

- **النمط الأول (المكالمة الصامتة):** المكالمة الصامتة هي مكالمة هاتفية بقصد التسويق عبر الهاتف تتولد بمهاتف تنبؤي (أو مهاتف تنبؤي) دون نية الوكيل أن يتعامل مع هذه المكالمة على الفور. وفي هذه الحالة، يمكن للمهاتف إنهاء المكالمة، فيسمع الطرف الذي اتصل به صمتاً ("سكوناً هامداً") أو نغمة من شركة الهاتف تشير إلى انقطاع المكالمة. ويحمل مصطلح "المكالمة المهجورة" المعنى نفسه. وعادة، يتوقع هذا النوع من المكالمات مكالمة جوايية.
- **النمط الثاني (المكالمة اللجوجة):** مكالمة هاتفية بقصد التسويق عبر الهاتف يمكنها كذلك أن تلح أو تزعج أو تفرع أو ترهب بمحتوى إباحي أو مهدد أو بمعلومات غير قانونية أو إعلان زائف وما إلى ذلك. وعادة، لن ينقطع هذا النوع من المكالمات حتى يُفتح الخط مع متلقي المكالمة.

7 تكنولوجيا مكافحة الرسائل الاقترامية الصوتية

1.7 الجوانب العامة

لا يمكن لأي من الحلول أن ينجح بشكل مستقل تماماً. وللتخفيف من التأثير السلبي للرسائل الاقترامية الصوتية، تدعو الضرورة لتنفيذ مجموعة شاملة من الحلول مع تكنولوجيا ملازمة لها، تصنّف بتكنولوجيا من جانب الشبكة وتكنولوجيا من جانب المستخدم من أجل تغطية السيناريو 1 والسيناريو 2 اللذين جاء وصفهما في الفقرة 1.6.

وللتوصية بتكنولوجيا ملموسة وعملية، يتعين النظر ملياً في خصائص الشبكة العاملة بتبديل الدارات، بما في ذلك معمارية الشبكة، وطوبولوجيا الشبكة وكدسة بروتوكول التشوير وما إلى ذلك. وبالإضافة إلى ذلك، يُنظر كذلك في عمليات الخدمة الصوتية والاتجاهات الوظيفية للمطاريق. ويمكن تصنيف التكنولوجيا الموصى بها كتكنولوجيا من جانب الشبكة وتكنولوجيا من جانب المستخدم.

والتكنولوجيا من جانب الشبكة هي تكنولوجيا أساسية للمشغلين، أي في الشبكات الهاتفية العمومية التبدلية (PSTN) وأنظمة الاتصالات المتنقلة الشاملة (UMTS) ونظام الاتصالات المتنقلة العالمي (GSM) وشبكات النفاذ المتعدد بتقسيم شفري (CDMA). وبالمقارنة مع التكنولوجيا من جانب الشبكة، فإن التكنولوجيا من جانب المستخدم أكثر مرونة بكثير وتعتمد على مبادرات المستخدم. وتُعتبر الملاحظات التقييمية من المستخدمين تكملة ضرورية للتكنولوجيا من جانب الشبكة. ولذلك، ينبغي أيضاً وضع آلية تعاون فعالة بين التكنولوجيتين.

2.7 التكنولوجيا من جانب الشبكة

تُشأ كل مكالمة هاتفية في شبكة النفاذ بالتشوير. ولكشف من يُشبهه بإرساله رسائل طفيلية صوتية، يتمثل الأسلوب الأساسي في جمع بيانات التشوير وتحليلها والتحقق منها. وينبغي النظر في هذا الأسلوب بشكل شامل. وبصفة عامة، تنطوي مرحلة إعداد مكالمة على إقامة اتصال بين طرفي الاتصال. وخلال مرحلة إعداد مكالمة، يكون تحديد هوية الهاتف هو تحديد الهوية (ID) الوحيد للمهاتف/الطرف المتصل به. ويؤدي ذلك إلى الملاحظة التالية.

- (1) ينبغي اتخاذ أي قرارات بشأن التعامل مع المكالمة في الوقت الفعلي قبل اكتمال إعداد المكالمة.

وتمثل الرسائل الاقتحامية الصوتية تحديات تكنولوجية معقدة، وبالتالي فإن إيجاد حلول للتخلص منها يحتاج إلى دعم بالإجراءات المناسبة، إلى جانب التدابير التكنولوجية. ويمكن أن يتضمن إجراء أساسي من جانب الشبكة لمكافحة الرسائل الاقتحامية الصوتية العمليات التالية المبينة في الشكل 2:



X.1246(15)_F02

الشكل 2 - إجراء من جانب الشبكة لمكافحة الرسائل الاقتحامية الصوتية

- تسجيل وجمع التشوير: تسجيل وجمع بيانات التشوير الأصلية في الوقت الفعلي.
 - تحليل: تحديد هوية من يشتبه بكونهم من أصحاب الرسائل الاقتحامية الصوتية، وإدراج أرقامهم في قائمة.
 - التحقق التفاعلي: للقيام بالتحقق المباشر من أجل معرفة أصحاب الرسائل الاقتحامية الصوتية الحقيقيين في قائمة المشتبه بهم.
 - التحكم: لتقييد أو تعطيل أصحاب الرسائل الاقتحامية الصوتية المؤكدين بعملية التحقق من أجل حماية المستخدمين العاديين.
- ويكاد يتكون الإجراء من جانب المستخدم من العمليات نفسها ولكن بتدابير أكثر بساطة في كل جزء. وفي بعض الحالات، يمكن إهمال التحقق التفاعلي.

وحسب الإجراء المتبع، تتعدد تكنولوجيات التعامل مع كل جزء على التوالي. وتجدر الإشارة إلى أن أيًا من التكنولوجيات التي يرد بحثها في الفقرات التالية ستكون بمثابة "حل سحري" أو الحل الوحيد الناجع للمشاكل التي تسببها الرسائل الاقتحامية الصوتية. وعلى العكس من ذلك، كل هذه التكنولوجيات متكاملة وستزداد فعاليتها عندما تُجمع معاً.

وستعرف هذه التوصية بالتكنولوجيات وتصنفها وفق مواضع نشرها، أي التكنولوجيات من جانب الشبكة ومن جانب المستخدم، ووفق العمليات (المشار إليها في الشكل 2).

1.2.7 تسجيل وجمع التشوير

إن تسجيل وجمع التشوير هو جمع بيانات سجل تفاصيل المكالمات جمعاً (شبه) آني للتحليل، ويمكن أن يشمل ذلك بيانات ذات صلة بالوقت أو ذات صلة برقم الهاتف، مثل:

- النقطة الزمنية لإنشاء المكالمات (COTP): نقطة زمنية يبادر فيها متصل إلى إجراء مكالمات هاتفية.
 - النقطة الزمنية لإقامة وصلة التشوير (SLETP): النقطة الزمنية لإقامة وصلة التشوير بين متصل ومتصل به.
 - النقطة الزمنية لاستمرار المكالمات (CCOTP): النقطة الزمنية لاستمرار مكالمات هاتفية وفتح المتصل به لخط الاتصال.
 - النقطة الزمنية لإجازة المكالمات (CCLTP): النقطة الزمنية لإجازة المكالمات من جانب متصل أو متصل به.
 - النقطة الزمنية لفك وصلة التشوير (SLRTP): النقطة الزمنية لفك وصلة التشوير بعد إجازة مكالمات.
 - رقم المشترك المنشئ للمكالمة (COSN): يُعرف عادة برقم المتصل، أي الرقم الذي يبادر متصل منه إلى إجراء مكالمات.
 - رقم المشترك الذي ينهي المكالمات (CTSN): يُعرف عادة برقم المتصل به، أي الرقم الذي منه أنهى متصل به المكالمات.
- وقد تختلف قليلاً قيم نفس البيانات، وخاصة البيانات المتعلقة بالوقت، حسب مواضع نقاط الجمع. بيد أن هذه التباينات يمكن تجاهلها دائماً في الواقع العملي.

وجدير بالذكر أن جميع البيانات المشار إليها في هذه الفقرة مستقاة من قنوات التشوير وليس من قنوات الخدمة. وفي عملية تسجيل التشوير هذه، توجد عموماً بالفعل كل البيانات التي ستُجمع في نظام إدارة التشوير المعد للمحاسبة وتشخيص الأداء، وبالتالي، تمكن إعادة استخدامها، مع مراعاة التوازن من حيث التكلفة.

ملاحظة – لن تُدرج فيما بعد إلا مصادر البيانات الشائعة (على أساس نظام التشوير رقم 7 (SS7) والشبكة الذكية (IN) والنظام الفرعي متعدد الوسائط قائم على بروتوكول الإنترنت (IMS) ونغمة رنين الاتصال المخصصة (CRBT) ومخيم البريد الصوتي (VMS)، وما إلى ذلك)، رغم أن هناك مصادر بيانات بديلة أخرى، مثل نظام التشوير R2 وأنظمة التنبيه إلى المكالمات الفائتة.

1.1.2.7 التشوير رقم 7 (SS7)

يمكن أن يكون التشوير رقم 7 مصدراً مفيداً للمساعدة في مراقبة الرسائل الاقتحامية الصوتية. ويمكن الاستفادة عملياً من إدخال نقطة جمع التشوير لتكرار معلومات ومعلومات نقطة جمع التشوير وتسجيلها. وتوصل نقطة جمع التشوير على التوازي مع وصلة التشوير بحيث تصبح الإشارة فعلياً "حزمة مفلوكة"، رغم أن نقطة الجمع لن تستهلك إلا جزءاً ضئيلاً من قدرة الإشارة. وفي هذه الحالة، لن تترتب أي آثار سلبية على وصلة التشوير جراء تعطل نقطة التشوير.

وهناك أسلوب آخر أيضاً لجمع التشوير رقم 7 عن طريق إدخال عقدة تشوير خفية بين عقدي تشوير صريحتين. وهذا يعني أن عقدة التشوير الخفية "ستعيق" الإشارة أولاً كي تسجلها ثم ترسلها دون أي تغيير ولكن بفارق كمون بسيط. غير أن هذه التكنولوجيا تنطوي على مخاطر تعطل نقطة واحدة. لذا تُلزم قدرة موثوقة لتجاوز الأعطال وتوفير الرديف الاحتياطي.

وتتمثل الميزة الكبيرة لاستخدام سجلات التشوير رقم 7 في احتوائها على البيانات التفصيلية للمكالمة التي يمكن أن يُستخلص منها مؤشرات مختلفة (انظر الفقرة 2.2.7). ولكن إذا زادت حركة المكالمات الصوتية وتوسعت الشبكة، سيزداد عدد نقاط جمع التشوير في الوقت نفسه لتغطية جميع/كبرى مصادر التشوير من أجل الحفاظ على مستوى مقبول من المراقبة، مما قد يؤدي إلى ارتفاع تكلفة مكافحة الرسائل الاقتحامية.

ويوصى بنشر نقاط جمع التشوير في الشبكات الأساسية/المحلية. ولتحقيق جمع إجمالي، ستشمل هذه النقاط جميع سطوح، تحكُّم الإدارة (Mc) وتحكُّم الشبكة (Nc)، البينية للبدالات. وعلاوة على ذلك، لتحقيق جمع متوازن، لن تشمل هذه النقاط إلا السطوح البينية لتحكُّم الشبكة كلها. وإذا انحصر التركيز على المكالمات الوطنية عبر مسافات طويلة أو المكالمات الدولية، ستشمل المسافات الطويلة/نقاط نقل التشوير (STP).

ملاحظة – إن نقطة جمع التشوير هي عنصر شبكة منطقي يمكن أن يتكون من أنواع مختلفة من عناصر الكيان.

2.1.2.7 الشبكة الذكية (IN)

هناك أسلوب قائم على نقطة تحكُّم في الخدمة (SCP) لجمع تطبيقات على مقياس منطوق الاتصالات المتقلة المعزز (CAMEL) أو تشوير بروتوكول تطبيق الشبكة الذكية (INAP) من أجل التحليل. ونقطة التحكُّم في الخدمة هي عقدة رئيسية في الشبكة الذكية (IN) وعامل محدد في اتخاذ قرار بشأن كيفية معالجة المكالمات الهاتفية.

وحيثما يتعاقد مستخدم على خدمة الشبكة الذكية، ستتحرك المكالمات الصادرة نقطة التحكُّم في الخدمة للاستفسار عن معلومات سجل موقع زائر المستخدم (VLR) المتصل به قبل إعداد وصلات الاتصال. وبما أن خدمات الشبكة الذكية تحظى بشعبية لدى بعض المشغلين، يسهل جمع وتسجيل بيانات التشوير للمكالمات المتولدة من المستخدمين المتعاقدين مع الشبكة الذكية.

وبما أن نقاط جمع التشوير يمكن أن تكون عند/حول نقطة تحكُّم في الخدمة، يحتاج هذا الأسلوب لجمع نقاط تشوير أقل مقارنةً بالتشوير رقم 7. وسواء كان هؤلاء المستخدمون المتعاقدون مع الشبكة الذكية متجولين أم لا، تسهل مراقبتهم باستخدام هذا الأسلوب.

ولكن هناك قيود على هذا الأسلوب. وإذا ظل انتشار خدمة الشبكة الذكية في مستوى منخفض، لن يراقب سوى جزء صغير من سلوكيات المستخدمين. إلا أن هذا الوضع يمكن حله من خلال مساعدة كل مستخدم في الاكتتاب ضمناً في خدمة مفصلة على مقياسه من خدمات الشبكة الذكية؛ خدمة ستحيل طلب الاستفسار دون شروط إلى نقطة التحكُّم في الخدمة عند إنشاء المكالمة الصادرة.

وهذا الأسلوب مقيد بالإجراءات الشائعة لخدمة الشبكة الذكية؛ لذلك لا يمكن جمع إلا أنماط بيانات محدودة، مثل COTP و SLETP و COSN و CTSN (انظر الفقرة 1.2.7). ومع ذلك هناك متسع للتحسين إذا أُدخلت إجراءات أكثر تعقيداً في خدمة الشبكة الذكية، كأن ترَجَّل نقطة التحكم في الخدمة جميع إشارات تشوير المهاتفة، على سبيل المثال.

ويمكن أن يتشابه بحث أسلوب النظام الفرعي متعدّد الوسائط قائم على بروتوكول الإنترنت (IMS) مع ما ورد أعلاه، لأن هذا النظام الفرعي يتشابه مع الشبكة الذكية في إجراءات تشويره.

3.1.2.7 نغمة رنين الاتصال المخصصة (CRBT)

إن نغمة رنين الاتصال المخصصة هي خدمة يقدمها بعض المشغلين تراعي خصوصية كل مستخدم. فما أن يتصل مستخدم بخدمة نغمة رنين الاتصال المخصصة، سيسمع المستخدمون الآخرون مقاطع موسيقية مطلوبة مسبقاً بدلاً من نغمة الرنين. ونتيجة لذلك، يمكن أن يتحقق تسجيل التشوير وجمع البيانات لدى مضيفي نغمة رنين الاتصال المخصصة.

وهذا الأسلوب مقيد بإجراءات الخدمة؛ لذلك لا يمكن جمع إلا بيانات محدودة لدى مضيفي الخدمة، مثل COTP و CCOTP و CCLTP و COSN و CTSN (انظر الفقرة 1.2.7)، ولا تكاد توجد أي تحسينات إضافية في إجراءات نغمة رنين الاتصال المخصصة لجمع المزيد من أنواع البيانات.

ولكن تمكن مراقبة صاحب الرسائل الاقتحامية الصوتية إذا أزعج مستخدم نغمة رنين الاتصال المخصصة. وبالتالي فإن الانتشار الواسع للخدمة هو شرط مسبق لجعل هذا الأسلوب عملياً. فإذا تحققت شروط هذا الوضع، ينبغي أن يكون الاستثمار في تسجيل التشوير وعمليات الجمع منخفضاً نسبياً.

4.1.2.7 مخدّمات البريد الصوتي (VMS)

تتعامل مخدّمات البريد الصوتي (VMS) مع المكالمات في أوضاع إعادة تسيير المكالمات في حالة عدم الرد وإعادة تسيير المكالمات في حالة انشغال الخط وإعادة تسيير المكالمات غير المشروطة، وما إلى ذلك. وفي معظم الحالات، لا يرد مخدّم البريد الصوتي على مكالمات صامتة إلا إذا كان المعيار غير مشروط. ويمكن لمخدّم البريد الصوتي أن يوفر تسجيلات صوتية لطرف متصل إذا نوى المتصل صاحب الرسالة الاقتحامية الصوتية توصيل مكالمته ورسالته الاقتحامية الصوتية إلى المتصل به مباشرة، وفي هذه الحالة يمكن لمخدّم البريد الصوتي أن يدعم عملية التحقق التفاعلية بقوة عبر تسجيلات صوتية مستقاة من ردود المستخدم أو تفويضه، انظر الفقرة 3.3.7.

وشأنه شأن نغمة رنين الاتصال المخصصة (CRBT)، فإن انتشار الخدمة واستخدام مخدّم البريد الصوتي شرط مسبق لجعل هذا الأسلوب عملياً.

5.1.2.7 المصيدة

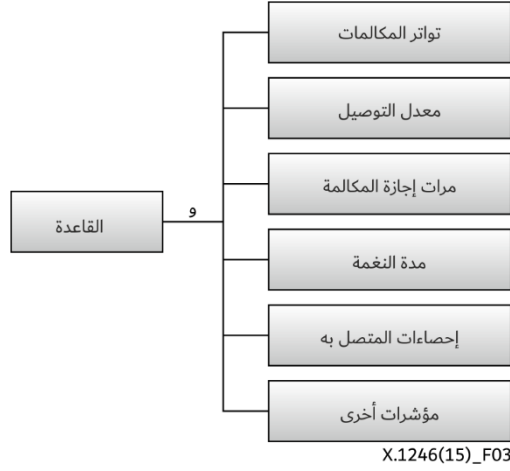
يُستخدم أسلوب المصيدة لإعداد كمية من أرقام الهواتف المتعاقبة أو العشوائية لجذب أصحاب الرسائل الاقتحامية الصوتية. وإلى جانب جمع البيانات، يمكن لأسلوب المصيدة أيضاً أن يسهل إجراء التحليل فضلاً عن إجراء التحقق التفاعلي.

وبما أن أي متصل يمكنه وضع أسلوب المصيدة على الخط (مكالمات صادرة)، يمكن بهذا الأسلوب جمع بعض الأنواع المعينة من البيانات، مثل COTP و CCOTP و CCLTP و COSN و CTSN، انظر الفقرة 1.2.7. وسيقوم أسلوب المصيدة بحساب ونقل البيانات لبعض التدابير التحليلية التي يرد وصفها في الفقرة 2.2.7.

2.2.7 التحليل

من أجل إجراء تحليل لمكافحة الرسائل الاقتحامية الصوتية باستخدام نظام المراقبة، يتعين حساب ما تُجمع من البيانات الأصلية وتحويله إلى مؤشرات ذات مغزى مثل معدل التوصيل ووقت فك المكالمات ومدة الرنين، وما إلى ذلك. ولتفريق الرسائل الاقتحامية الصوتية من جانب المستخدمين العاديين، ينبغي تعداد المؤشرات بشكل مستمر لفترة محددة، تُعرف عادة بالنافذة الزمنية (المدة). ويمكن للمشغلين ضبط المدة بقيمة مناسبة استناداً إلى خبرة الصيانة.

ويمكن توحيد جميع المؤشرات منطقياً في مؤشر أشمل يسمى "القاعدة"، يمكن استخدامه في خوارزمية ما لتحليل سلوك أصحاب الرسائل الاقتحامية الصوتية بقدر أعلى من الدقة. ويظهر في الشكل 3 نموذج القاعدة لتحليل أصحاب الرسائل الاقتحامية الصوتية.



الشكل 3 - نموذج القاعدة

يُستخلص نموذج القاعدة من العديد من المؤشرات بعملية الواو منطقية. ولما كانت مصادر البيانات مستقاة من مصادر مختلفة، ويمكن أن تُجمَع معاً، لا يمكن دعم المؤشرات كلها في نفس الوقت. ويتمثل حل مجدٍ للمشكلة في إسناد قيمة "صحيح" أو "1" إلى المؤشرات غير المدعومة لتجاهلها. فعلى سبيل المثال، بعد جمع البيانات وتحويلها إلى مؤشرات، لا تحتاج المصيدة إلا لمؤشر مدة النغمة لمعالجة إجراء التحليل اللازم، وإسناد قيمة "صحيح" أو "1" إلى المؤشرات الأخرى لحذفها.

ويرد أدناه ما يحتويه نموذج القاعدة من مؤشرات مع تعاريفها:

- تواتر المكالمات: عدد المكالمات في فترة معينة.
- معدل التوصيل: معدل اتصالات المكالمات أو إنشاء وصلة التشوير.
- مرات إجازة المكالمات: عدد المرات التي يجيز فيها المتصل أو المتصل به المكالمات من تلقاء نفسه.
- مدة النغمة: المدة الزمنية لنغمة الرنين.
- إحصاءات المتصل به: إحصاءات عن خصائص المتصل به، مثل التوزيع المنتظم والمتوالي الحسابية، وما إلى ذلك.

وينبغي للمشغلين تعديل قيمة عتبة المؤشرات استناداً إلى سيناريوهات الخدمة الواقعية لتحقيق التوازن بين الدقة والتكلفة. وعلاوةً على ذلك، ينبغي تحديد قواعد ملموسة لتناسب مع أنواع مختلفة من الرسائل الاقتحامية الصوتية.

على سبيل المثال، هناك نمطان معروفان على نطاق واسع من الرسائل الاقتحامية الصوتية وهما: المكالمات الصامتة والمكالمات اللجوجية، انظر الفقرة 2.6. والمكالمات الصامتة (تسمى أيضاً المكالمات المهجورة) هي مكالمات هاتفية يجريها مهاتف، لا وكيل متاح لديه على الفور، لمعالجة المكالمات. وفي هذه الحالة، يمكن للمهاتف إنهاء المكالمات، فيسمع الطرف الذي أتصل به صمتاً ("سكوناً هامداً") أو نغمة من شركة الهاتف تشير إلى انقطاع المكالمات. وعادة، يتوقع هذا النوع من المكالمات مكالمات جوابية. أما المكالمات اللجوجية فهي مكالمات هاتفية تقصد أن تلح أو تززع أو تفرع أو ترهب بمحتوى إباحي أو مهدد أو بمعلومات غير قانونية أو إعلان زائف وما إلى ذلك. وعادة، لن تنقطع هذه المكالمات حتى يُفتح الخط مع متلقي المكالمات.

ويمكن أن تُظهر المكالمات الصامتة والمكالمات اللجوجية (انظر الفقرة 2.6) ملامح مؤشر مختلفة على التوالي من حيث نموذج القاعدة المقترح. فارتفاع قيمة تواتر المكالمات أو مرات إجازة المكالمات، وانخفاض قيمة معدل التوصيل أو مدة الرنين يمكن أن يلوها أدعى للشك بصاحب رسالة طفيلية صوتية صامتة. ومن ناحية أخرى، قد تركز مكالمات لجوجية على متلقي محدد للمكالمات؛ وتميل إلى إطالة مدة الرنين فتحصل على معدل توصيل أعلى نسبياً.

وفي بعض الظروف، ستفتح مجموعة من المتصلين الصامتين خدمة "إعادة التسيير غير المشروطة" لإبلاغ الشبكة بإعادة تسيير المكالمات الواردة غير المشروطة إلى رقم معين، تعمل عليه منصة رد صوتي تفاعلي (IVR). ويمكن لفعل هذه المنصة أن يصل إلى حد إعادة الرسالة الاقتحامية الصوتية الصامتة إلى المتصل الوارد بواسطة نغمة رنين. وسيكون مفيداً للتحليل التأكيد مما إذا فتح المتصلون المشبهون خدمة "إعادة التسيير غير المشروطة" ومن ماهية رقم المقصد.

وتوجد على أرض الواقع بعض نماذج التحليل الأكثر تعقيداً وفعالية في مكافحة الرسالة الاقتحامية الصوتية، كالنموذج المتكامل مع تحليل المجتمع البشري، وتحليل سجلات المتصل الخاضعة للفترة، وهلم جرا. ومع ذلك، يمكن لنموذج القاعدة أن يكون أساساً لتطوير نماذج أكثر شمولاً.

3.2.7 التحقق التفاعلي

بناءً على طلب الجهات الإدارية أو اتفاق خدمة المستخدم، يتعين أن يُتحقق من أرقام المتصلين المدرجة في القائمة المشبوهة قبل اتخاذ بعض تدابير التحكم. وهناك أسلوبان بديلان لتشغيل التحقق من حيث المتطلبات. في الأسلوب الأول، يتعين على منظمات الاتصالات أن تواصل تحديث القائمة المشبوهة وأن تقدمها للجهات الإدارية وأن تستلم الردود التقييمية منها.

وفي الأسلوب الثاني، إذا سمح اتفاق خدمة المستخدم أو الجهات الإدارية بذلك، يمكن أن يقوم المشغل بإجراء اختبار مراقبة على رقم متصل مدرج في القوائم المشبوهة من أجل الحصول على تحقق مباشر. وباستخدام نتائج اختبار المراقبة، المعروف عادة باسم ملف السجل الصوتي، سيحاول موظفو التدقيق المخولون تبيان ما إذا كان السجل رسالة طفيلية أم لا. غير أن الإجراء التحكمي يتأثر بدقة وجودة التحقق التفاعلي.

وكما ذكر أعلاه، يمكن للمصيدة أن تتعامل مع التحقق التفاعلي بنفسها، أي إذا بينت نتيجة حساب المؤشرات ضمناً بأن المكالمات الصادرة هي مكالمات صامتة (انظر الفقرة 2.6)، سترد المصيدة بمكالمة لإثبات أدلة التحقق؛ وفي المقابل، عند تأكيد مكالمات لجوجة من خلال تحليل المؤشرات، ستفتح المصيدة خط المكالمة الهاتفية وستسجلها.

وعلاوةً على ذلك، قد يتسبب التنسيق بين مجموعة من المتصلين الصامتين ومنصة رد صوتي تفاعلي أو عدة منصات رد صوتي تفاعلي بإرباك بين المشغلين بشأن المصدر الحقيقي للرسالة الاقتحامية الصوتية. وفي بعض الأحيان، تعود منصات الرد الصوتي التفاعلي والمتصلين الصامتين إلى مشغلين مختلفين على التوالي. وبعد الحصول على سجل صوتي للرسالة الاقتحامية الصوتية، سيستفاد مثلاً من تتبع التوصيل المحتمل بين المتصل الصامت ومنصة الرد الصوتي التفاعلي عن طريق تقديم طلب إلى سجل المواقع الرئيسية (HLR).

4.2.7 التحكم

يُستخدم التحكم لتقييد أو تعطيل/إغلاق أصحاب الرسائل الاقتحامية الصوتية المؤكدين بالتحقق لحماية المستخدمين العاديين. ويناقش أسلوبان للتحكم أدناه.

1.4.2.7 القوائم البيضاء/القوائم السوداء

تُعرف القوائم البيضاء/القوائم السوداء عادة بقوائم الحسابات الرئيسية، ويستغرق إنشاؤها وقتاً طويلاً وهي تتطلب التحديث باستمرار. وتحتاج دورة حياة كل بند في القائمة البيضاء/القائمة السوداء إلى حسن الإدارة للحفاظ على دقته وفعاليتها. ويحتاج أيضاً كل بند في القائمة البيضاء/القائمة السوداء إلى حسن الصيانة بطريقة آمنة خلال دورة حياته.

وعلى النحو الموضح في التوصية [ITU-T X.1240]، تختلف جودة القوائم السوداء اختلافاً كبيراً حسب الكفاءة المهنية لمن يقوم بجمعها. ولا مناص من أن تتخلل القوائم السوداء أخطاءً تمنع بعض المكالمات المشروعة من الوصول إلى مستقبلها. وعلى الرغم من أن استخدامها يثير العديد من المخاوف، تقدم القوائم السوداء حلاً سريعاً يحول دون توصيل مصادر الرسائل الاقتحامية الصوتية بمستقبلها (من مستخدمي الهاتف).

وتُنشر عادة قوائم سوداء تتضمن أرقام أو قطاعات أرقام المستخدم في مركز التبدل المتنقل للبوابة (GMSC) وفي نقطة تحكم في الخدمة وفي البدالات وفي كيانات الشبكة الأخرى. وعموماً، يمكن نشر القوائم السوداء من شبكة المشغل نفسها في نقطة التحكم في الخدمة، أو البدالات أو كيانات الشبكة الأخرى، في حين لا يمكن نشر القوائم السوداء من شبكات المشغلين الآخرين إلا في مركز التبدل المتنقل للبوابة الذي قد تكون سعة القائمة السوداء فيه أصغر من أن تستوعب تخزين قائمة كبيرة من الأرقام. ولحل هذه المشكلة ببساطة، يمكن استخدام عقد تشوير خفية (انظر الفقرة 1.1.2.7) وراء مركز التبدل المتنقل للبوابة.

وقد تحتاج القوائم البيضاء للتفاعل مع قاعدة البيانات المخوّلة التي يُحتفظ بها لفرز من سبق تحديدهم كمتصلين ذوي صفة مشروعة وخصائص مماثلة لأصحاب الرسائل الاحتمالية الصوتية. فقد يكون هؤلاء المتصلون من مراكز اتصال أو خدمات تبليغ أو خدمات ردود/جمع بيانات كالرسائل التذكيرية بفواتير مستحقة الدفع أو ملاحظات تقييمية على خطط ترعاها الجهات الإدارية، أو برامج توعية، أو برامج متصلة بحالات الطوارئ أو الكوارث، وما إلى ذلك.

2.4.2.7 آلية اقتفاء الآثار

إن آلية اقتفاء الآثار تقتضي الآثار وصولاً إلى الموقع الفعلي الحقيقي لأصحاب الرسائل الاحتمالية الصوتية. وقد يستفاد منها في أوقات معينة لتبيان الموقع أو العنوان الدقيق لصاحب الرسائل الاحتمالية الصوتية إذا لزم الأمر.

ووفقاً للتقنيات القائمة، يمكن للمشغلين تحديد الموقع الحقيقي لصاحب الرسائل الاحتمالية الصوتية على أساس المعلومات التي يقدمها مركز التبدل المتنقل (MSC)؛ سوى أن هذه التقنية لا يمكنها إلا تحديد المنطقة التقريبية. ويمكن الاهتداء إلى معلومات أدق عن الموقع من خدمة معلومات الموقع لدى المشغل، بمساعدة خدمة تحديد المواقع العالمية مثلاً.

3.7 التكنولوجيات من جانب المستخدم

ينبغي أن تكون التكنولوجيات من جانب المستخدم مكتملاً فعلاً للتكنولوجيات من جانب الشبكة. ويمكن لقدر من الملاحظات التقييمية أن يوفر معلومات تفصيلية عن الرسائل الاحتمالية الصوتية (كما يرد بحثه في الفقرة 3.3.7)؛ وهي رديف ذو أهمية خاصة بالنسبة للمشغلين. وقد تحتاج التكنولوجيات من جانب المستخدم إلى مساعدة من ميزات تمتاز بها بعض الهواتف المتنقلة الذكية، والتي يمكن أن يختلف دعمها باختلاف منافذ البيع.

1.3.7 القوائم البيضاء/السوداء

يمكن للمستخدمين الاستفادة من ميزة التحكم في التوصيل ضمن الهواتف لحجب أرقام أو قطاعات أرقام محددة كقوائم سوداء، بينما تسمح ميزة التحكم في التوصيل في الوقت نفسه بفتح الخط دوماً لأرقام معينة (يحددها المستخدمون أو تتزامن عبر بعض التطبيقات المتنقلة) عندما تعادل كقوائم بيضاء.

ويمكن أن ينجح هذا الأسلوب على أساس القائمة البيضاء/القائمة السوداء عندما يتزامن من جانب الشبكة، في حين يخضع جانب المستخدم عادة للتفضيلات الشخصية لأن المستخدمين يمكنهم إدارة قوائمهم الخاصة.

2.3.7 تأخير المكالمات

تأخير المكالمات هو تقنية على مستوى التشوير تنجح في المكالمات الصامتة على وجه التحديد (انظر الفقرة 2.6).

فبعد إقامة وصلة التشوير بين المتصل والمتصل به، ستتولد نغمة الرنين دورياً من الوصلة. وستجرى بعض المكالمات الصامتة وسيتلقى المستخدمون صمتاً ("سكوناً هامداً") أو نغمة تمتد لمدة قصيرة وتشير إلى انقطاع المكالمات.

وبدعم هاتف متنقل ذكي، يمكن للمستخدمين حجب المكالمات الصامتة في جانب المطراف (جانب المستخدم). وبما أن المستخدمين يمكنهم ضبط قيمة مدة النغمة (العتبة) لكل مكالمات واردة في طبقة التشوير، يمكن حذف المكالمات الصامتة حينما تقل مدة النغمة عن العتبة. بيد أن سجل المكالمات سيخزن في قائمة سجل المكالمات على الهاتف المتنقل للسماح للمستخدم بمعاودة التحقق في حالة تجاهل "نغمة رنين قصيرة" لمكالمات عادية.

3.3.7 ملاحظات تقييمية

بعد تلقي رسالة طفيلية صوتية، يمكن للمستخدمين أن يوافقوا المشغلين بملاحظات تقييمية تبين رقم الرسالة الاقتحامية الصوتية ومعلومات تفصيلية أخرى. وتشمل قنوات الملاحظات التقييمية إرسال رسائل نصية ومكالمات هاتفية ورسائل البريد الإلكتروني أو حتى الموقع الرسمي لدائرة خدمة العملاء (أو ما يعادلها من الدوائر الأخرى) لدى المشغلين. وينبغي لجميع القنوات أن توفر للمستخدمين إجراءات ملائمة وسهلة الاتباع كي يدلوا بملاحظاتهم التقييمية. ويمكن إنشاء قناة سهلة الاستخدام بتطبيقات في مطايرف أو بطاقات وحدة تعريف المشترك (SIM) ومنصات مثل منصة إدارة الجهاز (DMP) أو منصة عبر الأثير (OTAP) في الشبكة.

وعلاوة على ذلك، حالما ترد الملاحظات التقييمية إلى دائرة الخدمة لدى المشغلين، ينبغي لمُدقق معتمد أن يتحقق من صحة معلومات الملاحظات التقييمية وفعاليتها، وأن يطبق إجراء تحقق تفاعلي مماثلاً قبل اتخاذ مزيد من الإجراءات المناسبة. وفي حال وجود تسجيل صوتي كدليل من مخدّم البريد الصوتي (VMS) وسماح المالك بالنفذ إلى التسجيل، يمكن أن يكون التحقق أكثر فعالية وأكثر كفاءة.

4.7 آلية التعاون

يمكن للمشغلين أن يتعاونوا مع الجهات الإدارية أو المشغلين الآخرين أو المستخدمين لإنشاء أسلوب مقابل للتعاون والتواصل، من أجل مكافحة الرسائل الاقتحامية الصوتية.

ويمكن للمشغلين أن ينشئوا أو يدعموا نظام تبادل معلومات (ISS). ويمكن لهذا النظام المحدد أن يغطي تبادل المعلومات الأساسية بشأن الرسائل الاقتحامية الصوتية مع المنظمات الأخرى، بما في ذلك قائمة المتصلين الذين يُشبهه بقيامهم/تأكد قيامهم بإرسال الرسائل الاقتحامية الصوتية، وتصنيف كل من الرسائل الاقتحامية الصوتية، وتكنولوجيايات مكافحة، وما إلى ذلك.

ويمكن للجهات الإدارية أن تنظر في تنفيذ نظام تبادل معلومات وإنشاء آلية لتبادل المعلومات أو حتى تنظيم اجتماعات رسمية للمشغلين والمنظمات التي تشكل طرفاً ثالثاً لتبادل أحدث المعلومات.

ويمكن للمستخدمين تبادل القوائم السوداء مع المخدّم في جانب الشبكة برفع أو تنزيل القوائم السوداء. ولكن ينبغي للمشغلين أن يمتلكوا آلية تحقق يمكنهم من خلالها كشف ما إذا كان بند مدرج في قائمة سوداء شخصية هو من أصحاب الرسائل الاقتحامية الصوتية حقاً أم لا. وينبغي للمشغلين أن يوفروا سطحاً بينياً لرفع وتنزيل القوائم السوداء. ويمكن أن تتفاعل هذه الآلية مع ملاحظات العملاء. وفي الوقت نفسه، ينبغي للجهات الإدارية أن تدقق المعلومات المحدّثة لتجنب إدراج معلومات غير مناسبة.

ومن أجل تنفيذ آلية تبادل معلومات، يمكن للمشغلين أن يوافقوا الجهات الإدارية بقوائم سوداء تم التحقق منها، على أساس متكرر، وأن يحجّبوا القوائم السوداء المثبتة التي تُنفذها الجهات الإدارية.

ويمكن للجهات الإدارية أيضاً أن تدمج كل القوائم السوداء التي وردت من جميع المشغلين، وأن تطبق التدابير والإجراءات المناسبة. وبالإضافة إلى ذلك، يمكن للجهات الإدارية أن تتحمل المزيد من المسؤوليات، مثل تقييد الرسالة الاقتحامية الصوتية في المصدر، فيما تتأكد من قيام المشغلين بواجباتهم.

5.7 الحلول المقترحة

لا يمكن لأي من الحلول المذكورة أعلاه أن ينجح بمفرده تماماً. ولمكافحة الرسائل الاقتحامية الصوتية مكافحة فعّالة، ينبغي نشر التكنولوجيايات من جانب الشبكة ومن جانب المستخدم بنحو شامل في كل إجراء.

ومن أجل الحصول على درجة عالية من الدقة، يمكن لإجراء سجل التشوير أن يدمج مصادر البيانات المختلفة معاً. سوى أن تنفيذ مصدر بيانات شامل من شأنه أن يكون مكلفاً للغاية.

وينبغي النظر في الحالات التالية:

فيمكن أن تكون سجلات التشوير رقم 7 بمفردها خياراً (انظر الفقرة 1.2.7) لأن التشوير رقم 7، بالمقارنة مع مصادر البيانات الأخرى، يغطي جميع وصلات التشوير في السعي للحصول على البيانات الأكثر فائدة، من أجل ضمان مكافحة الفعالة للرسالة الاقتحامية الصوتية.

من ناحية أخرى، يمكن أن يكون نظام جمع البيانات على أساس الشبكة الذكية (IN) أو نغمة رنين الاتصال المخصصة (CRBT) أو مخدّم البريد الصوتي (VMS) بديلاً مجزياً من حيث التكلفة، إذا سبق للمشغلين إطلاق خدمات الشبكة الذكية أو نغمة رنين الاتصال المخصصة أو مخدّم البريد الصوتي. إلا أن مصادر البيانات المستقاة من نغمة رنين الاتصال المخصصة أو الشبكة الذكية قد لا تغطي جميع البيانات المحددة التي جاء بحثها في الفقرة 1.2.7. ومن ثم، يمكن أن يكون مصدر البيانات المأخوذ من هذه الخدمات مكتملاً.

ويسهل استخدام النموذج المقترح في الفقرة 2.2.7 وهو ليس مكلفاً؛ ويشجع نشره أيضاً في مكافحة الرسائل الاحتمالية الصوتية. ولزيادة دقة التحليل، يمكن استخدام نماذج وخوارزميات قاعدة أكثر تطوراً. فعلى سبيل المثال، يمكن للإحصاءات عن رموز أسباب فك الاتصال والإحصاءات عن رموز المكالمات المرفوضة أن تقلص كثيراً من قائمة الأرقام المشبوهة.

بيد أن نماذج أو خوارزميات القاعدة الشاملة قد تؤدي إلى درجة عالية من تعقيد النظام وإلى إجراءات تستغرق وقتاً طويلاً، مما يزيد بدوره من تأخير إجراء مكافحة الرسائل الاحتمالية الصوتية بأكمله، الأمر الذي قد يقلل في النهاية من رضا العملاء. وبالنظر إلى كل ذلك، يشكل الاختيار الحكيم لنماذج أو خوارزميات القاعدة السليمة عاملاً مهماً جداً للمشغلين.

وقد يختلف إجراء التحقق التفاعلي من بلد إلى آخر. وبالتالي، يمكن للجهات الإدارية أن تساعد المشغلين في وضع إجراءات التحقق السليم على أساس العرف الوطني.

وكما يتبين من إجراء التحكم الذي ورد وصفه في الفقرة 4.2.7، ينبغي تحسين دمج الأسلوبين من جانب المستخدم ومن جانب الشبكة للتخفيف من كم الرسائل الاحتمالية الصوتية. ويمكن لدائرة خدمة العملاء لدى المشغلين أن تؤدي دوراً هاماً في إجراء التحكم وأن تلي طلبات العملاء.

الملحق A

التدابير التفاعلية والتقنية لمكافحة المكالمات الاقتحامية

(يشكل هذا الملحق جزءاً أساسياً من هذه التوصية.)

ملخص

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

ويوفر هذا الملحق الأساس التقني لمكافحة الرسائل الاقتحامية عندما يقوم المشترك بإخطار المشغل بواسطة مكالمات قصيرة إلى رقم مكافحة الرسائل الاقتحامية بعد تلقي المكالمات الاقتحامية 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 الاقتحامية إلى المطاريف الهاتفية

تعرف التوصية [ITU-T X.1247] بمفهوم آليات التغذية الراجعة للمستعمل وتقارير المستعمل المستخدمة في معالجة الرسائل الاقتحامية. وتعرف التوصية ITU-T X.1246 بآليات تفاعلية مختلفة للتحقق من الرسائل الاقتحامية 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 المكالمات الاقتحامية مع مشغل الاتصالات/مقدم الخدمة في قيام المشترك بمكالمة قصيرة إلى رقم محدد لمكافحة الرسائل الاقتحامية لدى مشغل الاتصالات/مقدم الخدمة أو إعادة توجيه الرسالة الاقتحامية المستلمة إلى هذا الرقم.

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

يشمل سيناريو استخدام طلب رقم مكافحة الرسائل الاقتحامية من أجل تحديد مكالمات اقتحامية باستخدام المعالجة الأوتوماتية للتفاصيل CDR/CLI، الخطوات التالية:

- 1 يستلم المتلقي/العميل/المشترك مكالمات واردة، يحددها على أنها مكالمات اقتحامية أو مكالمات مشبوهة (رسائل صوتية اقتحامية، رسائل اقتحامية في خدمة الرسائل القصيرة أو رسائل اقتحامية في خدمة الرسائل متعددة الوسائط).
- 2 تُخزن المعلومات CDR/CLI بشأن هذه المكالمات (وكذلك بشأن أي مكالمات أخرى) في نظام إدارة الاتصالات (أو في أي نظام آخر/أنظمة أخرى) الخاص بـمشغل الاتصالات. وتحتوي المعلومات CDR_n/CLI_n هذه على معرف هوية المتصل (المصدر المحتمل للمكالمة الاقتحامية)، ومعرف هوية متلقي المكالمات (مستلم المكالمات الاقتحامية) ووقت المكالمات.
- 3 بعد الانتهاء من هذه المكالمات مباشرة/بأسرع ما يمكن، يقوم المتلقي/العميل/المشترك بطلب رقم مكافحة الرسائل الاقتحامية 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 مكالمات صادرة إلى رقم مكافحة الرسائل الاقتحامية 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 الاحتمالية 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 احتمالية محتملة، ويبدأ بجمع معلومات عن الطرف الطالب المحتمل المسؤول عن الرسالة الاحتمالية (وربما يتبادل هذه المعلومات مع مشغلين/منظمين).
- 6 إذا كانت المكالمات إلى رقم مكافحة الرسائل الاحتمالية فريدة و/أو خاطئة، قد لا تكون هناك حاجة إلى مزيد من الخطوات.
- 7 وإذا كان هناك عدة مكالمات موجهة إلى رقم مكافحة الرسائل الاحتمالية، من العديد من المتلقين للمكالمات الاحتمالية المحتملة، وحدد نظام المعالجة CDR، في كل حالة، نفس الرقم طالب النداء أو المعلومات CLI_n لآخر مكالمات واردة إلى المشترك/المستعمل قبل مكالمته الموجهة إلى رقم مكافحة الرسائل الاحتمالية، سيزيد احتمال كشف المصدر الحقيقي للمكالمات الاحتمالية للمساعدة في العثور على المقتحمين.
- 8 من الممكن اختيارياً تحديد عتبات مختلفة لأنظمة المعالجة CDR للقضاء على الإنذارات الزائفة.

2.A المتطلبات التقنية

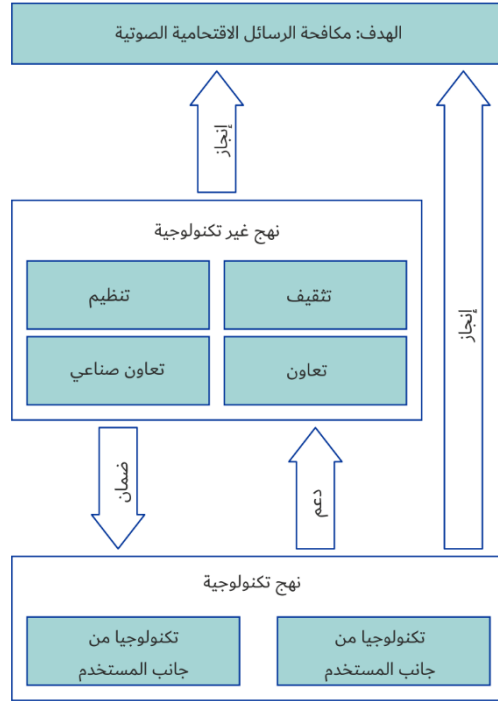
- 1.2.A يُطلب أن يكون لدى مشغل الاتصالات/مقدم الخدمة رقم خاص لمكافحة الرسائل الاحتمالية لاستلام مكالمات التغذية الراجعة من الجهة المتلقية لهذه المكالمات.
- 2.2.A لمعالجة العدد الكبير من مكالمات التغذية الراجعة، يُطلب أن يكون لمشغل الاتصالات/مقدم الخدمة إمكانية استقبال ومعالجة هذه المكالمات بشكل كامل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

التذييل I

تدابير شاملة بشأن مكافحة الرسائل الاحتمالية الصوتية

(لا يشكل هذا التذييل جزءاً أساسياً من هذه التوصية.)

يبين الشكل 1.I هُجماً تكنولوجياً وغير تكنولوجياً لمكافحة الرسائل الاحتمالية الصوتية. وبما أن مكافحة الرسائل الاحتمالية الصوتية ليست مشكلة تقنية بسيطة، ينبغي تطبيق نهج متنوعة معاً:



الشكل 1.I - هيكل مكافحة الرسائل الاحتمالية الصوتية

- يمكن للوائح أن تساعد في حماية المستخدمين والمشغلين من الرسائل الاحتمالية الصوتية.
- تعاون دوائر الصناعة ضروري كي تقوم الجهات المشاركة من أوساط الصناعة بتطوير أنواع مختلفة من التكنولوجيات المناسبة وتركيبها.
- يمكن للتعاون أن يساعد المشغلين والجهات الإدارية في تبادل المعلومات بشأن اعتماد اللوائح وتطوير التكنولوجيا على نحو الفعّال.
- تثقيف المستخدمين مهم لتقليل الخسارة الاقتصادية التي تلحقها الرسائل الاحتمالية الصوتية.

التذييل II

حل مقترح بشأن التحقق التفاعلي

(لا يشكل هذا التذييل جزءاً أساسياً من هذه التوصية.)

ينطوي كل تحقق تفاعلي عموماً على الاتصال برقم متصل يُشتبه به وتسجيل نغمة الرنين قبل التوصيل وتسجيل الصوت بعد التوصيل، وأخيراً تدقيق المحتوى للتحقق مما إذا كان رسالة طفيلية صوتية أم لا. فإذا أجريت كل هذه الخطوات يدوياً، يمكن أن يستنفد ذلك الموارد البشرية للمشغلين بنحو هائل. لذا، يُنظر في نهج أمثل يحقق توازن التكاليف.

ويمكن تشغيل التحقق التفاعلي بطريقة مركزية لمراقبة السجلات والتدقيق شبه التلقائي للنسخ الصوتية لمن يُشتبه بكونهم من أصحاب الرسائل الاحتمالية الصوتية، المتناثرين ربما في كل ركن من أركان الشبكة.

فينفذ النهج المركزي وظيفة المراقبة والتسجيل تلقائياً بدرجة عالية من التزامن، ومن شأنه أن يحد من تدقيق المدققين في النسخ الصوتية الناجحة الخالية من الضوضاء البيضاء وغيرها من نغمات الرنين عديمة الفائدة.

التذييل III

اعتبارات السياسة العامة في مجال مكافحة الرسائل الاقتحامية الصوتية

(لا يشكل هذا التذييل جزءاً أساسياً من هذه التوصية.)

الرسائل الاقتحامية الصوتية هي أداة خطيرة تُستخدم للإعلان وارتكاب الاحتيال والمضايقة وغير ذلك، ويمكن أن تصادف في الاتصالات اليومية. ومن أجل مكافحة الرسالة الاقتحامية الصوتية على نحو فعال، ينبغي النظر في مختلف نُهج الجوانب المتنوعة للمجموعات المشاركة وفي الأنماط المتنوعة للتكنولوجيات المقدمة في هذه التوصية. والمجموعات المشاركة هي المستخدمون (أو المشتركون) والمشغلون والجهات الإدارية والمنظمات التي تشكل طرفاً ثالثاً. ومن ثم، يصف هذا التذييل عدة جوانب للمجموعات المشاركة ينبغي النظر فيها لدى مكافحة الرسالة الاقتحامية الصوتية.

1.III المستخدمون

المستخدمون هم الضحايا النهائيون في سلسلة اتصالات الرسائل الاقتحامية الصوتية، ولذلك يحدوهم حافز كبير لحجب الرسائل الاقتحامية. وبالتالي، ينبغي للمستخدمين تنفيذ بعض الأساليب المطبقة في كامل عملية مكافحة الرسائل الاقتحامية. وتشمل النهج المقترحة التي قد تختلف حسب الموقف ما يلي:

- ينبغي للمستخدمين تثبيت تطبيقات مكافحة الرسائل الاقتحامية على الأجهزة التي بحوزتهم، كالهواتف المتنقلة الذكية، إذا أمكن ذلك. وفعالية أفضل، يجب أن يواكب تطبيق مكافحة الرسائل الاقتحامية آخر التحديثات.
- ينبغي للمستخدمين أن يوافقوا مشغلي الاتصالات أو المنظمات التي تشكل طرفاً ثالثاً بجميع المعلومات التفصيلية عن مرسل الرسالة الاقتحامية الصوتية بمجرد تلقيها.
- ينبغي للمستخدمين أن يتوخوا قدرماً أكبر بكثير من الحرص في الاتصالات اليومية على عدم إفشاء المعلومات الشخصية لأصحاب الرسائل الاقتحامية الصوتية.

2.III المشغلون

يشكل المشغلون الجهات الفاعلة الهامة في كامل إجراء مكافحة الرسالة الاقتحامية الصوتية. ولئن أمكن للرسائل الاقتحامية الصوتية أن تتسبب بتهاوي معدلات رضا المستخدمين ويهدر كبير لموارد الشبكة، ينبغي أن يتنبه المشغلون للرسائل الاقتحامية الصوتية وأن ينفذوا نُهجاً لحماية شبكاتهم وتقديم خدمات أفضل. وقد تشمل هذه النهج ما يلي:

- وينبغي أن يراقب المشغلون شبكة الاتصالات برمتها لكشف الرسائل الاقتحامية الصوتية المحتملة التي يمكن أن تتسبب بشذوذ إرسالات التشوير أو أنماط الحركة.
- وينبغي أن يثبت المشغلون مسبقاً أحدث نسخة من تطبيقات مكافحة الرسائل الاقتحامية في جميع الأجهزة التي يمكن أن تُستهدف بالرسائل الاقتحامية الصوتية من خلال قنوات التوزيع أو البيع الخاصة بهم. وبالنسبة لقنوات التوزيع عبر طرف ثالث، ينبغي أن يضمن المشغلون حماية جميع الأجهزة حماية كاملة بأحدث التطبيقات.
- وينبغي للمشغلين أن يقوموا بحملات توعية وتدريب وأن يشجعوا المستخدمين على الإدلاء بملاحظات تقييمية بشأن الرسائل الاقتحامية الصوتية عن طريق تقديم معلومات تفصيلية لمنظمات تشكل طرفاً ثالثاً؛ ويمكن تنشيط هذه الملاحظات التقييمية ببرامج حوافز.
- وينبغي إشراك المشغلين في بناء تحالفات مع الجهات الإدارية والمنظمات التي تشكل طرفاً ثالثاً كي تتضافر الجهود في مكافحة الرسائل الاقتحامية الصوتية.

3.III الجهات الإدارية والمنظمات التي تشكل طرفاً ثالثاً

يمكن للجهات الإدارية والمنظمات التي تشكل طرفاً ثالثاً أن تشرف على المشغلين أو توجههم مباشرة، بل وأن تزودهم بالدعم الضروري:

- يمكن للجهات الإدارية والمنظمات التي تشكل طرفاً ثالثاً أن تدرب المستخدمين والمشغلين أو تقوم بحملات توعية وتدريب لهم لمكافحة الرسائل الاقتحامية الصوتية.
- وينبغي للجهات الإدارية والمنظمات التي تشكل طرفاً ثالثاً أن تجري المزيد من الأبحاث بشأن اتجاهات الرسائل الاقتحامية الصوتية وينبغي أن تسعى إلى إيجاد نهج أو تكنولوجيات مكافحة أكثر فعالية للتصدي لآخر أنماط الرسائل الاقتحامية الصوتية.
- وينبغي للجهات الإدارية والمنظمات التي تشكل طرفاً ثالثاً أن تكسر الجمود الذي يعترض قنوات الإعلان أو الترويج لتطبيع بيئة الاتصالات الصوتية الحالية، أو أن تنظم أنظمة الاتصالات الإعلانية المجازة للجهة العاملة في مجال الترويج.
- وينبغي للجهات الإدارية والمنظمات التي تشكل طرفاً ثالثاً أن تُطلع المشغلين وحتى المستخدمين على أحدث القوائم السوداء؛ وينبغي أن تدار هذه القوائم السوداء بدعم من المشغلين والمستخدمين.
- وينبغي للجهات الإدارية أن تقدم الموارد اللازمة لتعزيز قوة مكافحة الرسائل الاقتحامية الصوتية في إطار الحماية المقدمة كجزء من مزايا العرض التجاري للمستخدمين.

بييليوغرافيا

- [[b-ITU-T E.370](#)] Recommendation ITU-T E.370 (2001), *Service principles when public circuit-switched international telecommunication networks interwork with IP-based networks*.
- [[b-ITU-T M.60](#)] Recommendation ITU-T M.60 (1993), *Maintenance terminology and definitions*.
- [[b-ITU-T M.1400](#)] Recommendation ITU-T M.1400 (2015), *Designations for interconnections among operators' networks*.
- [[b-ITU-T X.1231](#)] Recommendation ITU-T X.1231 (2008), *Technical strategies for countering spam*.
- [[b-ITU-T X.1242](#)] Recommendation ITU-T X.1242 (2009), *Short message service (SMS) spam filtering system based on user-specified rules*.
- [[b-ITU-T X.1245](#)] Recommendation ITU-T X.1245 (2010), *Framework for countering spam in IP-based multimedia applications*.
- [[b-ITU-T Y.1001](#)] Recommendation ITU-T Y.1001 (2000), *IP framework – A framework for convergence of telecommunications network and IP network technologies*.
- [b-IETF RFC 5039] IETF RFC 5039 (2008), *The Session Initiation Protocol (SIP) and Spam*.

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