الاتحـــــــــاد الدولـــــــــي للاتصـــــــــالات

ITU-T

قطاع تقييس الاتصالات
في الاتحاد الدولي للاتصالات

X.1246
(2015/09)

السلسلة X: شبكات البيانات، والاتصالات بين الأنظمة المفتوحة ومسائل الأمن

أمن الفضاء السيبراني – مكافحة الرسائل الاقتحامية

التكنولوجيات المشاركة في مكافحة الرسائل الاقتحامية الصوتية في منظمات الاتصالات

التوصية ITU-T X.1246

الاتحاد الدولي للاتصالات

توصيات السلسلة X الصادرة عن قطاع تقييس الاتصالات

شبكات البيانات والاتصالات بين الأنظمة المفتوحة ومسائل الأمن

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

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

التكنولوجيات المشاركة في مكافحة الرسائل الاقتحامية الصوتية في منظمات الاتصالات

ملخص

الاتصالات الصوتية خدمة أساسية تقدمها شبكات الاتصالات. ومع تطور الاتصالات الصوتية، تزايدت أيضاً الرسائل الاقتحامية الصوتية وما يترتب عليها من آثار سلبية متعددة على المستعملين النهائيين ومشغلي الشبكات. وتشمل الرسائل الاقتحامية الصوتية بصورة عامة محتوى يتراوح بين الإعلانات التجارية والمواد الإباحية المسيئة التي تؤدي إلى آثار سلبية مختلفة على المستعملين النهائيين ومشغلي الشبكات. ويمكن أن تتسبب الرسائل الاقتحامية الصوتية في إغواء أو إزعاج أو مضايقة أو حتى تخويف المستعملين 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 الاقتحامية الصوتية.

والغرض من التوصية ITU-T X.1246 هو استعراض الحلول التقنية لمكافحة الرسائل الاقتحامية الصوتية دون اعتبار المخاطر التي تنطوي عليها حقيقة هوية الجهة المتطفلة. وتعطي هذه التوصية لمحة عامة عن الرسائل الاقتحامية الصوتية وتلخص التكنولوجيات الحالية لمكافحة الرسائل الاقتحامية التي يستخدمها المستعملون النهائيون وشبكات الاتصالات على السواء وكذلك آليات التعاون فيما بينهم. ويوصى أيضاً بحلول تقنية إضافية مقترحة استناداً إلى التكنولوجيات وآليات التعاون هذه المضادة للرسائل الاقتحامية.

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

الكلمات الأساسية

الرسائل الاقتحامية، الرسائل الاقتحامية الصوتية.

* للنفاذ إلى التوصية، اطبع العنوان الإلكتروني: http://handle.itu.int/ في حقل العنوان من متصفح الويب الذي تستعمله، متبوعاً بمعرف الهوية الفريد للتوصية. ومثال على ذلك http://handle.itu.int/11.1002/1000/11830-en.

تمهيد

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

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

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

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

ملاحظة

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

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

حقوق الملكية الفكرية

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

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

جدول المحتويات

الصفحة

التكنولوجيات المشاركة في مكافحة الرسائل الاقتحامية الصوتية في منظمات الاتصالات

1 مجال التطبيق

تقدم هذه التوصية لمحة عامة عن الرسائل الاقتحامية الصوتية وتستعرض التقنيات القائمة المستخدمة للمساعدة في مكافحة الرسائل الاقتحامية الصوتية، بما في ذلك التكنولوجيات من جانب شبكة ومن جانب المستخدم وآلية التعاون بينهما. وبالإضافة إلى ذلك، تقترح هذه التوصية أيضاً حلولاً إضافية عملية لمكافحة الرسائل الاقتحامية، مثل سجلات التشوير والتحقق التفاعلي وتدابير التحكم، وما إلى ذلك.

وتركز هذه التوصية حصراً على مكافحة الرسائل الاقتحامية الصوتية الصادرة من حيز تبديل الدارات في شبكات الاتصالات مع مراعاة محددة لخصائص البنية التحتية للشبكة. أما تكنولوجيات مكافحة الرسائل الاقتحامية 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.

وتنبغي مراعاة الامتثال للقوانين والتشريعات ذات الصلة كافة قبل اعتماد أساليب مكافحة الرسائل الاقتحامية 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 يضفي على الوثيقة في حد ذاتها صفة التوصية.

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

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

3 التعاريف

1.3 المصطلحات المعرَّفة في وثائق أخرى

تستخدم هذه التوصية المصطلحات التالية المعرَّفة في وثائق أخرى:

1.1.3 شبكة عاملة بتبديل الدارات [b-ITU-T M.60]: شبكة توفر توصيلات لاستخدام المستخدمين الحصري طوال مدة مكالمة 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 المشغِّل [b-ITU-T M.1400]: عبارة عن منظمة مسؤولة عن تحديد هوية موارد الاتصالات وإدارتها. ويجب أن يكون هذا المشغل معترف به قانوناً من جانب إدارة الاتصالات الموجودة في البلد، أو الوفد المعني بذلك. وقد يُقصد بالمشغل أحد الشركاء التجاريين أو لا يُقصد به ذلك.

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 المعرَّفة في هذه التوصية

تعرِّف هذه التوصية المصطلحات التالية:

1.2.3 الرسائل الاقتحامية الصوتية: مكالمات هاتفية مسجلة مسبقاً تُرسَل 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 تتنوع الآثار الضارة للرسائل الاقتحامية الصوتية على المستخدمين والمشغلين.

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

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

4 المختصرات والأسماء المختصرة

تستعمل هذه التوصية المختصرات والأسماء المختصرة التالية:

CAMEL تطبيقات على مقاس 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)*

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)*

ID تحديد الهوية *(Identification)*

ISIS نظام تبادل المعلومات *(Information Sharing System)*

IMS نظام فرعي متعدّد الوسائط قائم على بروتوكول الإنترنت *(IP Multimedia Subsystem)*

IN شبكة ذكية *(Intelligent Network)*

INAP بروتوكول تطبيق شبكة ذكية *(Intelligent Network Application Protocol)*

IP بروتوكول الإنترنت *(Internet Protocol)*

IVR رد صوتي تفاعلي *(Interactive Voice Response)*

MSC مركز تبديل متنقل *(Mobile Switching Centre)*

OTAP منصة عبر الأثير *(Over- the- Air Platform)*

PSTN الشبكة الهاتفية العمومية التبديلية *(Public -Switched Telephone Network)*

SCP نقطة تحكم في الخدمة *(Service Control Point)*

SIM وحدة هوية المشترك *(Subscriber Identity Module)*

SLETP النقطة الزمنية لإقامة وصلة التشوير *(Signalling Link Establishment Time Point)*

SLRTP النقطة الزمنية لفك وصلة التشوير *(Signalling Link Release Time Point)*

SS7 نظام التشوير رقم 7 *(Signalling System No.7)*

STP نقطة نقل التشوير *(Signalling Transfer Point)*

UMTS نظام الاتصالات المتنقلة الشامل *(Universal Mobile Telecommunications System)*

VLR سجل موقع الزائر *(Visitor Location Register)*

VMS مخدِّم البريد الصوتي *(Voice Mail Server)*

VoIP الاتصالات الصوتية عبر بروتوكول الإنترنت *(Voice over Internet Protocol)*

5 الاصطلاحات

لا توجد.

6 لمحة عامة عن الرسائل الاقتحامية الصوتية

الرسائل الاقتحامية الصوتية هي مكالمات هاتفية مسجلة مسبقاً تُرسَل 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. وتتعدد الآثار الضارة للرسائل الاقتحامية الصوتية بأنواعها المختلفة على المستخدمين والمشغلين.

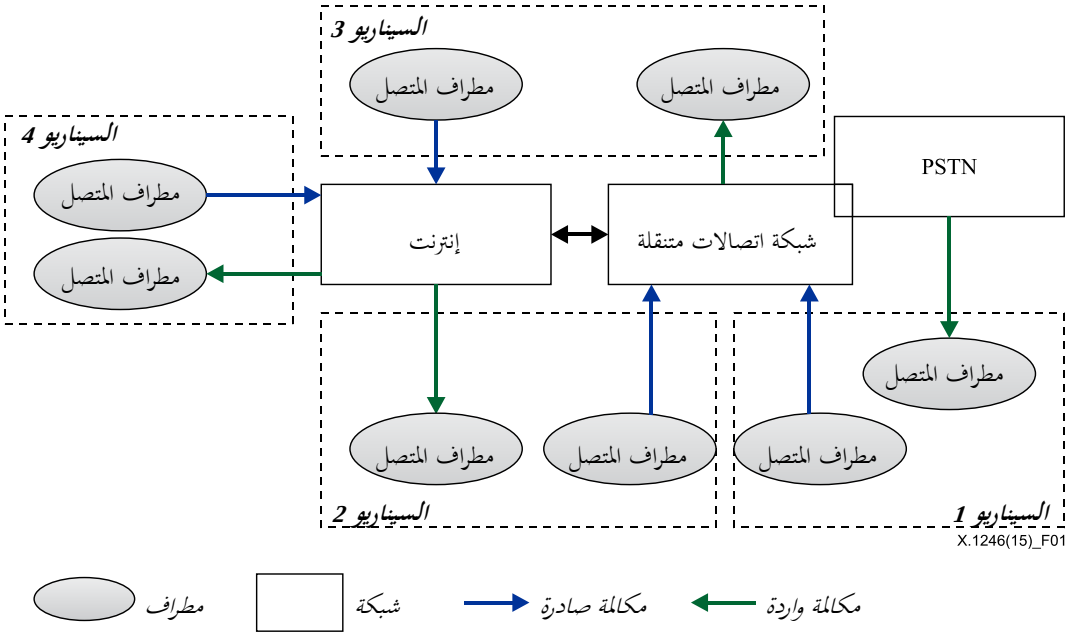
1.6 سيناريوهات الاتصالات الصوتية

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 ببروتوكول الإنترنت.
- السيناريو 3: IP-CS: اتصالات صوتية تصدر عن مستخدم مهاتفة عاملة ببروتوكول الإنترنت وتنتهي عند مستخدم اتصالات متنقلة/ثابتة بتبديل الدارات.
- السيناريو 4: IP-IP: اتصالات صوتية بين مستخدمي مهاتفة عاملة ببروتوكول 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 مطراف المبين هنا في الشكل رقم 1، هواتف متنقلة وهواتف ثابتة وحواسيب محمولة وحواسيب شخصية، وما إلى ذلك، مما يمكّنه من النفاذ إلى شبكات الاتصالات بتبديل الدارات/القائمة على بروتوكول الإنترنت. وبصفة عامة، فإن معظم المستخدمين يثقون بمصدر الاتصالات الصوتية. ونتيجة لذلك، فإن أصحاب الرسائل الاقتحامية الصوتية على استعداد لاستخدام الاتصالات الصوتية 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 مملة أو خادعة أو محتويات تنطوي على ترهيب 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 الاقتحامية الصوتية الأكثر رواجاً في نمطين دون الاقتصار عليهما:

- **النمط الأول (المكالمة الصامتة)**: المكالمة الصامتة هي مكالمة هاتفية بقصد التسويق عبر الهاتف تتولد بمهاتِف تنبؤي (أو مهاتِفات تنبؤية) دون نية الوكيل أن يتعامل مع هذه المكالمة على الفور. وفي هذه الحالة، يمكن للمهاتف إنهاء المكالمة، فيسمع الطرف الذي اتُصل 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 جوابية.
- **النمط الثاني (المكالمة اللجوجة)**: مكالمة هاتفية بقصد التسويق عبر الهاتف يمكنها كذلك أن تلح أو تزعج أو تفزع 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 تكنولوجيات مكافحة الرسائل الاقتحامية الصوتية

1.7 الجوانب العامة

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

وللتوصية بتكنولوجيات 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 للمطاريف. ويمكن تصنيف التكنولوجيات الموصى بها كتكنولوجيات من جانب الشبكة وتكنولوجيات من جانب المستخدم.

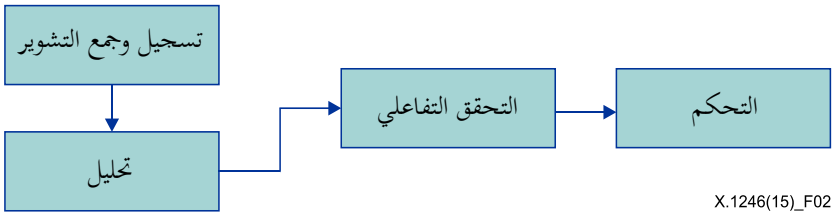
والتكنولوجيات من جانب الشبكة هي تكنولوجيات أساسية للمشغلين، أي في الشبكات الهاتفية العمومية التبديلية (PSTN) وأنظمة الاتصالات المتنقلة الشاملة (UMTS) ونظام الاتصالات المتنقلة العالمي (GSM) وشبكات النفاذ المتعدد بتقسيم شفري (CDMA). وبالمقارنة مع التكنولوجيات من جانب الشبكة، فإن التكنولوجيات من جانب المستخدم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

2.7 التكنولوجيات من جانب الشبكة

تُنشأ كل مكالمة هاتفية في شبكة النفاذ بالتشوير. ولكشف من يُشتبه 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 المهاتف هو تحديد الهوية (ID) الوحيد للمهاتف/الطرف المتصَل 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:



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 أياً 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 تُجمَع معاً.

وستعرَّف 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 المكالمة جمعاً (شبه) آني للتحليل، ويمكن أن يشمل ذلك بيانات ذات صلة بالوقت أو ذات صلة برقم الهاتف، مثل:

- النقطة الزمنية لإنشاء المكالمة (COTP): نقطة زمنية يبادر فيها متصل إلى إجراء مكالمة هاتفية.
- النقطة الزمنية لإقامة وصلة التشوير (SLETP): النقطة الزمنية لإقامة وصلة التشوير بين متصِل ومتصَل به.
- النقطة الزمنية لاستمرار المكالمة (CCOTP): النقطة الزمنية لاستمرار مكالمة هاتفية وفتح المتصَل به لخط الاتصال.
- النقطة الزمنية لإجازة المكالمة (CCLTP): النقطة الزمنية لإجازة المكالمة من جانب متصِل أو متصَل به.
- النقطة الزمنية لفك وصلة التشوير (SLRTP): النقطة الزمنية لفك وصلة التشوير بعد إجازة مكالمة.
- رقم المشترك المنشئ للمكالمة (COSN): يُعرف عادة برقم المتصِل، أي الرقم الذي بادر متصِل منه إلى إجراء مكالمة.
- رقم المشترك الذي ينهي المكالمة (CTSN): يُعرف عادة برقم المتصَل به، أي الرقم الذي منه أنهى متصَل به المكالمة.

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 متعدّد الوسائط قائم على بروتوكول الإنترنت (IMS) ونغمة رنين الاتصال المخصصة (CRBT) ومخدِّم 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. وتمكن الاستفادة عملياً من إدخال نقطة جمع التشوير لتكرار معلومات ومعلمات نقطة جمع التشوير وتسجيلها. وتوصَل نقطة جمع التشوير على التوازي مع وصلة التشوير بحيث تصبح الإشارة فعلياً "حزمة مفلوقة"، 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 عقدتي تشوير صريحتين. وهذا يعني أن عقدة التشوير الخفية "ستعيق" الإشارة أولاً كي تسجلها ثم ترحِّلها دون أي تغيير ولكن بفارق كمون بسيط. غير أن هذه التكنولوجيا تنطوي على مخاطر تعطل نقطة واحدة. لذا تلزم قدرة موثوقة لتجاوز الأعطال وتوفر 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، ستُشمل 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 تحكم في الخدمة (SCP) لجمع تطبيقات على مقاس منطق الاتصالات المتنقلة المعزز (CAMEL) أو تشوير بروتوكول تطبيق الشبكة الذكية (INAP) من أجل التحليل. ونقطة التحكم في الخدمة هي عقدة رئيسية في الشبكة الذكية (IN) وعامل محدد في اتخاذ قرار بشأن كيفية معالجة المكالمات الهاتفية.

وحالما يتعاقد مستخدم على خدمة الشبكة الذكية، ستحرك المكالمات الصادرة نقطة التحكم في الخدمة للاستفسار عن معلومات سجل موقع زائر المستخدم (VLR) المتصَل 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 تحكم 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 يراقَب سوى جزء صغير من سلوكيات المستخدمين. إلا أن هذا الوضع يمكن حله من خلال مساعدة كل مستخدم في الاكتتاب ضمناً في خدمة مفصلة على مقاسه من خدمات الشبكة الذكية؛ خدمة ستحيل طلب الاستفسار دون شروط إلى نقطة التحكم في الخدمة عند إنشاء المكالمة الصادرة.

وهذا الأسلوب مقيد بالإجراءات الشائعة لخدمة الشبكة الذكية؛ لذلك لا يمكن جمع إلا أنماط بيانات محدودة، مثل COTP وSLETP وCOSN وCTSN (انظر الفقرة 1.2.7). ومع ذلك هناك متسع للتحسين إذا أُدخلت إجراءات أكثر تعقيداً في خدمة الشبكة الذكية، كأن ترحِّل 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 وCCOTP وCCLTP وCOSN وCTSN (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 مخدِّمات البريد الصوتي (VMS)

تتعامل مخدِّمات البريد الصوتي (VMS) مع المكالمات في أوضاع إعادة تسيير المكالمة في حالة عدم الرد وإعادة تسيير المكالمة في حالة انشغال الخط وإعادة تسيير المكالمة غير المشروطة، وما إلى ذلك. وفي معظم الحالات، لا يرد مخدِّم البريد الصوتي على مكالمة صامتة إلا إذا كان المعيار غير مشروط. ويمكن لمخدِّم البريد الصوتي أن يوفر تسجيلات صوتية لطرف متصِل إذا نوى المتصل صاحب الرسالة الاقتحامية الصوتية توصيل مكالمته ورسالته الاقتحامية الصوتية إلى المتصَل به مباشرة، وفي هذه الحالة يمكن لمخدِّم 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 مخدِّم البريد الصوتي شرط مسبق لجعل هذا الأسلوب عملياً.

5.1.2.7 المصيدة

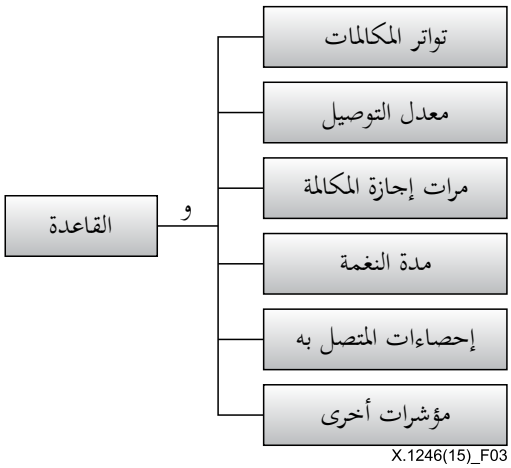
يُستخدم أسلوب المصيدة لإعداد كمية من أرقام الهواتف المتعاقبة أو العشوائية لجذب أصحاب الرسائل الاقتحامية الصوتية. وإلى جانب جمع البيانات، يمكن لأسلوب المصيدة أيضاً أن يسهل إجراء التحليل فضلاً عن إجراء التحقق التفاعلي.

وبما أن أي متصل يمكنه وضع أسلوب المصيدة على الخط (مكالمات صادرة)، يمكن بهذا الأسلوب جمع بعض الأنواع المعينة من البيانات، مثل COTP وCCOTP وCCLTP وCOSN وCTSN، 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 جُمع من البيانات الأصلية وتحويله إلى مؤشرات ذات مغزى مثل معدل التوصيل ووقت فك المكالمة 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، ولإسناد 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 المكالمة أو إنشاء وصلة التشوير.
- مرات إجازة المكالمة: عدد المرات التي يجيز فيها المتصل أو المتصَل به المكالمة من تلقاء نفسه.
- مدة النغمة: المدة الزمنية لنغمة الرنين.
- إحصاءات المتصَل به: إحصاءات عن خصائص المتصَل به، مثل التوزيع المنتظم والمتوالية 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 لتتناسب مع أنواع مختلفة من الرسائل الاقتحامية الصوتية.

على سبيل المثال، هناك نمطان معروفان على نطاق واسع من الرسائل الاقتحامية الصوتية وهما: المكالمات الصامتة والمكالمات اللجوجة، انظر الفقرة 2.6. والمكالمة الصامتة (تسمى أيضاً المكالمة المهجورة) هي مكالمة هاتفية يجريها مهاتف، لا وكيل متاح لديه على الفور، لمعالجة المكالمة. وفي هذه الحالة، يمكن للمهاتف إنهاء المكالمة، فيسمع الطرف الذي اتُصل به صمتاً ("سكوناً هامداً") أو نغمة من شركة الهاتف تشير إلى انقطاع المكالمة. وعادة، يتوقع هذا النوع من المكالمات مكالمة جوابية. أما المكالمة اللجوجة فهي مكالمة هاتفية تقصد أن تلح أو تزعج أو تفزع 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 المكالمة.

ويمكن أن تُظهر المكالمات الصامتة والمكالمات اللجوجة (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 يلوحا أدعى للشك بصاحب رسالة طفيلية صوتية صامتة. ومن ناحية أخرى، قد تركز مكالمة لجوجة على متلقٍ محدد للمكالمة؛ 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 مفيد للتحليل التأكد مما إذا فتح المتصلون المشبوهون 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 للفوترة، 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، اذا سمح اتفاق خدمة المستخدم أو الجهات الإدارية بذلك، يمكن أن يقوم المشغل بإجراء اختبار مراقمة على رقم متصل مدرج في القوائم المشبوهة من أجل الحصول على تحقق مباشر. وباستخدام نتائج اختبار المراقمة، 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 المكالمة الصادرة هي مكالمة صامتة (انظر الفقرة 2.6)، سترد المصيدة بمكالمة لإثبات أدلة التحقق؛ وفي المقابل، عند تأكيد مكالمة 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. ويناقَش 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 وفعاليته. 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 القوائمَ السوداء أخطاءٌ تمنع بعض المكالمات المشروعة من الوصول إلى مستقبليها. وعلى الرغم من أن استخدامها يثير العديد من المخاوف، تقدم القوائم السوداء حلاً سريعاً يحول دون توصيل مصادر الرسائل الاقتحامية الصوتية بمستقبليها (من مستخدمي الهاتف).

وتُنشر عادة قوائم سوداء تتضمن أرقام أو قطاعات أرقام المستخدم في مركز التبديل 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 التبديل 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 التبديل المتنقل للبوابة.

وقد تحتاج القوائم البيضاء للتفاعل مع قاعدة البيانات المخوَّلة التي يُحتفظ بها لفرز من سبق تحديدهم كمتصلين ذوي صفة مشروعة وخصائص مماثلة لأصحاب الرسائل الاقتحامية 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 تقتفي الآثار وصولاً إلى الموقع الفعلي الحقيقي لأصحاب الرسائل الاقتحامية الصوتية. وقد يستفاد منها في أوقات معينة لتبيان الموقع أو العنوان الدقيق لصاحب الرسائل الاقتحامية الصوتية إذا لزم الأمر.

ووفقاً للتقنيات القائمة، يمكن للمشغلين تحديد الموقع الحقيقي لصاحب الرسائل الاقتحامية الصوتية على أساس المعلومات التي يقدمها مركز التبديل 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 مكملاً فعّالاً للتكنولوجيات من جانب الشبكة. ويمكن لقدر من الملاحظات التقييمية أن يوفر معلومات تفصيلية عن الرسائل الاقتحامية 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 تعامَل 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 المكالمة

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

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

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

3.3.7 ملاحظات تقييمية

بعد تلقي رسالة طفيلية صوتية، يمكن للمستخدمين أن يوافوا المشغلين بملاحظات تقييمية تبين رقم الرسالة الاقتحامية الصوتية ومعلومات تفصيلية أخرى. وتشمل قنوات الملاحظات التقييمية إرسال رسائل نصية ومكالمات هاتفية ورسائل بالبريد 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 مطاريف أو بطاقات وحدة تعريف المشترك (SIM) ومنصات مثل منصة إدارة الجهاز (DMP) أو منصة عبر الأثير (OTAP) في الشبكة.

وعلاوةً على ذلك، حالما ترد الملاحظات التقييمية إلى دائرة الخدمة لدى المشغلين، ينبغي لمدقق 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 مخدِّم البريد الصوتي (VMS) وسماح المالك بالنفاذ 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 يُشتبه بقيامهم/تأكدَ قيامهم بإرسال الرسائل الاقتحامية الصوتية، وتصنيف كل من الرسائل الاقتحامية الصوتية، وتكنولوجيات المكافحة، 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 المخدِّم 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 المحدَّثة لتجنب إدراج معلومات غير مناسبة.

ومن أجل تنفيذ آلية تبادل معلومات، يمكن للمشغلين أن يوافوا الجهات الإدارية بقوائم سوداء تم التحقق منها، على أساس متكرر، وأن يحجبوا القوائم السوداء المثْبتة التي تُنْفِذها 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 التكنولوجيات 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 شانه 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 المكافحة 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 مخدِّم البريد الصوتي (VMS) بديلاً مجزياً من حيث التكلفة، إذا سبق للمشغلين إطلاق خدمات الشبكة الذكية أو نغمة رنين الاتصال المخصصة أو مخدِّم 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 مكملاً.

ويسهل استخدام النموذج المقترح في الفقرة 2.2.7 وهو ليس مكلفاً؛ ويشيع نشره أيضاً في مكافحة الرسالة الاقتحامية 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 الرسالة الاقتحامية 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.

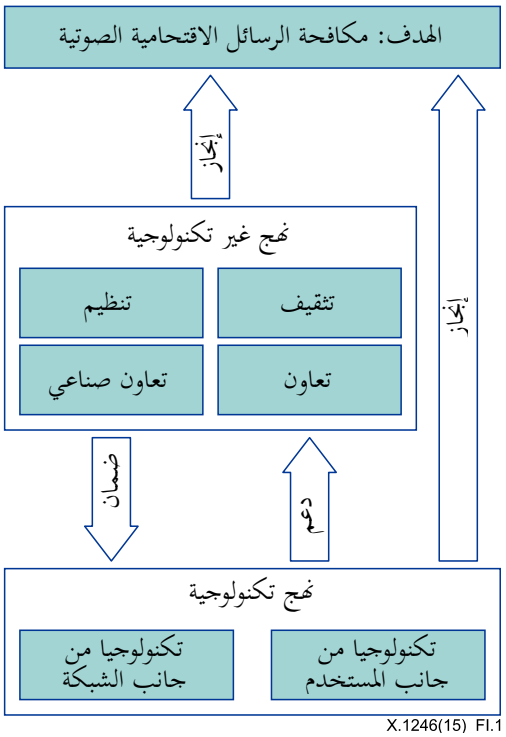
وكما يتبين من إجراء التحكم الذي ورد وصفه في الفقرة 4.2.7، ينبغي تحسين دمج الأسلوبين من جانب المستخدم ومن جانب الشبكة للتخفيف من كم الرسائل الاقتحامية الصوتية. ويمكن لدائرة خدمة العملاء لدى المشغلين أن تؤدي دوراً هاماً في إجراء التحكم وأن تلبي طلبات العملاء.

التذييل I

تدابير شاملة بشأن مكافحة الرسائل الاقتحامية الصوتية

(لا يشكل هذا التذييل جزءاً أساسياً من هذه التوصية)

يبين الشكل 1.I نُهُجاً تكنولوجية وغير تكنولوجية لمكافحة الرسائل الاقتحامية الصوتية. وبما أن مكافحة الرسائل الاقتحامية الصوتية ليست مشكلة تقنية بسيطة، ينبغي تطبيق نهج متنوعة معاً:



الشكل 1.I – هيكل مكافحة الرسائل الاقتحامية الصوتية

- يمكن للوائح أن تساعد في حماية المستخدمين والمشغلين من الرسائل الاقتحامية 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 الاقتحامية 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 لمراقمة السجلات والتدقيق شبه التلقائي للنسخ الصوتية لمن يُشتبه بكونهم من أصحاب الرسائل الاقتحامية الصوتية، المتناثرين ربما في كل ركن من أركان الشبكة.

فينفذ النهج المركزي وظيفة المراقمة والتسجيل تلقائياً بدرجة عالية من التزامن، ومن شأنه أن يحصر 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 تصادَف في الاتصالات اليومية. ومن أجل مكافحة الرسالة الاقتحامية الصوتية على نحو فعّال، ينبغي النظر في مختلف نُهُج 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 النُهُج 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. ولفعالية أفضل، يجب أن يواكب تطبيق مكافحة الرسائل الاقتحامية آخر التحديثات.
- ينبغي للمستخدمين أن يوافوا مشغلي الاتصالات أو المنظمات التي تشكل طرفاً ثالثاً بجميع المعلومات التفصيلية عن مرسل الرسالة الاقتحامية الصوتية بمجرد تلقيها.
- ينبغي للمستخدمين أن يتوخوا قدراً 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 وبهدر كبير لموارد الشبكة، ينبغي أن يتنبه المشغلون للرسائل الاقتحامية الصوتية وأن ينفذوا نُهُجاً لحماية شبكاتهم وتقديم خدمات أفضل. وقد تشمل هذه النُهُج 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 يعتري 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 المقدَمة كجزء من مزايا العرض التجاري للمستخدمين.

بيبليوغرافيا

[b-ITU-T E.370] التوصية ITU-T E.370 (2001)، *قواعد الخدمة في حالة تشغيل شبكات اتصالات دولية عمومية تعمل بتبديل الدارات مع الشبكات القائمة على بروتوكول الإنترنت*.

[b-ITU-T M.60] التوصية ITU-T M.60 (1993)، *مصطلحات الصيانة وتعاريفها*.

[b-ITU-T M.1400] التوصية ITU-T M.1400 (2015)، *تسمية التوصيلات البينية فيما بين شبكات المشغلين*.

[b-ITU-T X.1231] التوصية ITU-T X.1231 (2008)، *استراتيجيات تقنية لمكافحة الرسائل الاقتحامية*.

[b-ITU-T X.1245] التوصية ITU-T X.1245 (2010)، *إطار لمكافحة الرسائل الاقتحامية في التطبيقات متعددة الوسائط القائمة على بروتوكول الإنترنت*.

[b-ITU-T Y.1001] التوصية ITU-T Y.1001 (2000)، *إطار بروتوكول الإنترنت – إطار لتقارب تكنولوجيات شبكة الاتصالات والشبكة العاملة ببروتوكول الإنترنت*.

[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	المبادئ العامة للتعريفة
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، تغير المناخ، المخلفات الإلكترونية، كفاءة الطاقة، إنشاء الكبلات وغيرها من عناصر المنشآت الخارجية وتركيبها وحمايتها
السلسلة M	إدارة الاتصالات بما في ذلك شبكة إدارة الاتصالات (TMN) وصيانة الشبكات
السلسلة N	الصيانة: الدارات الدولية لإرسال البرامج الإذاعية الصوتية والتلفزيونية
السلسلة O	مواصفات تجهيزات القياس
السلسلة P	المطاريف وطرائق التقييم الذاتية والموضوعية
السلسلة Q	التبديل والتشوير
السلسلة R	الإرسال البرقي
السلسلة S	التجهيزات المطرافية للخدمات البرقية
السلسلة T	المطاريف الخاصة بالخدمات التليماتية
السلسلة U	التبديل البرقي
السلسلة V	اتصالات البيانات على الشبكة الهاتفية
السلسلة X	**شبكات البيانات والاتصالات بين الأنظمة المفتوحة ومسائل الأمن**
السلسلة Y	البنية التحتية العالمية للمعلومات وجوانب بروتوكول الإنترنت وشبكات الجيل التالي
السلسلة Z	اللغات والجوانب العامة للبرمجيات في أنظمة الاتصالات

طُبعت في سويسرا
جنيف، 2016