الاتحـــــــــــاد الدولـــــــــــي للاتصـــــــــــالات

ITU-T

قطـــاع تقييس الاتصـــالات
في الاتحاد الدولي للاتصالات

X.1244

(2008/09)

السلسلة X: شبكات البيانات والاتصالات بين الأنظمة المفتوحة ومسائل الأمن

أمن الاتصالات

الجوانب العامة لمكافحة الاقتحام الإلكتروني في تطبيقات الوسائط المتعددة القائمة على بروتوكول الإنترنت

التوصيـــة ITU-T X.1244

الاتحاد الدولي للاتصالات

توصيات السلسلة X الصادرة عن قطاع تقييس الاتصالات

شبكات البيانات والاتصالات بين الأنظمة المفتوحة ومسائل الأمن

الشبكات العمومية للبيانات	
الخدمات والمرافق	X.19–X.1
السطوح البينية	X.49–X.20
الإرسال والتشوير والتبديل	X.89–X.50
مظاهر الشبكة	X.149–X.90
الصيانة	X.179–X.150
الترتيبات الإدارية	X.199–X.180
التوصيل البيني للأنظمة المفتوحة	
النموذج والترميز	X.209–X.200
تعريفات الخدمات	X.219–X.210
مواصفات بروتوكول بأسلوب التوصيل	X.229–X.220
مواصفات بروتوكول بأسلوب دون توصيل	X.239–X.230
جداول إعلان عن مطابقة تنفيذ بروتوكول	X.259–X.240
تعرّف هوية البروتوكول	X.269–X.260
بروتوكولات الأمن	X.279–X.270
أشياء مسيرة على الطبقة	X.289–X.280
اختبار المطابقة	X.299–X.290
التشغيل البيني للشبكات	
اعتبارات عامة	X.349–X.300
الأنظمة الساتلية لإرسال البيانات	X.369–X.350
الشبكات القائمة على بروتوكول الإنترنت	X.379–X.370
أنظمة معالجة الرسائل	X.499–X.400
الدليل	X.599–X.500
التشغيل البيني لأنظمة التوصيل OSI ومظاهر النظام	
توصيل الشبكات	X.629–X.600
الفعالية	X.639–X.630
نوعية الخدمة	X.649–X.640
التسمية والعنونة والتسجيل	X.679–X.650
ترميز نحو مجرد واحد (ASN.1)	X.699–X.680
إدارة التوصيل البيني للأنظمة المفتوحة (OSI)	
الإطار والهيكل المعماري لإدارة الأنظمة	X.709–X.700
خدمة اتصالات الإدارة وبروتوكولاتها	X.719–X.710
هيكل معلومات الإدارة	X.729–X.720
وظائف الإدارة ووظائف الهيكل المعماري للإدارة الموزعة المفتوحة	X.799–X.730
الأمن	X.849–X.800
تطبيقات التوصيل البيني للأنظمة المفتوحة (OSI)	
الالتزام والتلازم والاستعادة	X.859–X.850
معالجة المعاملات	X.879–X.860
العمليات البُعدية	X.889–X.880
التطبيقات التنوعية للترميز نحو مجرد واحد (ASN.1)	X.890-X.899
المعالجة الموزعة المفتوحة	X.999–X.900
أمن الاتصالات	**X.1000–**

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

التوصيـــة ITU-T X.1244

الجوانب العامة لمكافحة الاقتحام الإلكتروني في تطبيقات الوسائط المتعددة القائمة على بروتوكول الإنترنت

ملخص

تحدد هذه التوصية المفاهيم الأساسية، والخصائص، والقضايا التقنية ذات الصلة بمكافحة الاقتحام الإلكتروني في تطبيقات الوسائط المتعددة القائمة على بروتوكول الإنترنت، كالمهاتفة عبر بروتوكول الإنترنت (IP)، والمراسلة اللحظية، وما إلى ذلك. فتصنّف الرسائل الاقتحامية في تطبيقات الوسائط المتعددة القائمة على بروتوكول الإنترنت، على اختلاف أنماطها، إلى فئات، وتصف كل فئة طبقاً لخصائصها. وتصف هذه التوصية مختلف التهديدات الأمنية الاقتحامية التي يمكن أن تسبب الاقتحام الإلكتروني في تطبيقات الوسائط المتعددة القائمة على بروتوكول الإنترنت. وقد استُنبطَت تقنيات متنوعة للسيطرة على الرسائل الاقتحامية التي أصبحت مشكلة اجتماعية. وبعض هذه التقنيات يمكن استعماله لمكَافحة الاقتحام الإلكتروني في تطبيقات الوسائط المتعددة القائمة على بروتوكول الإنترنت. وتحلل هذه التوصية الآليات التقليدية لمكافحة الاقتحام، وتبحث في إمكان تطبيقها على مكافحة الاقتحام الإلكتروني في تطبيقات الوسائط المتعددة القائمة على بروتوكول الإنترنت. وفي الختام تذكر هذه التوصية الجوانب المختلفة التي ينبغي أن تراعى عند مكافحة الاقتحام الإلكتروني في تطبيقات الوسائط المتعددة القائمة على بروتوكول الإنترنت.

المصدر

وافقت لجنة الدراسات 17 (2005-2008) لقطاع تقييس الاتصالات بتاريخ 19 سبتمبر 2008 على التوصية ITU-T X.1244 بموجب إجراء القرار 1 الصادر عن الجمعية العالمية لتقييس الاتصالات.

مصطلحات أساسية

الاقتحام الإلكتروني على المراسلة الفورية، الاقتحام الإلكتروني على تطبيقات الوسائط المتعددة القائمة على بروتوكول الإنترنت، الاقتحام الإلكتروني، اقتحام المهاتفة عبر بروتوكول الإنترنت.

تمهيـــد

الاتحاد الدولي للاتصالات وكالة متخصصة للأمم المتحدة في ميدان الاتصالات. 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، تعد المعايير اللازمة على أساس التعاون مع المنظمة الدولية للتوحيد القياسي (ISO) واللجنة الكهرتقنية الدولية (IEC).

ملاحظة

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

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

حقوق الملكية الفكرية

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

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

© ITU 2009

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

المحتويات

الصفحة

1 مجال التطبيق 1
2 المراجع 1
3 التعاريف 1
1.3 مصطلحات معرَّفة في مواضع أخرى 1
2.3 مصطلحات معرَّفة في هذه الوثيقة 2
4 المختصرات والأسماء المختصرة 3
5 الاصطلاحات 4
6 مفهوم اقتحام الوسائط المتعددة القائمة على بروتوكول الإنترنت وأنماطه الشائعة 5
1.6 اقتحام المهاتفة عبر بروتوكول الإنترنت 5
2.6 اقتحام رسائل الوسائط المتعددة القائمة على بروتوكول الإنترنت (IP) 5
3.6 اقتحام المراسلة اللحظية 6
4.6 اقتحام الدردشة 6
5.6 الاقتحام المتعدد الموجهات 7
6.6 اقتحام خدمة تبادل الملفات بين نظيرين 7
7.6 اقتحام موقع ويب 7
7 تصنيف الاقتحام على الوسائط المتعددة القائمة على بروتوكول الإنترنت (IP) 7
1.7 الرسائل الاقتحامية الصوتية في الوقت الفعلي 8
2.7 الرسائل الاقتحامية النصية في الوقت الفعلي 9
3.7 الرسائل الاقتحامية الفيديوية في الوقت الفعلي 10
4.7 الرسائل الاقتحامية الصوتية في غير الوقت الفعلي 10
5.7 الرسائل الاقتحامية النصية في غير الوقت الفعلي 10
6.7 الرسائل الاقتحامية الفيديوية في غير الوقت الفعلي 11
8 المسألة التقنية المتعلقة بمكافحة اقتحام الوسائط المتعددة القائمة على بروتوكول الإنترنت (IP) 11
1.8 استحداث الرسائل الاقتحامية وتسليمها 11
2.8 كشف الرسائل الاقتحامية وترشيحها 13
3.8 الإجراءات المتخذة بشأن الرسائل الاقتحامية المستقبلة 14
9 التهديدات الأمنية المرتبطة بالاقتحام 14
1.9 التهديدات الأمنية المرتبطة بالاقتحام 14
2.9 تصنيف التهديدات الأمنية المرتبطة بالاقتحام 16
3.9 التدابير المضادة 17

الصفحة

10 إمكان تطبيق آليات مكافحة الاقتحام المعروفة على تطبيقات الوسائط المتعددة القائمة على بروتوكول الإنترنت (IP) 18

1.10 الترشيح بتعرُّف الهوية 18

2.10 تغليف العنوان 20

3.10 الإثبات التفاعلي البشري 21

4.10 ترشيح المحتوى 22

5.10 الاستيقان بتبادل المفاتيح 22

6.10 ترشيح الرسائل الاقتحامية بالاستناد إلى الشبكة 23

7.10 الطابع الإلكتروني 24

8.10 ترشيح الرسائل الاقتحامية المعتمد على التخويل 25

9.10 الإجراءات القانونية واللوائح 26

11 اعتبارات تُراعى في مكافحة اقتحام تطبيقات الوسائط المتعددة القائمة على بروتوكول الإنترنت (IP) 26

1.11 مستعمل الخدمة (المشترك في الخدمة) 27

2.11 موردو الخدمات 27

3.11 مشغِّلو الشبكات 28

4.11 المنظمات العمومية 29

5.11 اعتبارات أخرى 29

بيبليوغرافيا 30

مقدمة

أصبح الاقتحام مشكلة اجتماعية في النظام البريدي الإلكتروني الشبكي. وقد استُنبطَت وطُبِّقت حلول متنوعة لحل هذه المشكلة، لكنّ أياً منها لم يُفلح في حلها بالفعل. وتضم تطبيقات الوسائط المتعددة القائمة على بروتوكول الإنترنت أنماطاً خدمية متنوعة، مثل المهاتفة عبر بروتوكول الإنترنت (IP)، والمراسلة اللحظية، وما إلى ذلك. وأخذ مرسلو الرسائل الاقتحامية يستهدفون بصورة متزايدة هذه الخدمات، لأن اقتحامها أبسط تقنياً وأجدى اقتصادياً. لذا يجب معالجة اقتحام تطبيقات الوسائط المتعددة القائمة على بروتوكول الإنترنت قبل أن يصير مشكلة عمومية.

وتصف هذه التوصية مفهوم وخصائص مختلف أنماط الاقتحام الممكن حصولها في تطبيقات الوسائط المتعددة القائمة على بروتوكول الإنترنت. وتدرس هذه التوصية، من الزاويتين التقنية والأمنية، بعض قضايا مكافحة اقتحام تطبيقات الوسائط المتعددة القائمة على بروتوكول الإنترنت، حيث تقدم بعض العناصر التي يجب أن يأخذها في الحسبان، عند مكافحة اقتحام تطبيقات الوسائط المتعددة القائمة على بروتوكول الإنترنت، العديد من الأطراف المشاركة في تقديم خدمات الوسائط المتعددة القائمة على بروتوكول الإنترنت (IP) (مثل موردي الخدمات، ومستعمليها، وغيرهم).

الجوانب العامة لمكافحة الاقتحام الإلكتروني في تطبيقات الوسائط المتعددة القائمة على بروتوكول الإنترنت

1 مجال التطبيق

تقدم هذه التوصية نظرة عامة لمسألة الاقتحام في تطبيقات الوسائط المتعددة القائمة على بروتوكول الإنترنت، على القضايا التالية:

- مفهوم وخصائص اقتحام تطبيقات الوسائط المتعددة القائمة على بروتوكول الإنترنت
- القضايا التقنية ذات الصلة باقتحام تطبيقات الوسائط المتعددة القائمة على بروتوكول الإنترنت
- التهديدات الأمنية المتصلة بالاقتحام
- أساليب مكافحة الاقتحام وإمكانية تطبيقها لمكافحة اقتحام تطبيقات الوسائط المتعددة القائمة على بروتوكول الإنترنت
- الجوانب المختلفة التي ينبغي أخذها في الحسبان من أجل مكافحة اقتحام تطبيقات الوسائط المتعددة القائمة على بروتوكول الإنترنت.

ملاحظة – في هذه التوصية لا يُستعمَل مصطلح "هوية" بمعناه المطلق. وهو لا يشكل تحديداً أي مدلول إيجابي.

2 المراجع

لا يوجد.

3 التعاريف

1.3 مصطلحات معرَّفة في مواضع أخرى

تستعمل هذه التوصية المصطلحات التالية المعرفة في مواضع أخرى:

1.1.3 قائمة التحكم في النفاذ (ACL) [b-ITU-T X.741]: يُستعمَل النعت "قائمة التحكم في النفاذ" لاحتواء هويّات الممهّدين المرخَّص لهم تحديداً بالنفاذ إلى المعلومات الإدارية أو المحظور عليهم تحديداً النفاذ إلى هذه المعلومات.

2.1.3 سلطة إصدار الشهادة (CA) [b-ITU-T X.509]: هي سلطة أولاها الثقة مستعمِل واحد أو أكثر لوضع وتخصيص شهادات المفاتيح العمومية. ويجوز لسلطة إصدار الشهادة وضع مفاتيح المستعملين اختيارياً.

3.1.3 المؤتمر [b-ITU-T T.124]: يُطلق مصطلح "مؤتمر" على عدد من العُقَد المرتبطة ببعضها، القادرة على تبادل معلومات سمعية بيانية ومعلومات سمعية مرئية، عبر شبكات متنوعة للاتصالات.

4.1.3 رسالة معرَّفةُ بمفاتيح الميادين (DKIM) [b-IETF RFC 4871]: آلية لتوقيع الرسائل الإلكترونية توقيعاً مجَفَّراً، تمكّن الميدان الموقِّع من إعلان مسؤوليته عن إدخال رسالة في تدفق الرسائل. ويستطيع مستقبلو الرسائل التحقق من التوقيع بطلب ميدان الموقِّع مباشرة، من أجل استرداد المفتاح العمومي المناسب، ومن ثَمَّ التأكد أن الرسالة سبق التصديق عليها من جانب طرف يملك المفتاح الخاص للميدان الموقِّع.

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

6.1.3 العلاقة بين نظيرين (P2P) [b-ITU-T T.180]: في علاقة بين نظيرين، يستطيع المستعمِلان التفاوض على خصائص التفاعل، ثم يقيمان الاتصال ملتزمين بالقواعد التي تفاوضا عليها: ويكون للمستعمِلَيْن (كيان ونظيره) حقوق متساوية عادةً. وتبيّن الوثيقة [b-IETF RFC 4981] أن الشبكات المتسمة بهذه العلاقة هي التي تبدي الخصائص الثلاث التالية: التنظيم الذاتي، والاتصال المتناظر، والتحكم الموزَّع.

7.1.3 بروتوكول الخصوصية الجيدة جداً (PGP) [b-IETF RFC 1991]: يستعمل هذا البروتوكول توليفة من مفتاح عمومي وتجفير تقليدي، لتوفير خدمات أمن لرسائل البريد الإلكتروني وملفّات البيانات. وتشتمل هذه الخدمات على السرّية والتوقيع الرقمي. وهذا البروتوكول PGP ابتكره فيليب زيمّرمان، وكان أول إصدار له في عام 1991 بالصيغة 1.0. ثم جرى تصميم وتنفيذ الصيغ اللاحقة، مثل الصيغة Open PGP الموصوفة في الوثيقة [b-IETF RFC 4880]، بمجهود تطوعي بحت، تحت إشراف فيليب زيمّرمان. *كما يعتبر PGP و Pretty Good Privacy ماركتين مسجلتين لفيليب زيمّرمان.*

8.1.3 بنية تحتية لمفاتيح عمومية (PKI) [b-ITU-T X.509]: هي البنية التحتية التي من شأنها دعم إدارة المفاتيح العمومية القادرة على دعم خدمات الاستيقان أو التجفير أو السلامة أو عدم الرفض.

9.1.3 أمن طبقة النقل (TLS) [b-ITU-T Q.814]: يوفِّر البروتوكول TLS اختيارياً سرّية الاتصالات. وهذا البروتوكول يمكّن تطبيقات العميل/المخدم من الاتصال بطريقة مصممَة للوقاية من التنصّت الخفي والعبَث والاقتحام. ويوفّر البروتوكول TLS أيضاً استيقاناً قوياً للنظير والسلامة لتدفق البيانات.

2.3 مصطلحات معرَّفة في هذه الوثيقة

تعرف هذه التوصية المصطلحات التالية:

1.2.3 اقتحام بالطُعم: استمد اسمه بشكل هزلي قياساً على الصيد (والتصيد الاحتيالي (انظر الفقرة 10.2.3))، الاقتحام بالطعم هو نوع من الاقتحام يشمل عنصراً، مثلاً موضوع بريد إلكتروني أو وصلة مرفقة لإغراء المستعملين. والمستعمِل المُغرَّر به يُعتَدى عليه باقتحام الطعم.

2.2.3 مدونة (Blog): مصطلح مُشتَقّ من إدغام "Web log"؛ وهي قائمة بالاهتمامات الشخصية لصاحبها على الخط ويحتمل أن تكون متعددة الوسائط، وهي متاحة لعامة الجمهور من أجل مشاهدتها وتعزيزها في بعض الأحيان.

3.2.3 برنامج روبوت (bot): "بوت" اختصار لروبوت، تُطلَق على برنامج يشتغل بمثابة وكيل لمستعمِل أو لبرنامج آخر، من أجل محاكاة تصرف بشري.

4.2.3 تسميم النسخة الخفية لنظام أسماء الميادين (DNS): يُطلق وصف "تسميم النسخة الخفية لنظام أسماء الميادين" على تقنية تقوم على خداع مخدم أسماء ميادين (مخدم DNS) بإيهامه أن عنوان DNS لمخدم معين قد تغيّر، خلافاً لواقع الحال. ومتى تسمم مخدم DNS تُحفَظ عادةً المعلومةُ المغلوطة لمدة ما من الزمن، فينتشر أثر هذا العدوان على مستعملي المخدم.

5.2.3 رسالة وسائط متعددة قائمة على بروتوكول الإنترنت: هي رسالة نصية أو صوتية أو فيديوية، تُسلَّم في مطراف أو مخدم وسائط متعددة قائم على بروتوكول الإنترنت، وتُخزَن لكي يفحصها متلقيها فيما بعد. فهي شبيهة بالرسالة الصوتية في خدمة المهاتفة، لكنها تُقدَّم في خدمة وسائط متعددة قائمة على بروتوكول الإنترنت (IP).

6.2.3 اقتحام الوسائط المتعددة القائمة على بروتوكول الإنترنت (IP): هي رسائل أو نداءات غير مرغوبة، تقتحم تطبيقات الوسائط المتعددة القائمة على بروتوكول الإنترنت (IP). وتتميّز هذه الرسائل الاقتحامية عن تلك الخاصة بالبريد الإلكتروني التقليدي بأنها تختص بالاقتحام على أحدث طرائق الاتصالات البازغة التي تتم عبر بروتوكول الإنترنت، مثل المراسلة اللحظية (IM)، أو الحضور، أو خدمات المهاتفة عبر بروتوكول الإنترنت (VoIP).

7.2.3 التشفيرات الموجَّهة (أو باختصار: الموجَّهات): يشير هذا التعبير في الاستخدام العام إلى الأشكال أو البروتوكولات أو الظروف التي تحيط بالاتصالات الرسمية. وفي سياق هذه التوصية، تشير إلى تشفيرات لمعلومات تحتوي معلومات يُدركها

الكائن البشري. وتشمل أمثلة التشفيرات البيانات النصية والبيانية والسمعية والفيديوية واللمسية، التي تُستعمَل على السطوح البينية بين الإنسان والحاسوب. والمعلومات المتعددة الموجهات يمكن أن تنطلق من أجهزة متعددة التوجيه أو تستهدف مثل هذه الأجهزة. وتشمل أمثلة السطوح البينية بين الإنسان والحاسوب، الميكروفون للدخل الصوتي، والقلم للدخل اللمسي، ولوحة المفاتيح للدخل النصّي، والفأرة للدخل الحركي، ومكبِّر الصوت للخرج الصوتي التركيبي، والشاشة للخرج البياني أو النصي، والجهاز الاهتزازي للتغذية الراجعة اللمسية، وجهاز كتابة برايل للمكفوفين.

8.2.3 الرسالة المتعددة الموجهات: عبارة عن رسالة متعددة الوسائط تحتوي على معلومات مختلفة التشفير، بقصد التفاعل عن طريق موجَّهات متعددة. فعلى سبيل المثال، من الجائز، في خدمة المراسلة المتعددة الوسائط (MMS)، أن تحمل الرسالة موجَّهات نصية وبيانية وسمعية؛ ويجوز أيضاً في صفحة الويب أن يكون محتواها موجَّهاً متعدد الوسائط، مشتملاً على نص وفيديو؛ وعلى غرار ذلك، يجوز في الرسالة الإلكترونية أن تحتوي مُرفقاً بيانياً وآخر نصياً. وبذلك يمكّن تعددُ التوجيه المستعمِلَ من انتقاء التشفيرة الموجَّهة التي يفضّلها، تبعاً للبيئة أو السهولة أو المحتوى.

9.2.3 لعبة على الخط: لعبة في الوقت الفعلي تُلعَب عبر الشبكات.

10.2.3 التمويه: محاولة للحصول بالإجرام والاحتيال على معلومات حساسة، مثل اسم المستعمِل وكلمات السر وتفاصيل حساباته المالية، عن طريق انتحال صفة كيان موثوق في الاتصالات الإلكترونية.

11.2.3 سرقة الدورة: آلية لسرقة دورة مستعملٍ صالحة، من أجل اكتساب نفاذ غير مخول إلى معلومات وخدمات.

12.2.3 اقتحام على المراسلة اللحظية (SPIM): اقتحام يستهدف مستعملي خدمة المراسلة اللحظية.

13.2.3 اقتحام على المهاتفة عبر الإنترنت (SPIT): اقتحام يستهدف مستعملي خدمة المهاتفة عبر الإنترنت.

14.2.3 المقتحِم: المقتحم هو مرسِل الرسائل الاقتحامية.

15.2.3 الاقتحام: سلسلةُ الأنشطة التي يقوم بها المقتحِمون من أجل إرسال رسائل اقتحامية، مثل تجميع قائمة المستهدفين، واستحداث الرسائل الاقتحامية وتسليمها، وما إلى ذلك.

16.2.3 مقتحِم المراسلة اللحظية: مُرسِل الرسائل الاقتحامية على المراسلة اللحظية.

17.2.3 مقتحِم المهاتفة عبر الإنترنت: مُرسِل الرسائل الاقتحامية على المهاتفة عبر الإنترنت.

18.2.3 محتويات يضعها المستعمِل (UCC): كل شكل من أشكال المحتوى، كالفيديو والمدونات والصور والمواد السمعية وغير ذلك، وضعه مستعمِل نهائي (من الجمهور العادي) لكي يكون متيسِّراً لعامة الجمهور.

19.2.3 محتويات يولدها المستعمِل (UGC): مرادف للمصطلح السابق (UCC).

20.2.3 التمويه الصوتي: نفاذ غير مشروع إلى معلومات الخصوصية الشخصية والمالية عن طريق المهاتفة عبر بروتوكول الإنترنت (الخدمة VoIP). ومصطلح Vishing مُشتَقّ من إدغام Voice وPhishing.

4 المختصرات والأسماء المختصرة

تستعمل هذه التوصية المختصرات والأسماء المختصرة التالية:

ACL قائمة التحكم في النفاذ (*Access Control List*)

APEC مجلس التعاون الاقتصادي لآسيا والمحيط الهادئ (*Asia-Pacific Economic Cooperation*)

ARP بروتوكول استبانة العنوان (*Address Resolution Protocol*)

ASCII الشفرة المعيارية الأمريكية لتبادل المعلومات (*American Standard Code for Information Interchange*)

CA سلطات التصديق/سلطة إصدار الشهادة (*Certificate Authority*)

DB	قاعدة بيانات (*Database*)
DKIM	رسالة معرَّفة بمفتاح الميدان (*Domain Keys Identified Mail*)
HTTP	بروتوكول نقل النص الفائق (*Hypertext Transfer Protocol*)
IM	المراسلة اللحظية (*Instant Messaging*)
IP	بروتوكول الإنترنت (*Internet Protocol*)
IPTV	التلفزيون القائم على بروتوكول الإنترنت (*Internet Protocol Television*)
IPv4	الإصدار 4 لبروتوكول الإنترنت (*Internet Protocol version 4*)
IPv6	الإصدار 6 لبروتوكول الإنترنت (*Internet Protocol version 6*)
IRC	دردشة عبر الإنترنت (*Internet Relay Chat*)
ISP	مورد خدمة الإنترنت (*Internet Service Provider*)
ITSP	مورد خدمة هاتفية بواسطة الإنترنت (*Internet Telephony Service Provider*)
IVR	استجابة صوتية تفاعلية (*Interactive Voice Response*)
MAC	التحكم بالنفاذ إلى الوسائط (*Media Access Control*)
MIPv4	الإصدار 4 لبروتوكول الإنترنت من أجل الأجهزة المحمولة (*Mobile IPv4*)
MIPv6	الإصدار 6 لبروتوكول الإنترنت من أجل الأجهزة المحمولة (*Mobile IPv6*)
NDP	بروتوكول اكتشاف الجار (*Neighbour Discovery Protocol*)
OS	نظام تشغيل (*Operating System*)
P2P	العلاقة بين نظيرين (*Peer-to-Peer*)
PGP	البروتوكول PGP *(Pretty Good Privacy)*
PKI	بنية تحتية لمفاتيح عمومية (*Public Key Infrastructure*)
PSTN	الشبكة الهاتفية العمومية التبديلية (*Public Switched Telephone Network*)
RTP	بروتوكول نقل في الوقت الفعلي (*Real-time Transport Protocol*)
SMS	خدمة الرسائل القصيرة (*Short Message Service*)
SMTP	بروتوكول نقل البريد البسيط (*Simple Mail Transfer Protocol*)
SQL	لغة استجواب مبَنْيَنة (*Structured Query Language*)
TCP	بروتوكول التحكم في الإرسال (*Transmission Control Protocol*)
TLS	أمن طبقة النقل (*Transport Layer Security*)
URI	معرِّف هوية الموارد الموحَّد (*Uniform Resource Identifier*)
URL	موقع الموارد الموحد (*Uniform Resource Locator*)
VoD	الفيديو عند الطلب (*Video on Demand*)
VoIP	المهاتفة عبر بروتوكول الإنترنت (*Voice over IP*)

5 الاصطلاحات

لا يوجد.

6 مفهوم اقتحام الوسائط المتعددة القائمة على بروتوكول الإنترنت وأنماطه الشائعة

يُستعمَل مصطلح "الاقتحام الإلكتروني"، على الرغم من أنه لا يوجد تعريف له متفق عليه عالمياً، للدلالة على اتصالات غزيرة غير مُلتمَسة عبر البريد الإلكتروني أو المراسلة المتنقّلة، لأغراض ترويج منتجات أو خدمات تجارية. وفي الوقت الحاضر، لا يقتصر الاقتحام على البريد الإلكتروني والمراسلة المتنقّلة. إذ إنه آخذ في الانتشار إلى تطبيقات الوسائط المتعددة القائمة على بروتوكول الإنترنت (IP)، مثل المهاتفة عبر بروتوكول الإنترنت (VoIP) والمراسلة اللحظية. ويمكن تعريف اقتحام الوسائط المتعددة القائمة على بروتوكول الإنترنت بأنه: اتصالات غزيرة إلكترونية غير مُلتمَسة، تُبَثّ على تطبيقات الوسائط المتعددة القائمة على بروتوكول الإنترنت (IP)، لأغراض ترويج منتجات أو خدمات تجارية. يحصل اقتحام الوسائط المتعددة القائمة على بروتوكول الإنترنت عبر مختلف تطبيقات الوسائط المتعددة القائمة على بروتوكول الإنترنت، مثل المهاتفة عبر بروتوكول الإنترنت (VoIP) والمراسلة اللحظية.

ويقدم هذا القسم قائمة بالأنماط الشائعة لاقتحام الوسائط المتعددة القائمة على بروتوكول الإنترنت (IP) التي يمكن أن تحدث على تطبيقات الوسائط المتعددة القائمة على بروتوكول الإنترنت (IP). ويعطي وصفاً لخصائص كل نمط منها.

1.6 اقتحام المهاتفة عبر بروتوكول الإنترنت

اقتحام المهاتفة عبر بروتوكول الإنترنت عبارة عن اقتحام ينشأ على خدمات المهاتفة عبر بروتوكول الإنترنت وهو عبارة عن رسائل اقتحامية صوتية في الوقت الفعلي، مثل الترويج التجاري عن بعد، وهي عملية تشتمل على اتصالات مع المروّج عن بعد وعلى التفاعل مع منظومات استجابة صوتية تفاعلية (IVR). ونظراً إلى أن خدمات الترويج التجاري عن بعد بواسطة خدمة المهاتفة عبر بروتوكول الإنترنت تتزايد بسرعة من خلال الانتشار السريع لخدمات المهاتفة تلك في جميع أرجاء العالم، فإن تهديدات اقتحام المهاتفة عبر بروتوكول الإنترنت (VoIP) تتزايد أيضاً، خاصة أن إنشاء كم غزير من النداءات ليس بالأمر الصعب. وبالإمكان استخدام عمالة رخيصة كمروجين من بلدان أخرى أرخص عادةً من العمالة المتاحة في البلد المستهدف، خاصة مع الانخفاض الهائل في أسعار النداءات الدولية عن طريق استخدام المهاتفة عبر بروتوكول الإنترنت (VoIP). ومن السهل جداً على المقتحمين جمع معلومات عن مستعملي تطبيقات الوسائط المتعددة القائمة على بروتوكول الإنترنت (IP) المستهدفين. وبهذا الدعم، يمكن لاقتحام المهاتفة عبر بروتوكول الإنترنت (VoIP) أن يبرز كتهديد خطير لموردي خدمة المهاتفة عبر بروتوكول الإنترنت (VoIP) ويستعملها.

2.6 اقتحام رسائل الوسائط المتعددة القائمة على بروتوكول الإنترنت (IP)

تكون رسالة الوسائط المتعددة القائمة على بروتوكول الإنترنت (IP) إما رسالة نصية أو صوتية أو فيديوية، تُسلَّم وتخزن في مطاريف أو مخدمات وسائط متعددة قائمة على بروتوكول الإنترنت (IP)، ريثما يتفقّدها المستقبل في وقت لاحق. إنها شبيهة بالرسالة الصوتية في خدمة المهاتفة، لكنها مُقدَّمة في خدمة وسائط متعددة قائمة على بروتوكول الإنترنت (IP). فاقتحام هذه الرسائل هو اقتحام يستعمل خدمة رسائل الوسائط المتعددة القائمة على بروتوكول الإنترنت (IP). ومستقبل الرسالة الاقتحامية يستقبلها ويستبعدها مثلما يفعل مع الرسائل الاقتحامية على البريد الإلكتروني ومع الرسائل الاقتحامية على المراسلة المتنقلة. وهناك مطاريف كثيرة لتطبيقات الوسائط المتعددة القائمة على بروتوكول الإنترنت (IP) مثل أجهزة المهاتفة عبر بروتوكول الإنترنت (VoIP)، تدعم وظائف المراسلة المتعددة الوسائط، ومن ثم فهي أهداف جيدة للمقتحم، فيوجه إليها هذا النوع من الاقتحام.

ويمكن تصنيف اقتحام رسائل الوسائط المتعددة إلى اقتحام لرسائل نصية واقتحام لرسائل صوتية/فيديوية. واقتحام الرسائل النصية عبارة عن رسالة قصيرة تتضمن نصاً تجاري القصد أو ذا قصد معين. ولها خصائص مشابهة لخصائص الرسائل الاقتحامية على البريد الإلكتروني أو تلك الواقعة على خدمة الرسائل القصيرة المتنقلة، على اعتبار أنها بشكل نص. إلا أن تكلفة اقتحام الرسائل النصية يتوقع لها أن تكون أقل بكثير من تكلفة اقتحام خدمة الرسائل القصيرة المتنقلة. واقتحام الرسالة الصوتية/الفيديوية عبارة عن رسالة ذات شكل صوتي/فيديوي، تشمل محتويات تجارية القصد أو ذات قصد معين. ويتوقع لهذا النمط من الاقتحام أن ينتشر على نطاق واسع انتشاراً مواكباً استعمال تطبيقات الوسائط المتعددة القائمة على بروتوكول

الإنترنت (IP). ومعلوم مسبقاً أن اقتحام الرسائل الصوتية/الفيديوية سيشغل قسماً كبيراً من صندوق البريد الصوتي/الفيديوي لمستعملي تطبيقات قائمة على بروتوكول الإنترنت (IP) أو قسماً كبيراً من القدرة التخزينية لموردي الخدمة IP، على اعتبار أن حجم رسائل الوسائط المتعددة أكبر بكثير من حجم الرسائل النصية. واقتحام رسائل الوسائط المتعددة يمكن أن يستعمل أيضاً من قبل مقتحمين أشرار لتسليم برمجيات ضارة مثل الديدان (worms)، والفيروسات، وبرمجيات التجسس، وأحصنة طروادة، وما إلى ذلك.

3.6 اقتحام المراسلة اللحظية

يمثّل الاقتحام على المراسلة اللحظية (SPIM) تهديداً آخر من تهديدات الاقتحام على تطبيقات الوسائط المتعددة القائمة على بروتوكول الإنترنت (IP)، حيث إنه يستهدف مستعملي خدمة المراسلة اللحظية (IM). وكثير من المستعملين يعوّلون على خدمة المراسلة اللحظية كوسيلة اتصالات ملائمة مع مستعملين آخرين عبر الشبكات. وأغلبية الرسائل الاقتحامية على المراسلة IM هي رسائل قصيرة معتمِدة على النص، وتشترك في خصائص كثيرة مع الرسائل الاقتحامية على البريد الإلكتروني، غير أن الرسائل الاقتحامية على المراسلة IM تتم في الوقت الفعلي، ويمكن أن تكون أشد إزعاجاً. واقتحام رسائل الوسائط المتعددة يمكن أن يحدث أيضاً في المراسلة IM، لأن هذه الخدمة تدعم كثيراً من الوظائف غير تسليم الرسائل النصية في الوقت الفعلي.

ربما كان من العسير إرسال رسائل اقتحامية على المراسلة اللحظية، بدون تلاعب تقني مخالف للقانون، على اعتبار أن أغلبية خدمات المراسلة اللحظية تعتمد قوائم رفاق مبنية على القبول، ولا يُسمح لمستعملين من خارج هذه القوائم بإرسال رسائل. ومع ذلك، فإن هشاشة نظام الأمن المعتمَد لخدمات المراسلة اللحظية قد تتيح للمقتحمين سرقة قائمة الرفاق أو القائمة البيضاء من عند أحد مستهدَفي الاقتحام، لإرسال رسائل اقتحامية منتحلين صفة عضو من أعضاء قائمة الرفاق.

وفي حين لا يمكن تسليم الرسائل إلا بين المستعملين المدرجين في قائمة الرفاق، فإن أي شخص يستطيع أن يطلب قبول إدراج اسمه ضمن قائمة الرفاق. وفي كثير من خدمات المراسلة اللحظية، يمكن أن تحتوي رسالة طلب الانضمام إلى القائمة بعض العبارات التي تعرِّف بالطالب، لمساعدة مستعمل الخدمة IM على معرفة من الذي يطلب الانضمام، والبت في قضية السماح للطالب بالانضمام إلى قائمة الرفاق. ومن ثم، فإن المقتحم غير الموجود على قائمة الرفاق يستطيع أن يرسل رسائل اقتحامية باستعماله هذه الوظيفة من وظائف الخدمة IM.

4.6 اقتحام الدردشة

يحدث اقتحام الدردشة في مختلف أنواع تطبيقات الوسائط المتعددة القائمة على بروتوكول الإنترنت (IP) المتوفّرة فيها وظائف دردشة بين مستعملي الخدمة. ووظيفة الدردشة تُقدم هي ووظيفة المراسلة في كثير من تطبيقات الوسائط المتعددة القائمة على بروتوكول الإنترنت (IP)، مثل خدمات الدردشة على الخط، وخدمات اللعب على الخط، وما إلى ذلك. ويكون اقتحام الدردشة عادة في نسق رسالة نصية قصيرة، يُرسل نصها تكراراً إلى جميع المشاركين في الدردشة. ولذا، فإن بعض خدمات الدردشة على الخط، وخدمات اللعب على الخط تحد من تكرار نفس الرسالة الجاري تسليمها، من أجل مكافحة تكرار الرسائل الاقتحامية. إلا أن جدوى هذه الطريقة محدودة، ويلزم اتخاذ مزيد من التدابير المضادة من أجل مكافحة مختلف أنماط اقتحام الدردشة.

ولخدمة الدردشة خصائص مشتركة مع خدمة المراسلة اللحظية (IM)، لكن أنماط الاقتحام التي تتعرض لها هاتان الخدمتان مختلفة. فمستعمل خدمة المراسلة اللحظية (IM) يتصل عادة مع أقرانه في قائمة الرفاق، الذين يخوّلهم مستعمل هذه الخدمة الاتصال. وهكذا يتحتّم على المقتحم اختراق هذه القائمة، لكي يرسِل رسالة اقتحامية. أما الدردشة فتجري في خدمات على الخط، ويكون المشاركون في الاتصال مجهولين عادة. وعليه، يستطيع أي شخص أن يشارك في خدمة الدردشة، ويستطيع المقتحم أن ينضم إلى خدمة الدردشة لإرسال الرسائل الاقتحامية. ويقوم نمط الاقتحام الذي يحدث في خدمة الدردشة على إرسال نفس الرسالة تكراراً. وهكذا، فإن اقتحام خدمة الدردشة أبسط بكثير من اقتحام خدمة المراسلة اللحظية.

5.6 الاقتحام المتعدد الموجهات

إن مشكلة أمن "مسار الاقتحام" تمتد إلى حالة التفاعلات المتعددة الموجهات، حيث يكون من شأن "رسالة اقتحامية" واحدة متعددة الوسائط أن تُصيب، على السطح البيني للمستعمل، أهدافاً متعددة متنوّعة تنوّع التشفيرات الموجَّهة (الموجَّهات). مثلاً: من شأن رسالة اقتحامية في شبكة أن تُسفِر عن تشغيل تسجيل سمعي لرسالة اقتحامية، وعن تشغيل تسجيل فيديوي لرسالة اقتحامية، وعن عرض رسالة اقتحامية نصية على الشاشة؛ ويكون لكل رسالة من هذه الرسائل الاقتحامية محتوى واحد أو محتوى مختلف. فتعدد التوجيه يزيد بحد ذاته من التعرض للاقتحام المتعدد الوسائط، ومن ثم، فإن مشكلة الاقتحام المتعدد الموجهات سائرة إلى التفاقم حين تصير التفاعلات المتعددة الموجهات أوسع انتشاراً.

6.6 اقتحام خدمة تبادل الملفات بين نظيرين

يمكن أيضاً أن تقوم تطبيقات الوسائط المتعددة القائمة على بروتوكول الإنترنت (IP) باقتحام تطبيقات الوسائط المتعددة القائمة على الإنترنت (IP) بين نظيرين (P2P)، المندرجة في سياق خدمات مستعمِلِين قائمة على العلاقة بين نظيرين (P2P)، مثل خدمة تبادل الملفات القائمة على هذه العلاقة. فالأشخاص الموصَّلون بشبكة قائمة على بروتوكول الإنترنت (IP) الذين يستعملون برمجيات بين نظيرين (P2P) يساعدون مستعملين آخرين على استعمال الاتصال القائم على العلاقة بين نظيرين من أجل تبادل أنواع مختلفة من الملفات الحاسوبية فيما بينهم. ففي سياق هذه الخدمات، يستطيع المقتحمون إغراء مستعملين آخرين بتنزيل ملفات اقتحام، عن طريق تسمية الملف المقحَم باسم فيلم مشهور، أو أغنية مشهورة وما إلى ذلك. وهكذا لا يحتاج المقتحمون إلى البحث عن أهداف. بل يحتاجون فقط إلى تبادل الملفات المقحَمة، لكي يحملوا مستعملين آخرين للخدمة P2P على النفاذ إلى هذه الملفات. ومن المتوقع أن يجري تنفيذ الكثير من الملفّات المقحَمة التي يتم تنزيلها، على اعتبار أن المستقبلين يقومون بتحميلها طوعاً. وهكذا، فإن الضرر الذي يسببه اقتحام خدمة P2P يمكن أن يكون فادحاً، حين يحتوي الملف المقحَم برمجيات ضارة، مثل الديدان والفيروسات، بدلاً من المحتويات التجارية.

7.6 اقتحام موقع ويب

يستطيع المقتحمون وضع مقالات أو ملفات ذات محتويات تجارية على مواقع ويب كثيرة مشغَّلة لأغراض متنوّعة. فالرسالة الاقتحامية الموضوعة على لوحة العرض الإلكتروني يستطيع مشاهدتها كثير من زوّار موقع الويب. مثلاً: الردود ذات المحتويات التجارية بخصوص أصناف كثيرة من بوابات الويب، والمواد التجارية على المدونات، يمكن أن تكون شكلاً من أشكال اقتحام مواقع الويب. وإضافةً إلى المقالات النصية، يستطيع المقتحمون وضع ملفات سمعية أو فيديوية ذات محتوى تجاري على مواقع تبادل المواد السمعية/الفيديوية، مثل المحتويات التي يكون واضعها أو مبتكرها هو المستعمِل (المحتويات UCC أو UGC)، أو على لوح عرض إلكتروني، لحمل مستعملي الخدمة الآخرين على مشاهدة الملفات الفيديوية التجارية. وهكذا، فإن اقتحام مواقع الويب يمكن أن يطلع عليه أو يشاهده عدد كبير من مستعملي خدمة مواقع الويب، ومن ثَمَّ ففي هذا النمط من الاقتحام أيضاً لا يحتاج المقتحمون إلى تجميع قائمة أهداف يرسلون إليها كمّاً من الرسائل الاقتحامية.

7 تصنيف الاقتحام على الوسائط المتعددة القائمة على بروتوكول الإنترنت (IP)

يُصنّف الاقتحام على تطبيقات الوسائط المتعددة القائمة على بروتوكول الإنترنت (IP) إلى مجموعتين تبعاً للخصائص. ويمكن تصنيفه تبعاً لمعايير متنوِّعة مثل نمط تطبيقات الوسائط المتعددة القائمة على بروتوكول الإنترنت (IP) التي يحدث فيها الاقتحام، ونمط الوسائط المستعملة في الاقتحام، والبروتوكول المستعمل للتزويد بالخدمة، ونمط رسالة البروتوكول، وما إلى ذلك. وفي هذا القسم، يصنف الاقتحام على الوسائط المتعددة القائمة على بروتوكول الإنترنت (IP) تبعاً للخصائص التالية التي تتميّز بها تطبيقات الوسائط المتعددة القائمة على بروتوكول الإنترنت (IP)، على اعتبار أن تقنيات مكافحة الاقتحام يمكن تطبيقها وفقاً لهذه الخصائص.

- اقتحام على الوسائط المتعددة القائمة على بروتوكول الإنترنت (IP) في الوقت الفعلي أو في غير الوقت الفعلي: خدمات تطبيقات الوسائط المتعددة القائمة على بروتوكول الإنترنت (IP) يمكن تصنيفها تبعاً لمعيار الحدوث في الوقت الفعلي.
- نمط وسائط الاقتحام على الوسائط المتعددة القائمة على بروتوكول الإنترنت (IP): إن خدمة تطبيقات الوسائط المتعددة القائمة على بروتوكول الإنترنت (IP) يمكن أن تدعم مواد نصية أو صوتية أو فيديوية أو مزيجاً من هذه المواد. والمواد الفيديوية تشمل الصورة الثابتة والصورة المتحركة على السواء.

وفي خدمات تطبيقات الوسائط المتعددة القائمة على بروتوكول الإنترنت (IP) في الوقت الفعلي، يقام الاتصال ثم تسلم رسالة ويقوم المتلقي بتفحص الرسالة في الوقت الفعلي. ومن الأمثلة النموذجية على تطبيقات الوسائط المتعددة القائمة على بروتوكول الإنترنت (IP) في الوقت الفعلي: خدمة المهاتفة عبر بروتوكول الإنترنت (VoIP)، وخدمة المراسلة اللحظية. أما خدمات تطبيقات الوسائط المتعددة القائمة على بروتوكول الإنترنت (IP) في غير الوقت الفعلي ففيها يستطيع المتلقي تفحص الرسائل متى شاء (شاءت). ومن الأمثلة على تطبيقات الوسائط المتعددة القائمة على بروتوكول الإنترنت (IP) في غير الوقت الفعلي: خدمات الويب، الخدمة القائمة على العلاقة بين نظيرَيْن (الخدمة P2P)، خدمات اللعب على الخط، وما إلى ذلك. ويأتي في الجدول 7-1 عرض لتصنيف الاقتحام على الوسائط المتعددة القائمة على بروتوكول الإنترنت (IP) مع الأمثلة النموذجية.

الجدول 7-1 – تصنيف الاقتحام على الوسائط المتعددة القائمة على بروتوكول الإنترنت (IP)

	نصي	صوتي	فيديوي
في الوقت الفعلي	• اقتحام مراسلة لحظية • اقتحام دردشة	• اقتحام مهاتفة عبر بروتوكول الإنترنت • اقتحام مراسلة لحظية	• اقتحام مراسلة لحظية
في غير الوقت الفعلي	• اقتحام رسائل نصية/وسائط متعددة • رسالة اقتحامية نصية على خدمة تبادل الملفات بين نظيرَيْن • رسالة اقتحامية نصية على موقع ويب	• اقتحام رسائل صوتية/وسائط متعددة • رسالة اقتحامية صوتية على خدمة تبادل الملفات بين نظيرين • رسالة اقتحامية صوتية على موقع ويب	• اقتحام على رسائل فيديوية/متعددة الوسائط • رسالة اقتحامية فيديوية على خدمة تبادل ملفات بين نظيرين • رسالة اقتحامية فيديوية على موقع ويب

1.7 الرسائل الاقتحامية الصوتية في الوقت الفعلي

يمكن تعريف الرسالة الاقتحامية الصوتية في الوقت الفعلي بأنها اتصالات صوتية في الوقت الفعلي غير ملتمَسة، بغرض الدعاية لمنتجات أو خدمات تجارية. ومثال نموذجي على الرسائل الاقتحامية الصوتية في الوقت الفعلي هو اقتحام المهاتفة عبر بروتوكول الإنترنت (VoIP). ربما كانت الرسائل الاقتحامية الصوتية في الوقت الفعلي أقل تواتراً من الرسائل الاقتحامية على البريد الإلكتروني، لكن ضرره على مستعمل الخدمة يُعتبَر أكبر بكثير. إذ إن الرسائل الاقتحامية الصوتية في الوقت الفعلي شديدة الإزعاج لمستقبليها. ففي خدمة البريد الإلكتروني، يستطيع مستعملو الخدمة تفقّد البريد متى شاؤوا، ويستطيعون التعرف على الرسائل الاقتحامية على بريدهم الإلكتروني في قليلٍ من الوقت، وحذف الرسائل الاقتحامية بجهد ضئيل نسبياً. أما الرسائل الاقتحامية الصوتية في الوقت الفعلي فإنها أشد تطفلاً، على اعتبار أنها تحتاج من متلقيها إجابة فورية. وإضافة إلى ذلك، يلزم وقت أطول لتحديد أن الرسالة المستقبلة عبارة عن رسالة اقتحامية صوتية. وهذه الرسائل الاقتحامية أقوى فعالية، مقارنة بالرسائل الاقتحامية على البريد الإلكتروني واقتحام خدمة الرسائل القصيرة (SMS) المتنقلة. إذ يحاول المقتحمون عادة إقناع متلقي الرسالة الاقتحامية بشراء منتَج معيّن أو خدمة معيّنة. وفي الرسائل الاقتحامية الصوتية في الوقت الفعلي، يحاول المروّجون عن طريق اتصال تفاعلي إقناع مستقبل الرسالة الاقتحامية وهي وسيلة أكثر اقتحاماً وتأثيراً على المستقبل، مقارنة بالرسائل الاقتحامية على البريد الإلكتروني وعلى خدمة الرسائل القصيرة (SMS) حيث يقتصر الاقتحام على تسليم نص قصير

أو مادة فيديوية بنسق غير تفاعلي. ويزداد عادة ضرر الاقتحام، كلما ازداد معدّل الإقناع من خلال الاقتحام. وهكذا، فإن الضرر الناجم عن الرسائل الاقتحامية الصوتية في الوقت الفعلي يمكن أن يكون كبيراً نسبياً، بالنظر إلى كمية الرسائل الاقتحامية.

وقد يعمل مستعملو الرسائل الاقتحامية الصوتية في الوقت الفعلي على تحسين فعالية هذا النمط من الاقتحام، باستعمالهم مختلف الخدمات القائمة على بروتوكول الإنترنت (IP) التكميلية، بالإضافة إلى الاتصالات الصوتية الأساسية. إذ إن الرسالة الاقتحامية الصوتية في الوقت الفعلي تسلَّم عادة إلى المستهدَفين بها بواسطة مطاريف تدعم خدمة المهاتفة عبر بروتوكول الإنترنت (VoIP). والكثير من مطاريف هذا النوع يمكنه دعم وظائف كثيرة إضافية مثل مراسلة الوسائط المتعددة، والمهاتفة الفيديوية، وتقاسم شاشة العرض، إلى جانب وظيفة الاتصالات الصوتية كوظيفة بالتغيّب. فيستطيع المقتحمون أن يحاولوا زيادة تأثير الرسائل الاقتحامية بالجمع بين الرسائل الاقتحامية الصوتية في الوقت الفعلي وخدمات إضافية كالفيديو أو النص.

ويمكن أن تكون الرسائل الاقتحامية الصوتية في الوقت الفعلي غير قانونية أو احتيالاً بنية شريرة، كما هو معروف حدوثه في خدمات المهاتفة السلكية التقليدية والمهاتفة المتنقلة. زِد على ذلك أن رُخص أسعار المهاتفة عبر بروتوكول الإنترنت (VoIP) من شأنه أن يجعل هذا الاقتحام الصوتي غير القانوني على المهاتفة عبر بروتوكول الإنترنت (VoIP) أنشط مما كان في خدمات المهاتفة التقليدية. مثلاً: يمكن لمقتحمون أشرار محاولة الحصول على معلومات مالية بتسليم رسالة تمويه صوتي على المهاتفة عبر بروتوكول الإنترنت (VoIP)، أي رسالة تمويه صوتي (vishing)، للحصول بصورة غير قانونية على معلومات عن مستعملي الخدمة. ويستطيع المقتحمون الأشرار إرسال رسالة اقتحامية طُعم لاجتذاب مستقبلها إلى استعمال خدمة عالية التكلفة دون أن يكون في نيته استعمالها. مثلاً: يستطيع المقتحمون استعمال آلة مؤتمتة ترنّ مرة واحدة. وتقيم هذه الآلة التوصيل مع متلقي الرسالة الاقتحامية وتنهي النداء بعد رنّة أو تقطع أو تفكّ التوصيل بعد كلمة قصيرة مثل "آلو". وفي هذه الحالة، يميل كثير من المتلقين إلى إقامة النداء ثانية باستعمال معلومات معرف هوية طالب النداء. عندها يتم توصيل مستقبِل الرسالة الاقتحامية هذا بمنظومة إعلان أوتوماتية أو بخدمة ما باهظة التكلفة. وهذا النوع من الاقتحام يستهوي المقتحمين إلى حد كبير، لأن تكلفة الاقتحام منخفضة جداً. ويستطيع المقتحمون الأشرار إرسال رسائل اقتحامية على نمط الطُعم من خلال الاستغلال السيئ لهشاشة الأمن في نظام المهاتفة عبر بروتوكول الإنترنت (VoIP). مثلاً: يستطيع المقتحمون انتحال هويّات عن طريق اختطاف دورة نداء في المهاتفة عبر بروتوكول الإنترنت (VoIP). ويستطيع المقتحمون أن يجعلوا مستعمل خدمة المهاتفة عبر بروتوكول الإنترنت (VoIP) يتصل بهم عن طريق انتحالهم هوية مستعملين آخرين يريد المستعمل إقامة الاتصال معهم. وعلى نحو مماثل، يمكن أن تصادف في تطبيقات الوسائط المتعددة القائمة على بروتوكول الإنترنت (IP) أنواعاً مختلفة من الرسائل الاقتحامية من نمط الطعم من أجل إغراء المتلقين.

2.7 الرسائل الاقتحامية النصية في الوقت الفعلي

يمكن تعريف الرسائل الاقتحامية النصية في الوقت الفعلي بأنها رسائل نصية غزيرة غير مُلتمَسة، في الوقت الفعلي، بقصد الدعاية لمنتجات أو خدمات تجارية مثلاً. وتُصادَف الرسائل الاقتحامية النصية في الوقت الفعلي في كثير من تطبيقات الوسائط المتعددة القائمة على بروتوكول الإنترنت (IP) التي تؤدي وظيفة تسليم رسائل نصية في الوقت الفعلي بين مستعملي الخدمة. وتشبه الرسائل النصية في الوقت الفعلي تلك الخاصة بالبريد الإلكتروني في خصائصها، من حيث إن الرسالة الاقتحامية عبارة عن رسالة نصية. لكن الرسائل الاقتحامية النصية في الوقت الفعلي أكثر إزعاجاً من نظيرتها في البريد الإلكتروني، لأن مستقبلها ينقطع عمله وقت استلامها. ومن الأمثلة على الرسائل الاقتحامية النصية في الوقت الفعلي اقتحام المراسلة اللحظية واقتحام الدردشة.

وفي كثير من الخدمات المعتمدة على تطبيقات الوسائط المتعددة القائمة على بروتوكول الإنترنت (IP)، بما فيها خدمة المراسلة اللحظية، وخدمة الدردشة على الخط، وخدمة اللعب على الخط، تؤدى وظيفة تسليم الرسائل لمستعمِلي الخدمة مجاناً أو لقاء ثمن زهيد. وهكذا يستطيع المقتحمون إرسال رسائل اقتحامية نصية بتكاليف منخفضة جداً. وكثيراً ما يستطيع المقتحمون الحصول على معلومات عامة أو خاصة عن مستعملي الخدمة بطرائق متنوعة. وهذه المعلومات من شأنها أن تزيد منفعة المقتحمين المنشودة من عملية الاقتحام، مقارنة بالرسائل الاقتحامية على البريد الإلكتروني التي تستهدف أناساً غير محددين.

3.7 الرسائل الاقتحامية الفيديوية في الوقت الفعلي

يمكن تعريف الرسائل الاقتحامية الفيديوية في الوقت الفعلي بأنها رسائل فيديوية غير مُلتمَسة، في الوقت الفعلي، ترسل بقصد الدعاية لمنتج تجاري أو خدمة تجارية. ويشمل الفيديو هنا الصور الثابتة والمتحركة على السواء. وقد تظهر الرسائل الاقتحامية الفيديوية في الوقت الفعلي في خدمات تطبيقات الوسائط المتعددة القائمة على بروتوكول الإنترنت (IP) التي تؤدى بين وظيفة الاتصال الفيديوي في الوقت الفعلي لمستعملي الخدمة.

وفي أولى مراحل الاقتحام على تطبيقات الوسائط المتعددة القائمة على بروتوكول الإنترنت (IP)، يمكن تسليم الرسائل الاقتحامية النصية أو الصوتية بتكلفة منخفضة، وهي تُصنَع بدون صعوبة كبيرة، ولا تشكل عبئاً على شبكة قائمة على بروتوكول الإنترنت (IP). وقد تكون الرسائل الاقتحامية الصوتية في الوقت الفعلي بشكل ترويج عن بعد هي القسم الأكبر في الاقتحام على تطبيقات الوسائط المتعددة القائمة على بروتوكول الإنترنت (IP). ولكن، بالنظر إلى أن تكنولوجيا تبادل الوسائط والتسليم بين مستعملي خدمات تطبيقات الوسائط المتعددة القائمة على بروتوكول الإنترنت (IP) آخذة في التطور وبالنظر إلى أن مقدرة الشبكة آخذة في الازدياد، فقد بات من الممكن أن يتسع أيضاً نطاق انتشار الرسائل الاقتحامية الفيديوية في الوقت الفعلي.

4.7 الرسائل الاقتحامية الصوتية في غير الوقت الفعلي

يمكن تعريف الرسائل الاقتحامية الصوتية في غير الوقت الفعلي بأنها رسائل صوتية غزيرة، غير ملتمَسة، في غير الوقت الفعلي، ترسل بغرض الدعاية لمنتجات أو خدمات تجارية. والمثال النموذجي على هذا النوع من الرسائل الاقتحامية هو الرسالة الصوتية المسجَّلة.

في كثير من الحالات، تستطيع خدمة المهاتفة عبر بروتوكول الإنترنت (VoIP) دعم خدمة المراسلة المتعددة الوسائط، مثل إرسال واستلام رسائل نصية وسمعية وفيديوية، بالإضافة إلى وظيفة توصيل النداء الصوتي في الوقت الفعلي. وهكذا يستطيع المقتحمون إرسال رسالة اقتحامية صوتية مسجلة بالفعل في مطراف المستقبِل، مستعملين هذه الوظيفة من وظائف خدمة المهاتفة عبر بروتوكول الإنترنت (VoIP). وهذا النوع من الرسائل الاقتحامية الصوتية يسبب ضرراً كبيراً لمستعملي خدمة المهاتفة عبر بروتوكول الإنترنت (VoIP) ومورديها، حيث تشغل صندوق البريد الصوتي أو مستودع التخزين، لأن حجم الرسالة الاقتحامية الصوتية كبير.

5.7 الرسائل الاقتحامية النصية في غير الوقت الفعلي

يمكن تعريف الرسائل الاقتحامية النصية في غير الوقت الفعلي بأنها رسائل نصية غزيرة غير مُلتمَسة، في غير الوقت الفعلي، ترسل بقصد الدعاية لمنتجات أو خدمات تجارية. وتشبه الرسائل الاقتحامية النصية في الوقت غير الفعلي في خصائصها الرسائل الاقتحامية على البريد الإلكتروني. ويمكن للرسائل الاقتحامية النصية في غير الوقت الفعلي أن تظهر في كثير من تطبيقات الوسائط المتعددة القائمة على بروتوكول الإنترنت (IP)، نظراً لسهولة استحداث وتسليم رسالة نصية، ولانخفاض تكلفة الاقتحام عادة.

والرسالة الاقتحامية النصية في غير الوقت الفعلي يمكن تسليمها إلى مطاريف قائمة على بروتوكول الإنترنت (IP) ذات مقدرة لاستلام رسالة نصية طويلة، مثل البريد الإلكتروني، أو إلى هواتف خدمة المهاتفة عبر بروتوكول الإنترنت (VoIP)، ذات المقدرة لاستلام رسائل نصية قصيرة كرسائل SMS التي يستقبلها الهاتف المتنقل. ويمكن تسليمها عبر كثير من خدمات تطبيقات الوسائط المتعددة القائمة على بروتوكول الإنترنت (IP)، بما فيها المراسلة اللحظية (IM) والخدمات الإلكترونية المختلفة. ويوجد، إضافة إلى هذه الأنماط من الرسائل الاقتحامية النصية التي تُسلَّم إلى المستقبِل دون رغبته، أنواع أخرى من الرسائل الاقتحامية النصية التي يتعرض لها مستعملو خدمات قائمة على بروتوكول الإنترنت (IP)، مثل الدعايات على مواقع الويب. إن خصائص الرسائل الاقتحامية النصية في غير الوقت الفعلي شبيهة بخصائص الرسائل الاقتحامية على البريد الإلكتروني، ومن ثم يمكن أن تطبَّق عليها كثير من التقنيات المضادة للرسائل الاقتحامية على البريد الإلكتروني. وقد تقل قابلية تطبيق هذه التقنيات حين يقل طول الرسالة الاقتحامية النصية.

6.7 الرسائل الاقتحامية الفيديوية في غير الوقت الفعلي

يمكن تعريف الرسائل الاقتحامية الفيديوية في غير الوقت الفعلي بأنها رسائل فيديوية غزيرة غير مُلتمَسة، في غير الوقت الفعلي، بقصد الدعاية لمنتجات أو خدمات تجارية. ويكون هذا النوع من الرسائل الاقتحامية على أحد النمطين التالي بيانهما: يتلقى مستعملو خدمة قائمة على بروتوكول الإنترنت (IP) أو يقومون بتحميل ملف رسالة اقتحامية فيديوية، أو ينفُذ مستعملو خدمة قائمة على بروتوكول الإنترنت (IP) إلى رسالة اقتحامية فيديوية بشكل الفيديو عند الطلب (VoD)، من خدمات تطبيقات الوسائط المتعددة القائمة على بروتوكول الإنترنت (IP). وتنقسم طرائق تسليم الرسائل الاقتحامية الفيديوية في غير الوقت الفعلي إلى نوعين. الأول: قد يستلم المستقبِل الملفات الإعلانية الفيديوية التي أرسلها المقتحِم بدون قصد. والثاني: يقوم مستعملو خدمات تطبيقات الوسائط المتعددة القائمة على بروتوكول الإنترنت (IP) بتحميل ملفّات الرسائل الاقتحامية عن طريق خدمات تبادل الملفات، دونما ظن بأن الملفّ عبارة عن رسالة اقتحامية.

وحين يقوم المستقبل بتحميل ملف الرسالة الاقتحامية الفيديوية، يلحقه ضرر إضاعة الوقت والجهد في تنزيل هذا الملف. وحين يستلم المستقبِل الرسالة الاقتحامية الفيديوية بغض النظر عما إذا كان ذلك بقصد أو عن غير قصد، تضر الرسالة الاقتحامية مستعمليَ الخدمة وموردِيها عن طريق شَغْل صندوق البريد أو حيِّز التخزين، على اعتبار أن الرسالة الاقتحامية الفيديوية تكون كبيرة الحجم بوجه عام.

8 المسألة التقنية المتعلقة بمكافحة اقتحام الوسائط المتعددة القائمة على بروتوكول الإنترنت (IP)

على غرار مكافحة الرسائل الاقتحامية على البريد الإلكتروني أو الخدمة SMS على الهواتف المتنقلة، فيما يلي سلسلة من الإجراءات المتعلقة باستحداث وإرسال ومنع الرسائل الاقتحامية التي ترسل على خدمات تطبيقات الوسائط المتعددة القائمة على بروتوكول الإنترنت (IP):

- استحداث الرسائل الاقتحامية وتسليمها؛
- كشف وترشيح الرسائل الاقتحامية على يد المستعملين و/أو موردي خدمة تطبيقات الوسائط المتعددة القائمة على بروتوكول الإنترنت (IP)؛
- تدابير المكافحة الواجب اتخاذها بشأن الرسائل الاقتحامية المستقبلة.

قبل إقامة الإطار التقني لمكافحة اقتحام تطبيقات الوسائط المتعددة القائمة على بروتوكول الإنترنت (IP)، لا بد من تقصّي مواطن الضعف في الوقاية من هذا النمط من الاقتحام، إزاء الإجراءات المذكورة أعلاه. ومراعاة لجوانب الضعف، ينبغي النظر عند كل خطوة من خطوات مكافحة اقتحام تطبيقات الوسائط المتعددة القائمة على بروتوكول الإنترنت (IP). في كل نمط من أنماط الوسائل التقنية ويرد أدناه تحليل مدى تأثير هذه الوسائل التقنية على عمليتَيْ استحداث وتسليم مُقحَمات هذه التطبيقات. فعند دراسة الإطار التقني والوسائل التقنية لمكافحة اقتحام الوسائط المتعددة القائمة على بروتوكول الإنترنت (IP)، سيكون تحليل المسألة الوارد في هذا المقطع مفيداً عند تحديد الوسيلة الناجعة لمكافحة اقتحام هذه التطبيقات.

1.8 استحداث الرسائل الاقتحامية وتسليمها

الافتراض الأساسي في عملية نشر الرسائل الاقتحامية على الوسائط المتعددة القائمة على بروتوكول الإنترنت (IP) هو أن تكون تكاليف الاقتحام منخفضة بالقياس إلى الربح الذي يتوقعه المقتحم من هذا الاقتحام. ولا تقتصر تكاليف الاقتحام على التكاليف المالية، بل تشمل أنواعاً شتى من الموارد كالوقت والجهد والصعوبة التقنية المطلوبة لاستحداث هذه الرسائل الاقتحامية وتسليمها. فالعوامل المؤثِّرة في تكاليف الاقتحام هي:

- تكلفة تجميع العناوين المستهدفة أو أرقام الهواتف المستهدفة: التكلفة التي يستلزمها تجميع العناوين وأرقام الهواتف المستهدفة بالاقتحام.
- تكلفة استحداث وتسليم الرسائل الاقتحامية: التكلفة التي يتحملها المقتحِم من أجل إنشاء وتسليم الرسائل الاقتحامية.

1.1.8 تجميع قائمة أهداف

قبل إرسال الرسائل الاقتحامية يتعيّن، قبل كل شيء، تجميع قائمة أهداف ترسل إليها هذه الرسائل. ويستطيع المقتحِم أن يحصل، بدون صعوبة كبيرة، على قائمة أهداف للرسائل الاقتحامية على البريد الإلكتروني، باعتداء معجمي النمط، وبواسطة برامج تجميع عناوين البريد الإلكتروني، وبالنفاذ غير المشروع إلى قائمة أهداف مجمَّعة. وفي حالة اقتحام الخدمة SMS للهواتف المتنقلة، يكفيه إجراء عملية توافقية بسيطة على الأرقام لتجميع قوائم الأهداف، على اعتبار أن مصدر أرقام الهواتف المتنقلة محدود.

ومن الجائز في نمط معرِّف الهوية الشخصي الخاص المستعمَل للاتصال وتبادل الرسائل بين مستعمِلي خدمة تطبيقات الوسائط المتعددة القائمة على بروتوكول الإنترنت (IP)، أن يتغير تبعاً لنمط هذه التطبيقات، وللبروتوكول، واللوائح الوطنية، وما إلى ذلك. فمعرِّفات الهوية الشخصية الممكن استعمالها في خدمة المهاتفة عبر بروتوكول الإنترنت (VoIP)، قد تكون بشكل أرقام هاتف، شبيهة بالأرقام المستعملة في خدمة الشبكة الهاتفية العمومية التبديلية (PSTN)، أو لعناوين بروتوكول الإنترنت (IP) أو لعنوان حساب في خدمة قائمة على بروتوكول الإنترنت (IP) مثل عنوان حساب البريد الإلكتروني، وما إلى ذلك. وبخصوص المراسلة اللحظية (IM)، يُستعمَل عادة عنوان البريد الإلكتروني معرِّفاً للهوية الشخصية، ويمكن أن تُستعمَل أيضاً أنواع أخرى من المعلومات مثل رقم الهاتف المتنقل.

فحين تكون هذه الأنواع من معرِّفات الهوية الشخصية مستعملة للمهاتفة عبر بروتوكول الإنترنت (VoIP) والمراسلة اللحظية (IM)، يستطيع المقتحمون تجميع المعرِّفات الشخصية وما يناظرها من حسابات هذه الخدمات، مستعملين لتجميع القوائم المستهدفة نفس الطرائق الموجودة المستعملة لاقتحام البريد الإلكتروني. فيُتوقَّع أن يتم تجميع عناوين مستعملي المهاتفة عبر بروتوكول الإنترنت (VoIP) والمراسلة اللحظية بدون صعوبة كبيرة، عن طريق اعتداء من النمط المعجمي، أو عن طريق برنامج لتجميع معرِّفات الهوية بالبحث عبر الشبكة، وغير ذلك من الطرائق.

عدا اقتحام المهاتفة عبر بروتوكول الإنترنت (VoIP) والمراسلة اللحظية (IM)، تُصادف أنماط اقتحام متنوعة في تطبيقات الوسائط المتعددة القائمة على بروتوكول الإنترنت (IP)، مثل خدمات الدردشة، وخدمات اللعب على الخط، والخدمات المعتمِدة على العلاقة بين نظيرين، وغير ذلك. وفي صدد هذه التطبيقات أيضاً يبدو أن تجميع قائمة مستهدفين لا يتطلب جهداً كبيراً. إذ إن كثيراً من تطبيقات الوسائط المتعددة القائمة على بروتوكول الإنترنت (IP) هذه، كالخدمات على الخط، تستعمل النمط الشائع استعماله من الحسابات، كعنوان البريد الإلكتروني ورقم الهاتف، معرِّفاً للهوية الشخصية. وليس من الصعب عادة الوصول إلى قائمة مستعملي خدمات تطبيقات الوسائط المتعددة القائمة على بروتوكول الإنترنت (IP) المقصورة على المستعملين المخولين، وتسليم ملفات أو رسائل. فنظراً إلى هذه الأمور، سيظل غير صعب على المقتحمين، من حيث التكنولوجيا واقتصادياً، تحصيل معرِّفات الهوية الشخصية لمستعملي خدمات تطبيقات الوسائط المتعددة القائمة على بروتوكول الإنترنت (IP) المتعددة الوسائط، ما لم تُتّخذ تدابير محددة تصعِّب ذلك على المقتحمين.

2.1.8 استحداث الرسالة الاقتحامية وتسليمها

يُتوقّع أن تكون تكاليف إنشاء وتسليم رسائل اقتحامية على تطبيقات الوسائط المتعددة القائمة على بروتوكول الإنترنت (IP) هي القسم الأكبر من تكاليف اقتحام هذه التطبيقات. إذ إن خدمة المهاتفة عبر بروتوكول الإنترنت (VoIP) أو خدمة الاتصالات الصوتية عبر شتى تطبيقات الوسائط المتعددة القائمة على بروتوكول الإنترنت (IP) تكلِّف في المعتاد أقل من خدمة المهاتفة السلكية المعتمِدة على الدارة أو خدمة الهاتف المتنقل. ولذا، فإن المهاتفة عبر بروتوكول الإنترنت (VoIP) أو خدمة الاتصالات الصوتية عبر تطبيقات الوسائط المتعددة القائمة على بروتوكول الإنترنت (IP) تشكل هدفاً مغرياً لتسليم الرسائل الاقتحامية بالنسبة إلى المقتحمين التقليديين الذين عملوا حتى اليوم بالترويج عن بعد بواسطة خدمات المهاتفة التقليدية السلكية أو اللاسلكية. علاوة على ذلك، تعتبر نداءات المسافات الطويلة والنداءات الدولية أرخص بكثير في هذه الخدمات منها في الخدمات الهاتفية التقليدية. وهكذا يمكن أن ينتشر الاقتحام الترويجي في بلدان أخرى تستعمل نفس اللغة، ويمكن أن تُستحدث الرسائل الاقتحامية الترويجية انطلاقاً من بلدان أخرى تكون فيها تكاليف المروِّج عن بعد وتكاليف تسليم الرسائل الاقتحامية منخفضة جداً.

وبالإضافة إلى خدمة المهاتفة عبر بروتوكول الإنترنت (VoIP)، يوفَّر مجاناً أو بتكلفة منخفضة جداً كثير من خدمات تطبيقات الوسائط المتعددة القائمة على بروتوكول الإنترنت (IP)، كالمراسلة اللحظية (IM) والخدمة المعتمِدة على العلاقة بين نظيرين (P2P) وخدمة الدردشة على الخط. ولذا لا يتوقَّع أن يستلزم استحداث الرسائل الاقتحامية وتسليمها على هذه التطبيقات كثيراً من الجهد أو التكلفة لكونها لا تتطلب في المعتاد كثيراً من المال أو الوقت ولا تنطوي على مصاعب تقنية.

2.8 كشف الرسائل الاقتحامية وترشيحها

إن كشف وترشيح الرسائل الاقتحامية على تطبيقات الوسائط المتعددة القائمة على بروتوكول الإنترنت (IP) هو أهم نقطة تقنية في مكافحة الاقتحام مكافحة فعالة. ومن الممكن عملياً استبعاد الرسائل الاقتحامية على البريد الإلكتروني في مخدم مورد خدمة الإنترنت (ISP)، أو في شبكة داخلية أو في مطراف مستقبِل البريد الإلكتروني قبل أن يتفقّد هذا المستقبل الرسائل الاقتحامية في صندوق بريده، على اعتبار أن خدمة البريد الإلكتروني تعتمد آلية تخزين الاتصالات ثم إعادة تسييرها. فيمكن استبعاد مقدار من الرسائل الاقتحامية على البريد الإلكتروني بواسطة تطبيقات تستعمل تقنيات ترشيح متنوعة، مثل تحليل المحتويات، لأن أغلبية رسائل البريد الإلكتروني محتوياتها معتمدة على النص. ولكن، خلافاً لحالة الرسائل الاقتحامية على البريد الإلكتروني، يُعتبَر من الصعب ترشيح الرسائل الاقتحامية على الوسائط المتعددة القائمة على بروتوكول الإنترنت (IP)، بسبب الخصائص التالية لهذه التطبيقات:

- حصول الاتصالات في الوقت الفعلي.
- صعوبة تحليل المحتويات الصوتية والفيديوية.
- صعوبة استيقان المقتحمين.

وتوفر بعض تطبيقات الوسائط المتعددة القائمة على بروتوكول الإنترنت (IP)، كالمهاتفة عبر بروتوكول الإنترنت (VoIP) والمراسلة اللحظية (IM)، اتصالات في الوقت الفعلي بين مستعملي الخدمة. وتسليم الرسائل الاقتحامية على هذه التطبيقات إلى المستقبِل يتم في الوقت الفعلي، بدون تخزين في المخدم. وفي بعض الحالات، لا تمر محتويات المهاتفة عبر بروتوكول الإنترنت (VoIP) والمراسلة اللحظية (IM) على مخدمات موردي الخدمات، بل تتسلم مباشرة إلى مستعمِل الخدمة. ولذا فإنه من الصعب الحصول على معلومات كافية عن الاتصال وتحليل محتوياته للتعرف على الرسالة الاقتحامية قبل إقامة النداء أو قبل تسليم الرسالة. مثلاً: متى تمت إقامة النداء بين مرسل ومستقبل الرسالة الاقتحامية، وعرف المستقبل أن هذه رسالة اقتحامية، يكون قد فات الآوان على ترشيح الرسالة الاقتحامية، على اعتبار أن التوصيل قد تم. وفي حالة اقتحام المراسلة اللحظية (IM)، ربما كان بالإمكان تحليل محتويات الرسالة اللحظية في غضون وقت قصير جداً، على اعتبار أن هذه الرسائل معتمدة على النص عادة. لكن قصر هذه الرسائل من شأنه أن يخفف فعالية تقنيات الترشيح التقليدية التي طوِّرت لمكافحة اقتحام البريد الإلكتروني. ومطاريف مستعملي الخدمة تتولّى مسؤولية ترشيح الرسائل الاقتحامية عندما لا تمر محتويات رسائل تطبيقات الوسائط المتعددة القائمة على بروتوكول الإنترنت (IP) عبر مخدم مورد خدمة الإنترنت. لكن إضافة ترشيح الرسائل الاقتحامية إلى مطاريف مستعملي الخدمة، مع إدارة المستعملين لوظيفة الترشيح هذه، ليس بالأمر البسيط. ومن ثم، فإن كشف وترشيح الرسائل الاقتحامية على تطبيقات الوسائط المتعددة القائمة على بروتوكول الإنترنت (IP) في الوقت الفعلي، كالرسائل الاقتحامية على المهاتفة عبر بروتوكول الإنترنت (VoIP) والمراسلة اللحظية (IM)، بطريقة تحليل المحتويات قد لا يصلح.

وربما أمكن اعتماد آليات تخزين الاتصالات ثم إعادة تسييرها مع بعض تطبيقات الوسائط المتعددة القائمة على بروتوكول الإنترنت (IP) التي لا تستلزم بالضرورة أن تتم في الوقت الفعلي، مثل المراسلة المتعددة الوسائط. وتسليم الملفات عبر الاتصال بين نظيرين (P2P)، يمكن أن تكون تقنية لمكافحة الاقتحام عن طريق تحليل المحتويات بناء على طلب موردي الخدمات أو مستعمليها. ومع ذلك، يظل من الصعب كشف الرسائل الاقتحامية وتصفيتها بطريقة تحليل المحتويات، لأن تكنولوجيا تمييز المواد الصوتية والفيديوية لم تبلغ بعد درجة النضوج، ولأن تطبيقات مثل هذه التكنولوجيا من شأنها أن تشكل عبئاً كبيراً على الشبكة.

ومن الممكن عملياً أيضاً التعرف على الرسائل الاقتحامية بالاستناد إلى المعلومات الخاصة بالمرسل، لا إلى معلومات الاتصالات نفسها. فيمكن تعرُّف ما إذا كان المرسل مقتحماً أم لا من خلال تقنيات متنوعة، مثل القوائم السوداء والقوائم البيضاء ونظام السمعة، وما إلى ذلك. لكن تطبيق هذه التقنيات على الرسائل الاقتحامية على تطبيقات الوسائط المتعددة القائمة على بروتوكول الإنترنت (IP) تكتنفه نقاط ضعف عديدة. أولاً، ليس من الصعب إنشاء حسابات خدمة أو معرفات هوية شخصية ل تطبيقات الوسائط المتعددة القائمة على بروتوكول الإنترنت (IP)، بل يمكن إنشاء كم كبير منها. وثانياً، يستطيع المقتحمون أن يضعوا بسهولة معرِّف هوية جديد إذا تم تصنيف معرِّف هويتهم القديم ضمن المقتحمين. وأخيراً، من الجائز أيضاً القول بأن هؤلاء المقتحمين هم بعض من مستعملي الخدمة العاديين، يسيئون استغلال جوانب الضعف الأمني لتطبيقات الوسائط المتعددة القائمة على بروتوكول الإنترنت (IP). فمراعاة لهذه الأمور، لا بد من الجمع بين تقنيات مكافحة الاقتحام التي تتعرّف على الرسالة الاقتحامية بالاستناد إلى معلومات المرسِل مع آليات استيقان فعالة.

3.8 الإجراءات المتخذة بشأن الرسائل الاقتحامية المستقبلة

يستطيع مستقبلو الرسائل الاقتحامية أن يتخذوا عدة إجراءات بعد استلامها. حيث يمكنه إضافة معرِّف هوية المقتحم إلى قائمة سوداء، لمنع المقتحم من إرسال مزيد من الرسائل الاقتحامية إليه أو إلى مستعملين آخرين. ويستطيع أيضاً أن يعطي عن المقتحم تقديراً سيئاً يظهر في أنظمة السمعة. ومن الممكن أيضاً الإبلاغ عن الاقتحام غير القانوني لمعاقبة المقتحمين. إلا أنه ليس من السهل، كما تقدم القول، تعرّف هوية المقتحمين عبر كثير من تطبيقات الوسائط المتعددة القائمة على بروتوكول الإنترنت (IP)، وليس من الصعب على المقتحمين وضع معرِّفات هوية جديدة. وهنا لا بد من اعتماد آلية استيقان فعالة لزيادة فعالية الإجراءات المضادة للرسائل الاقتحامية المستقبلة.

9 التهديدات الأمنية المرتبطة بالاقتحام

يتناول هذا القسم المسائل الأمنية المتعلقة باقتحام تطبيقات الوسائط المتعددة القائمة على بروتوكول الإنترنت (IP). فيعرِّف ويصنّف بعض التهديدات الأمنية ويذكر التدابير المضادة لها.

1.9 التهديدات الأمنية المرتبطة بالاقتحام

يبحث هذا القسم بعض التهديدات الأمنية التي تحصل في تطبيقات الوسائط المتعددة القائمة على بروتوكول الإنترنت (IP). فيعرِّف التهديدات الأمنية من زاوية إرسال الرسائل الاقتحامية إلى الشبكة. ويستطيع المقتحمون إرسال رسائل اقتحامية باستعمال الهجمات التقنية التالية في بيئات الوسائط المتعددة القائمة على بروتوكول الإنترنت (IP).

1.1.9 تجميع معرفات الهوية

لإرسال الرسائل الاقتحامية، يعمد المقتحم إلى تجميع معرِّفات هوية لكي يجد أهدافاً للاقتحام. وهكذا، فإن تجميع معرِّفات الهوية هو التهديد الأكثر شيوعاً بين تهديدات الاقتحام، وهو عملية تمهيدية لا بد منها. ويحاول المقتحم تجميع أكبر كم ممكن من معرّفات الهوية، إذ إن عدد المعرِّفات يعني عدد الأهداف التي يستطيع الهجوم عليها من منظور المقتحم. ومعرّفات الهوية يمكن تجميعها بطرائق متنوعة: مثلاً، بواسطة محرِّك بحث أو منتدى مفتوح أو غير ذلك. ويمكن توليد معرِّفات الهوية باستعمال ألفاظ أو أسماء عامة. وتُجمع أحياناً عن طريق معاملات غير مشروعة مع شركات أو مدارس يكون لديها معلومات شخصية كثيرة عن زبائنها.

ومما حصل في هذا النشاط استعمال معرِّفات هوية وحيدة كعنوان البريد الإلكتروني ومعرِّف هوية الموارد الموحَّد (URI) لتمييز المستعملين في كثير من تطبيقات الوسائط المتعددة القائمة على بروتوكول الإنترنت (IP). فالخدمات في تطبيقات الوسائط المتعددة القائمة على بروتوكول الإنترنت (IP) خلافاً للخدمة الهاتفية تتميز بمزايا عدة مثل تعدد قنوات الاتصال وانخفاض التكلفة وما إلى ذلك. ولهذا يحبذ المقتحمون كثيراً إرسال الرسائل الاقتحامية على وجه خاص في بيئات الوسائط

المتعددة القائمة على بروتوكول الإنترنت (IP). ومن ثَمّ ينبغي أن يكون المستعملون على حذر كبير بحيث يحمون معرّفات هويتهم ولا يتركونها عرضة للمقتحمين.

2.1.9 انتحال المقتحم هوية مرسل موثوق

الانتحال هو إحدى تقنيات القرصنة. يصنع غازي شبكة خبيث موقع ويب لنفسه ويُغري الناس بزيارة موقعه على الويب، لكي يكتسب تخويلاً من المستعمل، مستغلاً عيباً تنظيمياً في البروتوكول TCP/IP لسرقة المعلومات الشخصية لهؤلاء المغرر بهم. وعلاوة على ذلك، يستطيع المقتحم أن يُرسِل رسالة اقتحامية متنكّراً باسم شركة مشهورة، فيظن مستقبلها أنها من مرسِل موثوق. فهذه الرسالة الاقتحامية تتمتع بدرجة عالية لاحتمال قبولها. وهذا أيضاً يسمى "بالانتحال".

إن إرسال رسائل اقتحامية بانتحال هوية مرسل موثوق تهديد يتمثّل في تنكر المقتحم بصفة غيره، فيزوِّر حقل رأسية الرسالة أو يستعمل معرّف هوية مستعمَلاً لمرسل في تطبيقات الوسائط المتعددة القائمة على بروتوكول الإنترنت (IP). ومن شأن هذا التهديد أن يصيب القائمة البيضاء والقائمة السوداء بالخلل، وهما وسيلتان معروفتان لمكافحة الاقتحام. مثلاً: إذا غير المقتحم معرِّف هويته منتحلاً معرف هوية صالح لمستعمل مسجَّل عند المستقبِل في قائمة الرفاق أو في القائمة البيضاء، يستطيع المقتحم هكذا الالتفاف على السياسة المعتمِدة على القائمة البيضاء. وعلاوة على ذلك، بسبب طبيعة اتصالات الوسائط المتعددة، يكون من الصعب معرفة ما إذا كانت الرسالة هي من الرسائل الاقتحامية أم لا، قبل إقامة التوصيل. وعليه، ففي هذه الحالة، لا يستطيع المستقبِل إلا أن يخضع للاقتحام.

3.1.9 استشفاف معلومات التسجيل

استشفاف المعلومات هو السلوك الذي به يتنصّت المقتحم على التوصيلات الجارية بين مستعملين آخرين. والأداة المستعملة لذلك تسمّى المستشِفّ.

في بيئة الوسائط المتعددة القائمة على بروتوكول الإنترنت (IP)، يستطيع المقتحم إرسال رسائل اقتحامية باستعمال المستشِفّ استعمالاً غير مشروع. يعمد المقتحم أولاً إلى التنصت على معلومات تسجيل المستعمل الصالحة بواسطة مستشِفّ، ثم يستعمل المعلومات المكتسبة في توليد معلومات تسجيل ملفَّقة. وبعدئذ يُدرِج عنوان بروتوكول الإنترنت (IP) لمهاجم بدلاً من عنوان بروتوكول الإنترنت (IP) الصالح الخاص بالمستعمل، في رسالة التسجيل. وبعدئذ يستطيع المقتحم إرسال الرسائل الاقتحامية باستعمال التسجيل الملفَّق.

4.1.9 سرقة الدورة

سرقة الدورة هي تقنية بها يختطف شخص ما دورة اتصال بين مستعملين آخرين. وتُستعمل هذه التقنية لإرسال رسائل اقتحامية في بيئات الوسائط المتعددة القائمة على بروتوكول الإنترنت (IP). حيث يقوم المقتحم بفك التوصيل عنوة بين المستعمِلَيْن الآخرين في منتصف الدورة. وفي هذه الحالة، يحاول المستعملان الآخران إعادة إنشاء الدورة الجارية. وعندئذ يستطيع المقتحم سرقة الدورة، وإدراج إرسال وسائطي، معتَمِد على بروتوكول النقل بالوقت الفعلي (RTP)، يحتوي على رسالة اقتحامية في منتصف الدورة المعاد إنشاؤها.

5.1.9 حقن لغة استجواب مُبَنْيَنة

حقن لغة استجواب مبنينة (SQL) هو تقنية قرصنة تعطي نتائج غير عادية، عن طريق إدراج قواعد تركيب استجوابية لم يقصدها طالب الخدمة. وفي بيئة تطبيقات الوسائط المتعددة القائمة على بروتوكول الإنترنت (IP)، يمكن أن يُستعمل حقن لغة SQL حين تُطبّق آلية "HTTP Digest" من أجل الاستيقان. في هذه المناسبة يعدّل المقتحم رأسية الاستيقان ويُدرِج استجواباً مزيَّفاً بلغة SQL. ثم يزوِّر رأسية استيقان للرسالة في المخدم الوكيل تستعملها آلية "HTTP Digest" للاستيقان، ويُدرِج استجواباً مزيّفاً بلغة SQL. وإذا انتهت هذه الهجمة بنجاح، يستطيع المقتحم أن ينتحل شخصية مستعمل مُستَيْقَن، فيرسل رسائل اقتحامية تخويلها صالح بتلفيقه معلومات تسجيل لمستعمل صالح.

6.1.9 برنامج بوت (Bot) الاقتحامي

البوت الاقتحامي (Spam Bot) هو روبوت شرير بشكل برنامج أو شفرة يمكن التحكم فيه وتشغيله من موقع بعيد، ولكنه غير قابل لأن ينشط ذاتياً. على وجه العموم، يكون التحكم فيه عن طريق توصيل يستعمل بروتوكول الدردشة عبر الإنترنت (بروتوكول IRC). والشبكة المكوّنة من روبوتات تسمّى شبكة بوت (botnet). ومن الممكن لمقتحم أن يتحكم بكثير من الأنظمة الملوَّثة بواسطة أمر تحكم واحد، لأن الشبكات بوت يمكن ربطها ببعض. وعليه، فإن المقتحم يستطيع بواسطة هذه التقنية أن يرسل كمية كبيرة من الرسائل الاقتحامية في تطبيقات الوسائط المتعددة القائمة على بروتوكول الإنترنت (IP).

7.1.9 تسميم النسخة الخفية لنظام أسماء الميادين

تسميم النسخة الخفية لنظام أسماء الميادين هو هجمة تضع عناوين مغلوطة مكان عناوين ميادين صحيحة. وفي تطبيقات الوسائط المتعددة القائمة على بروتوكول الإنترنت (IP)، يُستعمَل تسميم النسخة الخفية لنظام أسماء الميادين من أجل بروتوكول استبانة العنوان (ARP) وبروتوكول اكتشاف الجار (NDP). والبروتوكول ARP يُستعمَل لمواءمة عنوان بروتوكول الإنترنت (IP) وعنوان MAC (التحكم بالنفاذ إلى الوسائط) في شبكة قائمة على الإصدار 4 لبروتوكول الإنترنت (IPv4)؛ ويُستعمَل البروتوكول NDP لاكتشاف الجيران في الشبكات القائمة على الإصدار 6 لبروتوكول الإنترنت (IPv6). ويعاد تسيير رزم البروتوكولين ARP وNDP إلى جميع الأجهزة الموصَّلة بوصلة واحدة. فيستطيع المقتحم أن يستعمل طريقة تسميم النسخة الخفية لتعديل محتويات النسخة الخفية لأحد هذين البروتوكولين، باعتراضه الرزم المعاد تسييرها.

مثلاً: يستطيع المقتحم أن يتنكر بصفة بوابة، فيستعمل تسميم النسخة الخفية للبروتوكول ARP ليعترض جميع الرزم في نفس الوصلة. وهكذا يستطيع المقتحم، إذا بدأ المستعمل توصيلاً، أن يُدرج، في الدورة الجارية رسالة اقتحامية معتمدة على بروتوكول النقل بالوقت الفعلي (RTP) مجهزة مسبقاً. ويستطيع المقتحم تغيير معرِّف هوية المستعمِل المستهدَف. وإذا تم تغيير معرِّف هوية المستعمِل المستهدَف، يحاول المستعمل إقامة توصيل آخر مع طرف آخر يكون معرِّف هويته هو الذي زوّره المقتحم ولكن ليس هو الطرف الأصلي. فبواسطة هذه الهجمة، يستطيع المقتحم أن يرسل رسالة اقتحامية إلى المستعمل الذي يطلب التوصيل.

8.1.9 التحكم بالتسيير

لنفترضْ أن الاتصال في إطار تطبيقٍ وسائط متعددة قائمة على بروتوكول الإنترنت (IP) جارٍ بين أجهزة تسيير ومستعملين، وأن المقتحم يمكن أن يقوم على سبيل القرصنة بدور تسيير في الاتصال الجاري داخلِ الشبكة. فإذا حاول مستعمل إنشاء توصيل مع مستعمل آخر ينتمي إلى هذه الشبكة المعيّنة، يستجيب المقتحم لطلبه متنكراً بصفة مستعمل صالح، ويرسل رسالة اقتحامية إلى المستعمل الذي طلب إقامة التوصيل.

9.1.9 ضعف نظام الإدارة

وهناك نمط تهديد آخر يستغل جوانب الضعف في نظام إدارة الخدمات. وفي هذه الحالة، يستطيع مقتحم تعديل معلومات التسجيل لمستعمل صالح، وإرسال رسالة اقتحامية باستعمال خصائص المستعمِل الصالح.

2.9 تصنيف التهديدات الأمنية المرتبطة بالاقتحام

يمكن تصنيف التهديدات الأمنية المذكورة أعلاه المرتبطة بالاقتحام تبعاً لتقنية الهجوم. ويعرض الجدول 9-1 هذا التصنيف.

الجدول 9-1 – تصنيف التهديدات الأمنية المرتبطة بالاقتحام تبعاً لتقنية الهجوم

تقنية الهجوم	التهديدات الأمنية المرتبطة بالاقتحام
شفرة شريرة/تحكم عن بعد	اقتحام بواسطة برنامج روبوت
سرقة الدورة	سرقة الدورة
حقن لغة SQL	حقن لغة استجواب مُبَنْيَنة (SQL)
الاستشفاف	استشفاف معلومات التسجيل
الانتحال	انتحال صفة المرسل، تسميم النسخة الخفية، التحكم بالتسيير
تقنيات أخرى	تجميع معرِّفات الهوية، ضعف نظام الإدارة

تقنية "الشفرة الشريرة/التحكم عن بعد" تمكّن من إرسال كمية كبيرة من الرسائل الاقتحامية بسهولة. فالمقتحم يستطيع توزيع شفرات شريرة بوسائل عديدة، والتحكم بالأجهزة الملوّثة لإرسال الرسائل الاقتحامية. ومن الأمثلة على ذلك برامج بوت للاقتحام.

وسرقة الدورة هي تقنية قرصنة تمكّن من سرقة دورة خاصة بشخص ما. ويمكن عادة إنفاذها بمجرد حزر معرِّف هوية الدورة واستعمال واشي (cookie) معرِّف هوية الدورة. فيستطيع المقتحم التنصّت على الاتصال القائم بين مخدم ومستعمِل دون الخضوع لإجراء الاستيقان أو تخويل المخدم.

وتقنية "حقن لغة استجواب مُبَنْيَنة (SQL)" هي مهارة قرصنة تستغل ضعف الحماية لقاعدة البيانات. وهذه التقنية من شأنها تغيير اللغة SQL العادية، وتجاوز عملية الاستيقان، بطريقة غير قانونية. وفي المعتاد، تُستعمل هذه الطريقة في عمليات القرصنة على مواقع الويب لسرقة معلومات المستعمِل.

و"الاستشفاف" تقنية تمكّن القرصان من التنصّت على تبادل الرزم بين مستعمِلَيْن أو أكثر.

و"الانتحال" تقنية تقوم على التنكر بصفة شخص آخر. ومن شأن هذه التقنية أن تخدع آلة الطرف الآخر فتجعلها تعتقد أن المقتحم هو شخص آخر موثوق.

3.9 التدابير المضادة

يوجد ثلاثة تدابير مضادة لحل مشكلة الاقتحام المتقدم عرضها: الاستيقان، والتخويل، وإدارة الأمن. يُقصَد بـ"إدارة الأمن" التدبير المضاد الذي يمكن تطبيقه على تشكيلة أمنية مناسبة، بتركيب وحدة أمنية ملحقة في بنيان المنظومة من أجل صيانتها وإصلاحها وزيادة وعي المستعمل لأمور الأمن. وهناك عدد من التدابير المضادة، مثل التحكم في التدفق، والتجفير، وغير ذلك، مما يمكن بحثه. أما هذا القسم فيتناول التدابير المضادة الثلاثة الرئيسية.

والعلاقات بين التدابير المضادة وتهديدات الاقتحام الأمنية يختصرها الجدول 9-2 التالي.

الجدول 9-2 – العلاقات بين التدابير المضادة وتهديدات الاقتحام الأمنية للاتصالات المتعددة الوسائط

التدابير المضادة / التهديدات	الاستيقان	التخويل	إدارة شؤون الأمن
تجميع معرِّفات الهوية			X
انتحال صفة المرسِل	X		
استشفاف معلومات التسجيل	X		
سرقة الدورة	X		
حقن لغة استجواب مُبَنْيَنة (SQL)		X	X
برنامج بوت الاقتحامي			X
تسميم النسخة الخفية	X		
التحكم بالتسيير	X		
هشاشة النظام الإداري		X	X

يمكّن الاستيقان من درء كثير من تهديدات الاقتحام بحله مشاكل الانتحال. فالانتحال يُستعمَل في كثير من التهديدات: مثل انتحال صفة المرسل، واستشفاف معلومات التسجيل، وسرقة الدورة، وتسميم النسخة الخفية، والتحكم بالتسيير. ففي معالجة انتحال صفة المرسِل، يُستَيقَن كل مرسل بإجراء الاستيقان بعد استلام الرسالة. وفي درء هجمات استشفاف معلومات التسجيل، يُمنَع المستعمِل غير المستَيْقَن من تعديل معلومات التسجيل، بفضل إجراء الاستيقان. وفي درء هجمات سرقة الدورة وتسميم النسخة الخفية، يستطيع المستعمِل المستَيْقَن منه الانضمام إلى الاتصالات الجارية. وبخصوص التحكم في التسيير، لا يتحكم بجهاز التسيير إلا المستعمِل المستَيْقَن منه.

لكن الاستيقان لا يكفي لدرء تهديدات الاقتحام الأمنية المتمثلة في حقن لغة استجواب مُبَنْيَنة (SQL). ولذا يتعيّن في مثل هذه الحالة وضع سياسة تخويل. ويدخل في هذه الحالة هشاشة النظام الإداري. فينبغي أن يعطي مدير النظام تخويلات نفاذ مختلفة باختلاف حسابات المستعملين.

وفي النهاية، يتطلب بعض تهديدات الاقتحام الأمنية عناية بإدارة الأمن. ويدخل في هذه الحالة تجميع معرِّفات الهوية، وحقن لغة استجواب مُبَنْيَنة (SQL)، وبرنامج بوت اقتحامي، وهشاشة النظام الإداري. فالمقتحم يستطيع تجميع معرّفات هوية المستعملين بطرائق كثيرة ثم يرسل الرسائل الاقتحامية. ولذا يتعيّن تشديد الحرص في إدارة معرِّفات الهوية. فينبغي على مطوري الأنظمة مراعاة ذلك، لأن تهديدات حقن لغة استجواب مُبَنْيَنة (SQL)، تنشأ أحياناً من جراء شفرة مغلوطة. وتهديد برنامج البوت الاقتحامي سببه الإصابة ببرنامج بوت شرير. ولذا ينبغي أن يكون مستعملو الحواسيب شديدي الحذر عند تحميل الملفات أو النفاذ إلى مواقع الويب، وأن يحموا أنظمتهم التشغيلية. وفي حالة نظام إدارة هش، ينبغي أن يكون مديرو الأنظمة شديدي الحذر عند إدارة أنظمتهم.

10 إمكان تطبيق آليات مكافحة الاقتحام المعروفة على تطبيقات الوسائط المتعددة القائمة على بروتوكول الإنترنت (IP)

أُجريت دراسات كثيرة على آليات مختلفة لمكافحة الاقتحام التقليدي الذي يتعرض له البريد الإلكتروني. وبعض الحلول التي وجدتها هذه الدراسات لمكافحة اقتحام البريد الإلكتروني يمكن تطبيقها في مكافحة اقتحام تطبيقات الوسائط المتعددة القائمة على بروتوكول الإنترنت (IP). ولذا يتعيّن، قبل الخوض في مجال الحلول بخصوص اقتحام هذه التطبيقات، تحليل الآليات الكلاسيكية لمكافحة الاقتحام، والنظر في قابلية إعمالها في مكافحة اقتحام تطبيقات الوسائط المتعددة القائمة على بروتوكول الإنترنت (IP). وعليه، فإن هذا القسم ينظر في بعض الآليات المشهورة لمكافحة الاقتحام من حيث قابلية تطبيقها على مكافحة اقتحام هذه التطبيقات.

1.10 الترشيح بتعرُّف الهوية

1.1.10 القائمة السوداء

القائمة السوداء هي قائمة تعرُّف (كعنوان البريد الإلكتروني بالنسبة لخدمة البريد الإلكتروني، مثلاً) لهوية الأطراف المشبوهين أو المؤكَّد كونهم مقتحمين. والغرض من هذه الآلية ترشيح الرسائل أو النداءات المرسلة من الأطراف المدرجة في القائمة. وقد تشتمل هذه القائمة على عناوين IP، وأسماء ميادين، وهويات أو عناوين طالبي النداءات، ومحتويات لرأسيات أو لمتون، وخليط من هذه الأنماط المختلفة، ما من شأنه المساعدة على تعرّف الرسائل الاقتحامية.

إلا أن مجرد استعمال قائمة سوداء قد لا يكون مجدياً بخصوص التطبيقات القائمة على بروتوكول الإنترنت (IP). فالمقتحم يستطيع أن يستعمل هوية أناس أبرياء، وأن ينتحل صفة المستقبل. وهذه المشكلة يمكن حلها بآليات استيقان تقوم على العنوان الأصلي. ولهذه الطريقة مشكلة أخرى وهي أن المستعمل يستطيع استحداث هوية جديدة بسهولة كبيرة. وكثير من تطبيقات الوسائط المتعددة القائمة على بروتوكول الإنترنت (IP) المخصصة للاتصالات تستعمل عناوين البريد الإلكتروني. وهذا العنوان يمكن بسهولة استحداثه عن طريق مواقع بوابية متنوعة مشهورة. وتستعمل أغلبية المشتركين العاديين غير الممارسين للاقتحام هذه العناوين المستمَدّة من مواقع بوابية مشهورة، وهكذا فإن اسم الميدان للمواقع البوابية لا يمكن إدراجه في القائمة السوداء.

ولذا يجب على موردي الخدمات البوابية، في سبيل حل هذه المشكلة، أن يزيدوا بعض الشيء في تعقيد استحداث عنوان جديد. فإذا تطلّب استحداث عنوان جديد جهداً ووقتاً طويلاً من المقتحم، فسيستعمل في النهاية طريقة ما أخرى لاستحداث عناوين جديدة يستهدفها بالاقتحام، ومن المرجح إلى حد كبير أن يتم ترشيح هذه العناوين الجديدة بواسطة إدراج أسماء الميادين في القائمة السوداء. وعليه، فإن طريقة القائمة السوداء تصير مجدية متى استُعملت متضافرة مع طرائق أخرى.

وطريقة القائمة السوداء لا تنطبق إلا في بدء الاتصال حين تصادَف هوية المصدر للمرة الأولى. وهكذا يصير من الممكن استعمال طريقة القائمة السوداء بخصوص أي نمط من تطبيقات الوسائط المتعددة القائمة على بروتوكول الإنترنت (IP) يستعمل تعرّف الهوية مثل عنوان المصدر. ويمكن استعمال هذه الطريقة في تطبيقات مواقع الويب، لأنه في الإمكان تطبيقها بمنح حقوق النشر على الموقع فقط لمن لا يتعاطون الاقتحام، يعني المستعملين غير المدرجين في القائمة السوداء. وهكذا يمكن استعمال طريقة القائمة السوداء لحجب أي نمط من الرسائل الاقتحامية على تطبيقات الوسائط المتعددة القائمة على بروتوكول الإنترنت (IP) التي تستعمل أي نمط لتعرف الهوية في تطبيقات الوقت الفعلي أو تطبيقات غير الوقت الفعلي.

2.1.10 القائمة البيضاء

طريقة القائمة البيضاء معاكسة لطريقة القائمة السوداء. فهي تحتوي معلومات المستعملين الموثوقين. فالرسائل الإلكترونية الصادرة من مرسلين مدرجين في القائمة البيضاء تكون دائماً مقبولة. وخلافاً لطريقة القائمة السوداء، لن يُجدي شيئاً في محاولة اختراق القائمة البيضاء استحداثُ عناوين بريد إلكترونية بكثافة، لكن القائمة البيضاء تظل عرضة لانتحال عنوان صالح. إلا أن الاقتحام بانتحال عنوان ما، يمكن ترشيحه بسهولة باستعمال طرائق استيقان صارمة.

وعلى الرغم من مقدرة طريقة القائمة البيضاء لترشيح جميع الرسائل الاقتحامية تقريباً، يظل الشخص العادي بحاجة إلى الاتصال بأناس ليسوا مدرجين في القائمة البيضاء. وإذا احتاج مرسِل غير مُدرَج في القائمة البيضاء الاتصال بالمستعمِل، يلزمه نمط ما لطريقة الاستيقان، لكي يتمكّن من دخول قائمة المستعمل البيضاء. ويكون على المستعملين التأكد من المرسل بتعرّف هويته أو بواسطة ملاحظات تعريفية يقدمها المرسِل. ويستطيع المستعمِل أن يقبل أو يرفض طلب الاتصال. والمرسِل المقبول طلبه يدخل قائمة المستعمل البيضاء. ولكن إذا كان على المستعمِلين أن يقبلوا أو يرفضوا كل طلب جديد، يصير الأمر مزعجاً إلى حد كبير لأن أغلبية الطلبات الجديدة عادة ما تكون محاولات اقتحام. ولهذه الطريقة مشكلة أخرى وهي أنه يتعيَّن على المستعمل تشكيل القائمة البيضاء كلما تغيرت بيئته، ما يمثّل هدراً للوقت والطاقات.

ومفهوم القائمة البيضاء معمول به في نظام المراسلة اللحظية (IM) حيث تسمّى بقائمة الرفاق. فكثير من أنظمة المراسلة اللحظية (IM) لا يسمح بالاتصال إلا للمستعملين المدرجين في قائمة الرفاق المتصفين بمقدرة موافقة من حيث السماح لمستعمل جديد بالانضمام إلى قائمة الرفاق. وهكذا يمكن لهذه الطريقة، بفضل آليات استيقان قوية، أن تكون مفيدة في مكافحة اقتحام المراسلة اللحظية. لكن المهاتفة عبر بروتوكول الإنترنت (VoIP) تختلف خصائصها عن خصائص أنظمة المراسلة اللحظية. وكما في حالة البريد الإلكتروني، يمكن أن تكون طريقة القائمة البيضاء مفيدة كطريقة مكمِّلة لاستعمال طرائق أخرى، على اعتبار أن المستعملين يميلون رغم ذلك إلى قبول نداءات من طالبين مجهولين.

وطريقة القائمة البيضاء تُستعمل فقط في بداية الاتصال، فهي من ثَمّ مناسبة لتطبيقات الاتصال في الوقت الفعلي وفي غير الوقت الفعلي. ويمكن أيضاً أن تُستعمَل طريقة القائمة البيضاء هذه في تطبيقات مواقع الويب، على اعتبار أنه من الممكن حصر منح حقوق النشر على الموقع بالمستعملين المدرجين في قائمة الموقع البيضاء.

3.1.10 نظام السمعة

يُستعمل نظام السمعة بالاقتران مع طريقة القائمة السوداء أو طريقة القائمة البيضاء. فإذا رغِب مرسِل غير مدرج في قائمة المستقبِل البيضاء أو السوداء في الاتصال بالمستقبل، يُعرَض تقييم سمعته على شاشة مطراف المستقبِل. فيساعد تقييم السمعة هذا المستقبل على اتخاذ القرار بقبول النداء أو رفضه. وإذا قبل المستعمل طلب الاتصال ثم اكتشف أن المرسِل مقتحم، يستطيع إخبار نظام السمعة بالاقتحام، فلا تضاف هوية المقتحم إلى قائمة المستعمِل البيضاء. وتتراكم التقارير في مخدم السمعة فتشكل قاعدة لتقييم السمعة.

لكن مشكلة هذه الطريقة هي أن المقتحم السيِّئ السمعة يستطيع تغيير هويته ويستأنف الاقتحام بهوية جديدة. فلا يكون للهوية الجديدة رصيد تقييم سيّئ، وينقضي حتماً بعض الوقت قبل أن يُعتبَر هذا المستعمل مقتحماً نتيجة لتراكم الإفادات السلبية عنه. ولهذه الطريقة مشكلة أخرى هي أن بعض مجموعات الأشرار تستطيع ترهيب ضحية بريئة وحملها على إظهار سمعة سلبية، فيصير من الصعب على هذه الضحية الاستمرار في معاملاتها التجارية عبر الشبكات القائمة على بروتوكول الإنترنت (IP).

ويوجد أيضاً نظام سمعة إيجابي. يعطي المستقبِل تقييماً إيجابياً لغير المقتحمين. ولن يكون من السهل مع هذه الطريقة الاقتحام باستعمال هوية جديدة قائمة على هذه الطريقة، على اعتبار أن الهوية الجديدة سيكون رصيدها الإيجابي ضعيفاً نسبياً. لكن المشكلة التي تواجهها هذه الطريقة هي أن عدة مقتحمين يستطيعون أن يتواطأوا ويعطوا أرصدة تقييم إيجابية لبعضهم البعض. ولكن في هذه الحالة، يتعين على المقتحمين أن يشكلوا شبه اتحاد لكي يحققوا ذلك، وتشكيل شبه اتحاد مكلف جداً. وعليه، فإن نظام السمعة الإيجابي أنجع من نظام السمعة السلبي.

ويحتاج نظام السمعة، لكي يعمل، إلى نظام اتصالات متصف بتحكم مركزي وأحادي. وهذه الطريقة يمكن أن تنجح مع أنماط تطبيقات المراسلة اللحظية التي يشغِّلها عادة مورد خدمة وحيد. أما تطبيقات المهاتفة عبر بروتوكول الإنترنت (VoIP) فتوفِّر الاتصال بين موردي خدمات مختلفين. وقد يختلف تقدير السمعة من مورد لآخر، على اعتبار أنه لا يوجد تعريف معياري. وعليه، فإن هذه الطريقة غير مناسبة لتطبيقات مثل المهاتفة عبر بروتوكول الإنترنت (VoIP) التي لا يوجد لها نظام معياري للوصف.

ويمكن أيضاً استعمال نظام السمعة في التطبيقات التي تستعمل نوعاً من تعرُّف هوية المرسِل، على اعتبار أن رصيد السمعة يمكن إعطاؤه للهوية. فإذا نجح المرسل في اجتياز نظام السمعة، يضاف إلى قائمة المستقبِل البيضاء. وهكذا يمكن استعمال هذه الطريقة في أي تطبيق، سواء كان التطبيق في الوقت الفعلي أو غير الوقت الفعلي.

ويمكن استعمال هذه الطريقة بخصوص التطبيقات القائمة على الويب، بجعل حقوق النشر على المواقع حكراً على المستعملين الذين يتجاوزون مستوى معين في رصيد السمعة. وفي مقدور موقع الويب أن يحفظ رصيد سمعة لكل عضو عن طريق حفظه لرصيد الأنشطة السابقة.

4.1.10 دوائر الثقة

تقوم طريقة دوائر الثقة على أن يتجمّع الناس الموثوقون أو الميادين الموثوقة ويتبادلوا القوائم البيضاء. وتستند هذه المنهجية إلى أن صديق الموثوق موثوق. وتشكل المجموعة فيما بينها علاقة موثوقة. ولذا فإنها قد تتفق على إنفاذ نوع من العقوبات بحق من يُقبض عليه من الأعضاء وهو متورط في عملية اقتحام.

ويتفرّع عن طريقة دوائر الثقة طريقة القائمة السوداء الموزعة، وهي طريقة يتقاسم فيها تجمع من الأفراد أو مجموعات الموثوقين القوائم السوداء. وهذه الطريقة فعالة جداً في ترشيح الرسائل الاقتحامية المخلّة بالأصول. وهناك مخدمات كثيرة تجمع القوائم السوداء بالاستناد إلى هذه الطريقة، وتفتح هذه المجموعة من القوائم السوداء أمام الجمهور لاستعمالها.

وهذا النمط من طرائق المكافحة يصلح جيداً في حالة مجموعة صغيرة أو مجموعات صغيرة من الموردين، حيث يكون تقاسم هذه السياسة وإنفاذها مجدياً. أما إذا كبرت دوائر الثقة، فيصعب التوصل إلى توافق آراء مناسب على إقرار مستوى ملائم من العقوبات بحق الاقتحام.

2.10 تغليف العنوان

يلزم امتلاك عنوان لكي يمكن استعمال عدد من تطبيقات الوسائط المتعددة القائمة على بروتوكول الإنترنت (IP). فمن الأهمية بمكان عدم تعريض هذا العنوان لعامة الجمهور. ولكن عند استعمال خدمات الويب، لا بد من تقديم العنوان للزبون الجديد لكي يسهل عليه الاتصال بالمالك. فيستغل المقتحمون هذا الضعف لتجميع عناوين يستهدفونها بالاقتحام، حيث يتناولون بالمسح صفحات شتى من شبكة الويب ويجمعون عناوين يكون في بنيتها "@" و"." ثم يستعملون ما يتجمّع لديهم من

العناوين في الاقتحام، ويبلّغون هذه العناوين إلى مقتحمين آخرين، على اعتبار أن المقتحمين يميلون إلى تبادل العناوين المستهدفة.

فتغليف العنوان طريقة لإخفائه بحيث لا يستطيع المقتحم التقاطه أوتوماتياً. وأبسط طريقة لتغليف العنوان تتمثل في وضع AT مكان "@" وDOT مكان ".". وعلى هذا النحو، يبدو العنوان كأنه نص عادي، أي يمكن له أن يفلت من نظام مسح العناوين الأوتوماتي الذي يستعمله المقتحمون.

وتغليف العنوان لا يعد طريقة لمكافحة الاقتحام، بل هو طريقة للوقاية من الاقتحام. إنه طريقة تقي من تعريض العنوان لبرنامج تجميع أوتوماتي للعناوين يستعمله المقتحمون. وعليه، فإن هذه الطريقة مناسبة لاتقاء الاقتحام في تطبيقات الوسائط المتعددة القائمة على بروتوكول الإنترنت (IP) التي تستعمل نفس العنوان في الخدمة القائمة على الويب.

ويصف هذا الجزء بعض التقنيات الأخرى الممكن استعمالها لتغليف العنوان.

1.2.10 التغليف بكتابة Java (JavaScript)

في بيئة "JavaScript" يسهل إضافة نمط عنوان "abc@xyz.com" باستعمال وظائف Java. وعندئذ تعلن صفحة الويب العنوان بالشكل "abc@xyz.com"، ولكن عند استعمال الوظيفة document.write() في JavaScript، يسهل جداً إخفاء عنوان البريد الإلكتروني. ونعرض فيما يلي مثالاً على ذلك.

```
<SCRIPT TYPE="text/javascript">
document.write('abc@' + 'xyz.com')
</SCRIPT>
```

ويمكن استعمال وظائف أو طرائق JavaScript أخرى من أجل إخفاء عنوان المراسلة الإلكترونية. لكن المهم هنا هو بيان أنه من الممكن إخفاء العنوان في بيئة JavaScript. وفي هذه الحالة، باستعمال كتابة JavaScript لإخفاء العناوين، يصعب على المقتحمين أن يجمّعوا بطريقة أوتوماتية عناوين البريد الإلكتروني، حتى لو عرضت صفحة الويب بوضوح عنوان البريد الإلكتروني العادي.

وهذه الطريقة لا تستعمل إلا في بيئات JavaScript. ولكن، إذا أراد المستعمل تحرير معرِّف هويته في المراسلة اللحظية أو عنوانه للمهاتفة عبر بروتوكول الإنترنت (VoIP) على صفحة ويب مستعملاً كتابة JavaScript، فإن هذه الطريقة يمكن أن تساعد تفادي التحول إلى هدف سهل للمقتحمين.

2.2.10 استعمال الشفرة ASCII

طريقة الشفرة المعيارية الأمريكية لتبادل المعلومات (ASCII) تقوم على إخفاء المعلومات الهامة بشفرة ASCII التي هي "&#number". والمعلومة الهامة يمكن أن تكون عنوان بريد إلكتروني أو رقم هاتف، أي من مستهدفات المقتحمين. وبهذه الطريقة لا تُعرض صفحة الويب بشكل نص عادي، بل بشكل صورة. وهكذا لا يظهر من صفحة الويب، في حال تحميلها، إلا شفرة ASCII. أما إذا كان المقتحم يمتلك، داخل أداته للبحث عبر صفحات الويب وظيفة تحويل الشفرة ASCII، فعندئذ يستطيع بسهولة فك هذه الشفرة.

3.10 الإثبات التفاعلي البشري

في هذه الطريقة، يتلقّى كل مستعمل أحجية أو مسألة تحدٍّ مصممة بحيث يستطيع الإنسان فقط حلها، وتعجز عن حلها الآلات. ويكون ذلك صورة أو صوتاً لكلمة أو عدد، لا يستطيع فهمه إلا شخص، وليس الآلة. وقد يكون صورة مخفية خلف ألوان متنوعة أو صوتاً مخفياً خلف مصادر ضوضاء متنوعة، بحيث يصعب أن تفهم الآلة شيئاً منها. ولكن في أيامنا أصبح صنع الأحاجي التي لا تستطيع الآلات فهمها مهمّة أكثر صعوبة مما في الماضي، نظراً للتقدم المحرز في مجالات الصورة الأوتوماتية ومعالجة الصوت والذكاء الاصطناعي.

ويُستعمَل الإثبات التفاعلي البشري عادة في التطبيقات المعتمِدة على الويب، طيلة مرحلة ما من الاشتراك في الخدمات الشبكية، فهو من ثَمّ مناسب جداً لمكافحة الاقتحام القائم على الويب. وهذه الطريقة يمكن أيضاً استعمالها لترشيح الاقتحام على النداءات باستعمال طريقة التخويل المعتمِدة على الأصوات. مثلاً: حين يبدأ طالب نداء غير مدرج في القائمة السوداء أو البيضاء نداءً صوتياً، ينشِّط المستقبِل أوتوماتياً جهاز الاستجابة الصوتية التفاعلية (IVR) الذي يطلب من طالب النداء إدخال رقم ما بواسطة لوحة أرقام الهاتف. فإذا أدخل طالب النداء الرقم بلا خطأ، يضاف رقم هاتف طالب النداء أوتوماتياً إلى القائمة البيضاء لدى المستعمِل. وقبل الانضمام إلى الدردشة، يمكن أن يخضع المستعمل لإجراء الإثبات التفاعلي البشري.

4.10 ترشيح المحتوى

ترشيح المحتوى على خط الموضوع هو الطريقة الدارجة الأكثر شيوعاً لمكافحة الاقتحام على البريد الإلكتروني. ويجري مسح خط الموضوع لمعرفة الألفاظ المشبوهة التي يكثر استعمالها في الاقتحام.

وتنطوي المراسلة اللحظية على تبادل رسائل نصية قصيرة، ولذا يسهل تطبيق هذه الآلية في مكافحة اقتحام المراسلة اللحظية. ويتم مسح محتوى كل مراسلة لحظية باستعمال نفس التقنية المستعملة لمسح خط الموضوع في حالة البريد الإلكتروني.

إلا أن هذه الطريقة لا يمكن تطبيقها حتى وقتنا هذا على المهاتفة عبر بروتوكول الإنترنت (VoIP) ولا على اتصالات الوسائط المتعددة القائمة على بروتوكول الإنترنت (IP) المشتملة على مواد سمعية و/أو فيديوية. وذلك لأن الوسائط تُرسَل بعد إقامة النداء، فلا جدوى ممكنة من ترشيح المحتوى مسبقاً. كما أنه، حتى لو تم تسليم الرسالة الاقتحامية بشكل رسالة صوتية أو فيديوية وخُزِّنت في مخدم، فإن التكنولوجيا الحالية المستعملة لمسح بعض الألفاظ جيدة بما يكفي بحيث يمكن استعمالها في مكافحة الاقتحام.

5.10 الاستيقان بتبادل المفاتيح

طريقة الاستيقان تمكّن من تعرّف مأمون لهوية مرسِل رسائل وسائط متعددة قائمة على بروتوكول الإنترنت (IP)، حيث تساعد على صد كثير من هجمات الاقتحام الانتحالية بحجبها.

1.5.10 بنية PKI وبروتوكول PGP

من الممكن استيقان المرسل من أجل الحجب على طلبات الاتصال الصادرة عن مقتحم متنكِّر بصفة غيره، ولا سيما صفة شخص مدرج على القائمة البيضاء. فالبنية التحتية لمفاتيح عمومية (PKI) والبروتوكول بمثابة طريقتين شهيرتين للاستيقان تستعملان آليات المفاتيح العمومية. وتستعمل البنية التحتية PKI آلية مفتاح عمومي، يمكن بفضله استيقان المرسل، نظراً لتصديق هذا المفتاح من قبل سلطات التصديق (CA). ويستعمل البروتوكول PGP برنامجاً حاسوبياً، يوفّر وظيفة توقيع من أجل الاستيقان. ففي أنظمة البريد الإلكتروني، تُستعمَل هذه الآليات لتجفير الرسائل وإضافة توقيع رقمي. إنهما آليتان قويتان لمنع الاقتحام.

وآليات تبادل المفاتيح هذه مفيدة، تكاد فائدتها تشمل جميع أنظمة اتصالات الوسائط المتعددة القائمة على بروتوكول الإنترنت (IP). وينبغي الاحتراس عند استعمالها في الخدمات المؤتمرية القائمة على بروتوكول الإنترنت (IP)، على اعتبار أن المفتاح الجماعي للخدمة المؤتمرية معرض جداً للسرقة.

إن طريقتي البنية PKI والبروتوكول PGP يمكن استعمالهما استعمالاً يكاد يعم جميع أنماط تطبيقات الوسائط المتعددة القائمة على بروتوكول الإنترنت (IP)، مثل المهاتفة عبر بروتوكول الإنترنت (VoIP) والمراسلة اللحظية (IM). ويمكن استعمال هذه الطريقة في التطبيقات المعتمدة على الويب التي تسمح بتحميل الملفات فقط لحملة الشهادات المصدّقة.

2.5.10 الرسالة المعرَّفة الهوية بمفاتيح الميادين (DKIM) [b-IETF RFC 4871]

الرسالة المعرَّفة الهوية بمفاتيح الميادين (DKIM) هي طريقة ابتكرها فريق مهام هندسة الإنترنت (IETF)، يمكن استعمالها للاستيقان من البريد الإلكتروني. حيث يُلحِق مخدم البريد الإلكتروني بالرسالة توقيعاً تجفيرياً من أجل تأكيد أن المخدم أرسل

بالفعل الرسالة الواصلة. فالطريقة DKIM تمكن منظمة ما من تحمّل مسؤولية التحقق من صلاحية رسالة بالنسبة إلى المستقبل. إن الطريقة DKIM تحدد إطار استيقان بالتوقيع الرقمي على مستوى الميدان، من أجل البريد الإلكتروني، من خلال استعمال تجفير لمفتاح عمومي وتكنولوجيا مخدم مفاتيح. إذ إن بإمكان رسالة احتيالية أن تسبب ضرراً لا يقتصر على مستقبلها، بل يطال أيضاً سمعة شركة أو منظمة كبرى. فاستعمال الطريقة DKIM من شأنه أن يحمي الشركة أو المنظمة من هذه الأضرار.

ويمكن أن يمنع استعمال الطريقة DKIM الاتصالات الاحتيالية بالمهاتفة عبر بروتوكول الإنترنت (VoIP) أو بالمراسلة اللحظية (IM). إذ إن المستقبِل يستطيع التدقيق مع مخدم المرسِل في كون الرسالة المستقبلة (أو النداء) صادرة فعلاً عن المرسل المعلَن. وإجراء الاستيقان يمكن إنفاذه في بداية الاتصالات، وهكذا لن يكون له أثر ولا حتى على تطبيق حساس في الوقت الفعلي.

3.5.10 الاستيقان بالبروتوكول HTTP وتوصيل أمن طبقة النقل (TLS)

إن استعمال طريقة الاستيقان بالبروتوكول HTTP digest [b-IETF RFC 5090] المصحوب بتوصيل مع المخدم مأمونة فيه طبقة النقل (Transport Layer Security)، (التوصيل TLS)، هو استعمال فعال جداً ل تطبيقات الوسائط المتعددة القائمة على بروتوكول الإنترنت (IP)، القائمة بنيتُها على العلاقة بين العميل والمخدم. وفي هذه الطريقة يتولى مخدم الميدان إقرار صلاحية مستعمليه من خلال الاستيقان بالبروتوكول HTTP digest. ويُستعمل هذا البروتوكول لاستيقان مستعمل تطبيقات الوسائط المتعددة القائمة على بروتوكول الإنترنت (IP) بواسطة اسم المستعمِل مشفوعاً بكلمة سر. وفي هذه العملية، يستبقي العميل، أي المستعمِل، توصيله المأمون طبقة النقل (TLS) ثابتاً مع المخدم. ويتحقق العميل من هوية المخدم باستبقائه التوصيل TLS معه. والمخدم يستيقن من العميل بأن يستعمل معه تبادلاً من نمط digest عبر التوصيل TLS. وحين يرسل مستعمِل تم استيقانه رسالة إلى ميدان آخر، يصدِّق ميدان الإرسال على المستعمل، بأن يُدرِج توقيعاً من أجل إقرار صلاحية الرسالة. وينبغي أن يشكل ميدان الإرسال وميدان الاستقبال إجراء استيقان متبادل بحيث يصدِّق كل منهما على مستعملي الآخر.

وهذه الطريقة يمكن استعمالها لاستيقان المستعملين الذين يتواصلون بالمراسلة اللحظية (IM) أو بالمهاتفة عبر بروتوكول الإنترنت (VoIP). ويمكن إجراء عملية الاستيقان في بداية الاتصال، وهكذا لن يكون له أثر ولا حتى على تطبيق حساس في الوقت الفعلي.

6.10 ترشيح الرسائل الاقتحامية بالاستناد إلى الشبكة

صُمِّمت آليات ترشيح الرسائل الاقتحامية التي تَقدّم النظرُ فيها، من أجل تشغيلها في الاتصالات في جانب المخدم وفي جانب العميل على السواء. لكنه من المهم أيضاً بناء شبكات مأمونة تجنباً للاقتحام. ويناقش هذا القسم باختصار بعض طرائق ترشيح الرسائل الاقتحامية القائمة على الشبكات.

1.6.10 رفض الرزم في الكيان الشبكي

من الممكن وضع سياسة ما، مثل قائمة التحكم في النفاذ (ACL)، في جهاز تسيير أو أي كيان شبكي، من أجل استبعاد الرزم المشبوهة كونها رسائل اقتحامية صادرة عن عنوان بروتوكول الإنترنت (IP) معين أو عن عنوان يحمل سابقة IP. والمقتحم يمكن أن يكون داخل الشبكة الخاصة بمورد خدمة الإنترنت أو خارجها. فيتعيّن على مورد خدمة الإنترنت (ISP) الذي يريد حماية شبكته من الاقتحام أن يجد حلاً لكلتا الحالتين، بطريقتين مختلفتين.

إذا كان المقتحم داخل شبكة مورد خدمة الإنترنت (ISP)، يستطيع المورد ISP أن يحمل الكيان الشبكي المصدر على قطع التوصيلية القائمة على بروتوكول الإنترنت (IP) لمصدر الاقتحام. فيتحقق المقتحم أنه فقد التوصيلية الشبكية، ويتحتّم عليه الإقرار بفعلته السيئة. إلا أنه ينبغي اعتماد معيار معين تجنباً لسوء الاستعمال. إذ يمكن لشخص ما أن يتهم بالكذب شخصاً بريئاً بأنه مقتحم، ثم تُقطَع توصيلية هذا البريء. ويمكن أن يستعمِل شخص غير مستقيم عنوان بروتوكول الإنترنت (IP) لشخص بريء في إرسال الرسائل الاقتحامية، ويستمر وقتاً ما على إرسال هذه الرسائل الاقتحامية، فيؤدي سلوكه هذا إلى قطع التوصيلية الشبكية للشخص البريء.

لنفترض أن هناك شبكةً للمورد A متصلة بشبكة للمورد B وأن المقتحم يستعمل شبكة المورد B. فإذا كان مصدر الاقتحام خارج شبكة المورد ISP A، يجب على هذا المورد التأكد من أن المورد ISP B التابع له المقتحم يريد ضبط أنشطة الاقتحام في شبكته. وإذا لم يكن لدى المورد ISP B أي سياسة لضبط أنشطة الاقتحام، يتوجّب عندئذ على المورد ISP A أن يضع سياسة لدرء الاقتحام في بوابة شبكة المورد ISP B ليمنع فيضان الرسائل الاقتحامية نحو شبكة المورد ISP A. وبهذه الطريقة لا يستطيع المورد ISP A حجب المقتحم عن التوصيلية الشبكية، لكنه يستطيع حماية شبكته من الاقتحام. ويمكن لهذه الطريقة أن تحمي وتنقذ موارد الشبكة. لكن لهذه الطريقة عيب وهي أنها يمكن أن تحجب مستعمِل بريء من شبكة المورد ISP B من الاتصال بشبكته.

وهناك مشكلة أخرى في هذه الطريقة هي أن المقتحم يستطيع تغيير عنوان بروتوكول الإنترنت (IP) الخاص به كثيراً. ولذا يجب على المورد ISP التابع له المقتحم أن يضبط ويستيقن من عنوان بروتوكول الإنترنت (IP) الذي يستعمله هذا المقتحم، لكي تكون هذه الطريقة مجدية.

إن طريقة رفض الرزم في الكيان الشبكي يمكن استعمالها في جميع التطبيقات ما دامت تتعلق ب تطبيقات الوسائط المتعددة القائمة على بروتوكول الإنترنت (IP).

2.6.10 القائمة السوداء الموزَّعة

القائمة السوداء الموزَّعة هي قائمة سوداء مستقرّة في الشبكة لكي يتقاسمها مجتمع الشبكات. ويتم عادة تطبيق القوائم السوداء الموزَّعة على مخدمات أنظمة أسماء الميادين (DNS). ويستطيع المستعملون أن يضيفوا إلى القائمة السوداء الموزّعة عنواناً وصلتهم منه رسالة اقتحامية. ومتى ورد عنوان بروتوكول الإنترنت (IP) في القائمة السوداء الموزّعة، تصير الرسائل الصادرة عن هذا العنوان مرفوضة في مواقع كثيرة. وقابلية تطبيق هذه الطريقة على تطبيقات الوسائط المتعددة القائمة على بروتوكول الإنترنت (IP) مكافئة لقابلية تطبيق طريقة القائمة السوداء.

3.6.10 مِصَدّ الاقتحام

تستعمل شبكات الشركات وشبكات موردي خدمة الإنترنت مصدّات اقتحام لوقاية شبكاتهم من الاقتحام. وتُستعمَل في مصدّ الاقتحام طرائق عديدة تقدم ذكرها من أجل منع الرسائل الاقتحامية قبل أن تدخل إلى الشبكة. فمستعمِل شبكة محمية قلّما يعاني من الرسائل الاقتحامية. وهذه الطريقة تجمع بين طريقة القائمة السوداء وطريقة ترشيح المحتوى، لأنها تستبقي القائمة السوداء وترشح المحتوى كلما دخلت الرزم الشبكة.

ومِصدّ الاقتحام يُستعمَل في الوقت الحاضر لحماية البريد الإلكتروني والمراسلة اللحظية. وهذه الطريقة قد لا تُجدي بالنسبة إلى خدمات المهاتفة عبر بروتوكول الإنترنت (VoIP)، على اعتبار أنه لا يمكن التقاط شيء في بداية نداءات المهاتفة عبر بروتوكول الإنترنت (VoIP). ولكن يمكن استعمال هذه الطريقة لترشيح الرسائل الاقتحامية القائمة على الويب، لأنه من الممكن ترشيحها بفحص المحتوى.

7.10 الطابع الإلكتروني

في طريقة الطابع الإلكتروني، يتعيّن على المرسل غير المدرج في القائمة البيضاء للمستقبل أن يشتري طابعاً من على الخط من أجل إرسال رسالته. وإذا أرسل مرسل غير وارد في القائمة البيضاء رسالة بدون طابع إلكتروني، يرفضها مخدم مورد الخدمة. فلا بد للمرسِل غير المدرج في القائمة البيضاء للمستقبل من شراء طابع إلكتروني لكي تظهر رسالته في مطراف المستقبِل. وإذا قبل المستقبِل استلام الرسالة، توجب عليه إعادة الطابع إلى المرسل. وعنوان هذا المرسِل المقبولة رسالته يضاف أوتوماتياً إلى القائمة البيضاء. وإذا تأكد لدى المستقبِل أن المرسل مقتحم، يستطيع الاحتفاظ بقيمة الطابع المشترى على الخط. وكلما زاد المقتحم من عدد رسائله الاقتحامية ازداد حجم نفقاته.

وهذه الطريقة يمكن استعمالها لحماية خدمات البريد الإلكتروني أو المهاتفة عبر بروتوكول الإنترنت (VoIP) أو المراسلة اللحظية (IM). وبما أن المرسل يتعيّن عليه أن يشتري طابعاً على الخط مرة واحدة فقط، فهذه الطريقة ليست مزعجة ولا

مكلفة أيضاً. ولا باهظة الثمن. وعليه، يمكن أن تكون فعالة في مكافحة الاقتحام، إذا استُعملت متضافرة مع استيقان مناسب لهوية المرسل.

8.10 ترشيح الرسائل الاقتحامية المعتمد على التخويل

إنه لعنصر هام من أجل ترشيح الرسائل الاقتحامية أن توفر آلية يُكلّف في إطارها بعض الكيانات الشبكية "بترشيح" طلبات التوصيل الواردة، تبعاً لسياسة المستعمل أو لسياسة الشبكة. ويمكن لكيانات متنوعة، مثل المستعملين أو مدراء الأنظمة، أن تضع وتعدِّل سياسات التخويل. وسياسة الشبكة ضرورية لتحديد تدفق الاتصالات بين الميادين.

ويمكن تطبيق سياسات التخويل في المضيف النهائي و/أو على يد عناصر الشبكة. والكيان الذي يضع القواعد يمكن أن يكون مستعملاً نهائياً يمتلك الجهاز أو مورد خدمة المهاتفة عبر بروتوكول الإنترنت (VoIP) أو شخصاً له علاقة مع المستعمل النهائي (مثلاً: أهل طفل مستعمِل لهاتف متنقل). ويتناول هذا القسم عدداً من آليات ترشيح الرسائل الاقتحامية المعتمد على التخويل.

1.8.10 الاتصالات المشروطة بالموافقة

الاتصالات المشروطة بالموافقة هي الاتصالات المعتمِدة على تخويل الرسالة تخويلاً مباشراً من مستقبِل الرسالة. وتُستعمل هذه الطريقة بالاقتران مع طريقة القائمة البيضاء أو السوداء. فإذا حاول مرسل غير مدرج في القائمة السوداء ولا في القائمة البيضاء أن يتصل بالمستعمل، يرسل إليه معرف هويته و/أو نصاً قصيراً لتعريف هويته. وفي أول الأمر يُرفض المرسِل. ثم يبلغ المستعمل أن طالب النداء يحاول الاتصال. وللمستعمل أن يقبل أو يرفض المرسِل من خلال تفحص معرف هويته و/أو النص القصير الوارد منه.

وهذه الطريقة في الترشيح تُستعمل حالياً في خدمات متعددة للمراسلة اللحظية. وثبت أنها فعالة جداً في إدارة القائمة البيضاء. ويمكن تطبيقها على النداءات الاقتحامية، إذ يتعيّن الحصول على الموافقة في البداية، لكنها لا تصلح لمكافحة الاقتحام القائم على الويب، لكون هذه الخدمة أحادية الاتجاه. وقد لا تكون مناسبة للخدمات التي تضم عدة مستعملين، إذ تبطل فعالية الخدمة بحكم لزوم الموافقة من جميع المشاركين في الخدمات الجارية.

والعائق في هذه الطريقة هو أن المستعمل يمكن أن يتضايق من كثرة طلبات الموافقة. وعليه ينبغي ترشيح بعض طلبات الموافقة بواسطة نظام ترشيح آخر.

2.8.10 التخويل المعتمد على سياسة المستعمل

في طريقة التخويل المعتمد على سياسة المستعمل، يحدد مستعمل تطبيقات الوسائط المتعددة القائمة على بروتوكول الإنترنت (IP) سياسة القبول لترشيح طلبات المرسلين المجهولين. وتوضع السياسة في مطراف المستعمل أو في مخدم التطبيقات، من أجل قبول أو رفض الطلبات أوتوماتياً. ويمكن تطبيق السياسة على عنوان مصدر الرسائل الاقتحامية، وعلى معرف هوية المرسل و/أو النص القصير التعريفي الوارد منه، كما هو الحال في طريقة الاتصالات المشروطة بالموافقة. ويمكن أيضاً تطبيق السياسة على محتوى الرسالة المستقبلة، صورة كان أو صوتاً أو نصاً، من أجل ترشيح أوتوماتي لطلب اتصال يخالف السياسة الموضوعة. وينبغي أن تُحفَظ المعلومات المتعلقة بالطلبات المرفوضة في سجل يومي، بحيث يستطيع المستعمل الرجوع إليها وتفقد الطلبات التي لم يكن واجباً رفضها. ويستطيع المستعمل تعديل السياسة تبعاً لاحتياجاته.

والعائق في طريقة الاتصالات المشروطة بالموافقة هو تضايق المستعمل من لزوم الإجابة عن جميع طلبات الاتصال. أما طريقة التخويل المعتمد على السياسة، فيجري فيها الترشيح الأوتوماتي لمعظم الرسائل الاقتحامية، بحيث لا يتبرم المستعمل من كثرة طلبات الموافقة. ورسم سياسة الترشيح مرهون بخصائص ما يُستعمَل من تطبيقات الوسائط المتعددة القائمة على بروتوكول الإنترنت (IP). فينبغي تحديد طريقة الترشيح المعتمد على سياسة المستعمل لجميع التطبيقات الهشة المعرضة للاقتحام.

وثبت أن هذه الطريقة فعالة جداً في إدارة القوائم البيضاء. وبما أنها مرهونة بسياسة المستعمل، فيمكن من ثَمّ استعمالها بخصوص جميع الخدمات الثنائية الاتجاه كالمهاتفة عبر بروتوكول الإنترنت (VoIP) والمراسلة اللحظية (IM).

3.8.10 التخويل المعتمد على سياسة الشبكة

ينبغي أن يستعمل مشغّل الشبكة التخويل المعتمد على سياسة الشبكة لترشيح الرسائل الاقتحامية توخياً لحماية شبكته. وسياسة الشبكة يمكن استعمالها في شبكة وحيدة أو بين الشبكات المتجاورة. وهذه الطريقة مكافئة لطريقة رفض الرزم عند وصولها إلى الكيان الشبكي.

وتوخياً لتوفير ترشيح قابل للتطور للرسائل الاقتحامية، يستطيع مشغّل الشبكة أن يوكل جزءاً من حقوق الإدارة إلى مستعملين نهائيين مهرة وأن يمكّنهم من تشكيل سياسة الشبكة على الوصلات التي توصلهم بشبكة المورد. وينفذ الاستيقان الضروري في مسيِّر الخدمة من أجل إقرار صلاحية هوية المستعمل وحقوقه الإدارية. ولا يخوَّل غير المستعملين المعتمَدين حق توفير سياسات الشبكات المقابلة طبقاً للحقوق الممنوحة لهم.

9.10 الإجراءات القانونية واللوائح

من الأهمية بمكان فيما يخص تحاشي الاقتحام أن توضع لوائح في هذا الصدد وقوانين تمنع الاقتحام، وإن تكن فعالية هذه الأمور موضع نقاش. وقد وضع كثير من البلدان قوانين تمكن المتضررين من مقاضاة المقتحمين. وفي أغلبية الحالات، تُلزم هذه التشريعات صاحب الدعاية أن يدرج مجموعة محتويات خاصة تفيد مستقبلي الرسائل أن الرسالة الاقتحامية هي مجرد دعاية، وإذا خالفوا القواعد تعرضوا للعقوبة.

وما يعوق هذه الطريقة هو ما يواجَه من الصعوبات في تطبيق القوانين الوطنية المكافحة للاقتحام على مقتحمين يرسلون رسائلهم الاقتحامية من بلدان أجنبية. فيجب إقامة اتفاق دولي بشكل ما بين العديد من البلدان لكي تكون هذه الطريقة فعالة. وفي الوقت الحاضر تقوم منظمات دولية مثل قطاع تقييس الاتصالات بالاتحاد الدولي للاتصالات، ومنظمة التعاون والتنمية في الميدان الاقتصادي (OECD)، ومجلس التعاون الاقتصادي لآسيا والمحيط الهادئ (APEC)، وغيرها، بمساعي في سبيل وضع تشريعات فعالة لمكافحة الاقتحام، وإقامة تعاون دولي، وإنفاذ التشريعات.

وهذه الطريقة غير تقنية، كما أنها لا تتعلق بخصائص تطبيقات الوسائط المتعددة القائمة على بروتوكول الإنترنت (IP).

11 اعتبارات تُراعى في مكافحة اقتحام تطبيقات الوسائط المتعددة القائمة على بروتوكول الإنترنت (IP)

لا يعد استعمال الشبكات القائمة على بروتوكول الإنترنت للدعاية اقتصادياً وحسب، لكنه فعال أيضاً إلى حد كبير. ومشاكل الاقتحام تنشأ عن إساءة استعمال الدعاية. ويمكن أن تحدث مشكلات اجتماعية خطيرة بسبب الاقتحام. وتشمل هذه المشكلات كثافة الدعاية، والاحتيال، والغش، وكلها أمور تسبب مضايقات وأضراراً لمستعملي الشبكة.

وفي هذه التوصية تم تناول عدد من طرائق مكافحة اقتحام تطبيقات الوسائط المتعددة القائمة على بروتوكول الإنترنت (IP). ولهذه التطبيقات خصائصها المتنوعة، وكذلك ما تتعرض له من الاقتحام له خصائصه المتعددة. واستعمال طريقة مكافحة واحدة أو اثنتين لن يكون مجدياً إزاء جميع أنماط اقتحام تطبيقات الوسائط المتعددة القائمة على بروتوكول الإنترنت (IP). فينبغي إجراء دراسة تفصيلية بشأن مختلف أنماط الاقتحام ذات الصلة بمختلف كيانات تطبيقات الوسائط المتعددة القائمة على بروتوكول الإنترنت (IP)، لكي يمكن إيجاد حل بالفعل لمشكلة الاقتحام أو العمل على تخفيف وطأتها. ومن ثَمّ يجب في طريقة مكافحة الاقتحام أن تخضع للتحليل طبقاً لخصائص تطبيقات الوسائط المتعددة القائمة على بروتوكول الإنترنت (IP). ويحاول هذا القسم عرض بعض النقاط الهامة في موضوع مكافحة اقتحام تطبيقات الوسائط المتعددة القائمة على بروتوكول الإنترنت (IP).

وتوخيا للفعالية في مكافحة اقتحام تطبيقات الوسائط المتعددة القائمة على بروتوكول الإنترنت (IP)، ينبغي النظر في نهج مختلفة ذات صلة بجوانب مختلفة حسب الفئات المشاركة في الخدمة. فهناك مستعمل الخدمة (و/أو المشترك في الخدمة)، وموردو الخدمات، ومشغّلو الشبكات، والمنظمات العمومية، ووكالات الدعاية والإعلان. وهكذا، فإن هذا الجزء يصف بعض النقاط الجديرة بالبحث من أجل مكافحة اقتحام تطبيقات الوسائط المتعددة القائمة على بروتوكول الإنترنت (IP)، بالنسبة إلى كل جانب من هذه الجوانب.

1.11 مستعمل الخدمة (المشترك في الخدمة)

مستعمل الخدمة و/أو المشتركون في الخدمة هم الضحايا الحقيقيون للاقتحام، ويفترَض أنهم يدركون أهمية حجب الاقتحام لحماية حقوقهم. وفيما يلي بعض النقاط التي ينبغي أن يأخذها مستعمل الخدمة في الاعتبار عند مكافحة الاقتحام، على الرغم من أن تطبيق هذه المقترحات قد تختلف باختلاف الوسط:

- ينبغي أن يتزوّد المستعمل بأدوات ترشيح للرسائل الاقتحامية، وأن تواكب دائماً أحدث التطورات من أجل حجب الرسائل الاقتحامية غير المرغوبة. ويمكن دائماً ظهور رسائل اقتحامية جديدة، ولذا ينبغي أن تظل أداة الترشيح مواكبة لأحدث التطورات بحيث تسيطر على هذه الرسائل.
- ينبغي أن يشترك المستعمل في مراشيح متنوعة للرسائل الاقتحامية، مثل القائمة السوداء، والقائمة البيضاء، وما إلى ذلك، وأن يحدّث قوائم الترشيح باستمرار.
- حين يصادف المستعمل رسالة اقتحامية، ينبغي أن يزيلها فوراً وأن يُعلم بها الجمهور، منعاً لوقوع ضحية مماثلة.
- ينبغي أن يشارك المستعملون في التدريب على منع الاقتحام، لكي يكونوا على علم بالرسائل الاقتحامية الجديدة والتقنيات الجديدة للمكافحة. إذ إنه من الممكن ظهور أنماط جديدة من الاقتحام في الخدمات التقليدية إلى جانب الخدمات الجديدة. وفي حين لا تستدعي الحاجة استعمال كل تقنيات المكافحة، ينبغي المحاولة لإيجاد حل واف لمكافحة الاقتحام.
- ينبغي توخي الحذر في وقاية المعلومات الشخصية للأفراد من تعرضها للمقتحمين، أي: تحاشي استعمال أنماط من معرّفات الهوية أو الأرقام التي يسهل حفظها أو حزرها.
- ينبغي استعمال تقنيات وقائية، من أجل حجب طلبات الاتصال الصادرة عن مقتحمين، كما ينبغي تشكيل النظام الخاص لكل شخص بحيث يصعب على المقتحم الاتصال.

2.11 موردو الخدمات

يستطيع مزوّدو الخدمات جني أرباح كبيرة من توفير خدمات تتسم بالجودة. فالاقتحام يمكن أن يصيب الخدمة بأضرار خطيرة، حيث يسيء المقتحمون استعمال الخدمة واستغلالها. ولذا ينبغي أن يكون موردو الخدمات مدركين لمشكلة الاقتحام من أجل حماية الشبكة ولكي يوفروا خدمات أفضل. وفيما يلي بعض النقاط التي يمكن أن يأخذها موردو الخدمات في اعتبارهم عند مكافحة الاقتحام:

- قبل إطلاق خدمة وسائط متعددة قائمة على بروتوكول الإنترنت (IP) جديدة، يمكن لمورد الخدمة إجراء تحليل لإمكانات تعرض خدمات أو تطبيقات الوسائط المتعددة القائمة على بروتوكول الإنترنت (IP) الجديدة للاقتحام. وليس كل خدمة وسائط متعددة قائمة على بروتوكول الإنترنت (IP) هدفاً للمقتحمين. لكن إجراء تحليل بخصوص إمكانات التعرض للاقتحام، وإيجاد حلول تصعِّب من عملية الاقتحام، من شأنه أن يزيد من إمكانات نجاح الخدمة الجديدة. أما إذا نُشرت خدمة محتمل اقتحامها بدون العملية المذكورة، فسيكون من الصعب لاحقاً السيطرة على الاقتحام، وبعدما يطغى الاقتحام على الخدمات الجديدة يتركها المستعملون.
- يمكن لمورد الخدمة التحقق من جميع الكيانات التي تشتمل عليها خدمات أو تطبيقات الوسائط المتعددة القائمة على بروتوكول الإنترنت (IP)، كالمستعملين، والشبكة، ومكوِّنات الخدمة، وما إلى ذلك، وأن يحلل في كل كيان مختلف طرائق الاقتحام، لكي يجد حلولاً أبسط وأنجع في مكافحة الاقتحام. ومن الممكن استعمال تقنيات مكافحة الاقتحام

فقط داخل خدمة الوسائط المتعددة القائمة على بروتوكول الإنترنت (IP)، ولكن يمكن أن يكون هناك حلول أفضل عند معالجة كيانات الشبكة بأكملها.

- يمكن أن يجري مورد الخدمة بحثاً مستمراً عن ظهور رسائل اقتحامية جديدة في تطبيقات تقليدية. فأنماط الرسائل الاقتحامية الجديدة يمكن أن تصادف حتى في أقدم الخدمات. وقد يرغب موردو الخدمات في رصد هذه الظاهرة، وأن يحاولوا إيجاد حلول لمعالجة أنماط الاقتحام الجديدة، حتى في الخدمات التقليدية.
- يمكن لموردي الخدمات استعمال مراشيح متنوعة، مثل القوائم البيضاء والقوائم السوداء، من أجل التحكم بنفاذ المستعملين إلى الخدمات. والأفضل هو منع المقتحمين من استعمال الخدمات، لأنهم إذا نفذوا إليها فإنما ينفذون من أجل إساءة استغلالها فحسب.
- إذا انطوت الخدمة على عملية اشتراك، ينبغي أن يصعّب مورد الخدمة الاشتراك بدرجة تمنع المقتحمين من الانضمام إلى الخدمة. إذ إن كثيراً من المقتحمين يستعملون طرائق أوتوماتية أو يستأجرون مستخدَمين بأجرة رخيصة ليسجلوا كثيراً من الاشتراكات، وهذا شيء فعال جداً في عملية الاقتحام. ويمكن أن تشتمل عملية الاشتراك على طرائق استيقان متينة، من أجل التحقق من المشترك، وعلى خطة تمنع تعدد الاشتراكات لمستعمل واحد، ومنع المقتحمين من الانضمام إلى الخدمة.
- إذا كانت الخدمة تحتفظ بقائمة بالمستعملين، يمكن أن يكون لدى مورد الخدمة طريقة لتقييم مصداقية مستعملي الخدمة، للتأكد من أن المستعملين لا يسيئون استغلال الخدمة، ولا يخدعون المستعملين الآخرين. وينبغي أن يكون لدى مورد الخدمة تقنية يمنع بها تعرض المعلومات الشخصية للمشتركين للاستباحة من قبل المستعملين الداخليين والخارجيين.
- إذا كانت الخدمة تحتفظ بسجلات، قد يرغب مورد الخدمة في مراقبة محتويات موقع الويب، من أجل إزالة الرسائل الاقتحامية منها. وتحليل المحتوى يمكن إجراؤه حتى على البيانات الفيديوية والسمعية من أجل كشف المحتويات غير المناسبة.
- ينبغي لمورد الخدمة أن يقوم باختيار طريقة تتيح للمستعملين مكافحة الاقتحام. وهذه الطريقة يمكن أن تكون جهاز ترشيح أو قائمة ترشيح أو أدوات لتشكيل السياسة أو مراجع لمكافحة الاقتحام أو أي شيء يمكن للمستعمل استعماله لمكافحة الاقتحام.

3.11 مشغِّلو الشبكات

من شأن الاقتحام أن يسبب هدراً في موارد الشبكة، خاصة إذا كانت الرسالة الاقتحامية ذات محتوى متعدد الوسائط. فينبغي أن يحاول مشغلو الشبكات حجب الرسائل الاقتحامية حمايةً للشبكة، ولتوفير خدمات شبكية فعالة. وفيما يلي بعض النقاط التي ينبغي أن يأخذها مشغِّلو الشبكات في اعتبارهم عند مكافحة الاقتحام:

- يمكن لمشغلي الشبكات مراقبة الحركة في الشبكة، لاكتشاف أي حركة غير عادية قد تكون اقتحاماً. وينبغي أن يكون مشغِّل الشبكة قادراً على تحليل الحركة غير العادية، وأن يتخذ الإجراء المناسب. ولن يكون من السهل التقاط الرسائل الاقتحامية بتحليل حركة الشبكة. لكن كثيراً من الرسائل الاقتحامية أو البرامج الشريرة تميل إلى إظهار نماذج حركة غير عادية.
- يمكن لمشغلي الشبكات الحد من حركة المقتحمين أو أن يؤدوا أية مهمة أخرى لوقف الاقتحام.
- يستطيع مشغلو الشبكات التعاون مع مورد الخدمة من خلال تبادل المعلومات المتعلقة بالاقتحام. ويستطيع مشغّل الشبكة بالفعل أن يوقف حركة الاقتحام، وهو ما يجعله عديم الفائدة.
- يمكن لمشغلي الشبكات استعمال مختلف مصدّات الاقتحام التي تحمي الشبكة.
- يمكن تزويد الشبكات بتشكيلة لا يدخل فيها إلا الشبكات الموثوقة، بحيث لا يتمكن من الاتصال سوى المستعملين الذين تم استيقانهم وتخويلهم في شبكة موثوقة. فإذا قامت بين الشبكات علاقات الثقة هذه، صار بإمكان كل شبكة التحكم في الحركة والمستعملين. وعندها يمكن للشبكة بأكملها أن تكون مؤمنة ضد الرسائل الاقتحامية والحركات الشريرة الأخرى عندما تثق الشبكات الفرعية جميعها في الحركة الصادرة عن الشبكات الفرعية النظيرة.

4.11 المنظمات العمومية

يمكن أن تكون المنظمة العمومية منظمة حكومية أو منظمة خاصة تضم فئات من أصحاب المصالح تعمل على مكافحة الاقتحام. وقد تكون المنظمة الخاصة ربحية أو غير ربحية، ويكون لديها حل ناجع لمكافحة الاقتحام. وفيما يلي بعض النقاط التي قد ترغب المنظمات العمومية أن تأخذها في الاعتبار عند مكافحة الاقتحام.

- يمكن للمنظمات العمومية أن تعتمد نظاماً يمكّن الضحايا من تقديم تقارير عن الأضرار التي يسببها الاقتحام. ويمكن أن تقوم المنظمة بتحذير المقتحمين أو تغريمهم. ويمكن أن تكون هذه المنظمة حكومية أو منظمة خاصة قوية لها سلطة فعالة في تحذير المقتحمين.
- قد يكون لدى المنظمة العمومية برنامج تدريب على مكافحة الاقتحام أو أن تزوِّد مستعملي خدمات الوسائط المتعددة القائمة على بروتوكول الإنترنت (IP)، وموردي هذه الخدمات، ومشغلي شبكات قائمة على بروتوكول الإنترنت (IP) بمبادئ توجيهية بشأن مكافحة الاقتحام. وبعض مهارات المكافحة تتطلب خبرة واسعة، التي قد لا تتوفر لدى مورد خدمة الوسائط المتعددة القائمة على بروتوكول الإنترنت (IP) الجديدة مشغّل الشبكة.
- ويمكن للمنظمات العمومية توفير قوائم سوداء أو مراشيح يتبادلها الجمهور. ويستطيع الجمهور المشاركة في تكوين القوائم السوداء أو المراشيح.
- ويمكن للمنظمة العمومية أن تعتمد نظام موافقة على أنشطة الدعاية والإعلان. وإذا اعتمدت هذه الأنشطة على تطبيقات بروتوكول الإنترنت (IP) المتعددة الوسائط اكتسبت فعالية كبيرة، فينبغي وجود طريقة تمكن القائمين بهذه الأنشطة غير الاقتحاميين من ممارستها، لأن الدعاية تقدم معلومات مفيدة جداً للناس المحتاجين إليها، وفي حالة الموافقة عليها من المفيد لوكالات الدعاية أن يكون هناك نظام للموافقة على أنشطة الدعاية والإعلان يصعب تزييفه ومستيقن منه، بحيث تستطيع وكالات الدعاية والإعلان استعماله بدون اعتبارها خطأ من جماعات الاقتحام.

5.11 اعتبارات أخرى

وهناك اعتبارات أخرى جديرة بالمراعاة لا تخص ما ورد ذكره آنفاً:

- يرجَّح أن مشكلة الاقتحام لن تزول، بصرف النظر عن شتى الجهود المبذولة الرامية إلى مكافحتها. فلن تنقطع أبداً عن الظهور رسائل اقتحام جديدة، وينبغي إجراء دراسات جديدة لمكافحة هذه الرسائل. ولكن إذا أجريت البحوث مسبقاً على طرائق مكافحة الاقتحام، يمكن أن تكون بيئة التطبيقات أفضل، والخدمات المعتمدة على هذه التطبيقات أفضل.
- ينبغي إعمال مختلف طرائق المكافحة معاً. إذ لا يوجد حتى الآن حل خارق، يقضي على مشكلة الاقتحام. فينبغي الأخذ بمختلف الطرائق معاً لمكافحة مختلف أنماط الاقتحام الممكن حدوثها في مختلف الأماكن بمختلف التقنيات.
- ربما كان الحل الأمثل هو جعل الاقتحام صعباً ومكلفاً. إذ إن جلّ ما يتوخّاه المقتحمون هو استعمال طريقة رخيصة وسهلة للدعاية والإعلان. ومتى صعب الاقتحام وزادت تكاليفه أو قَسَت عقوبته، يكفّ عندئذ المقتحمون عن مزاولة هذا النشاط.

بيبليوغرافيا

[b-ITU-T Q.814] Recommendation ITU-T Q.814 (2000), *Specification of an electronic data interchange interactive agent*.

[b-ITU-T T.124] Recommendation ITU-T T.124 (1998), *Generic Conference Control*.

[b-ITU-T T.180] Recommendation ITU-T T.180 (1998), *Homogeneous access mechanism to communication services*.

[b-ITU-T X.509] Recommendation ITU-T X.509 (2005) | ISO/IEC 9594-8:2005, *Information technology – Open Systems Interconnection – The Directory: Public-key and attribute certificate frameworks*.

[b-ITU-T X.741] Recommendation ITU-T X.741 (1995) | ISO/IEC 10164-9:1995, *Information technology – Open Systems Interconnection – Systems management: Objects and attributes for access control*.

[b-IETF RFC 1991] IETF RFC 1991 (1996), *PGP Message Exchange Formats*. <http://www.ietf.org/rfc/rfc1991.txt?number=1991>

[b-IETF RFC 3428] IETF RFC 3428 (2002), *Session Initiation Protocol (SIP) Extension for Instant Messaging*. <http://www.ietf.org/rfc/rfc3428.txt?number=3428>

[b-IETF RFC 4871] IETF RFC 4871 (2007), *DomainKeys Identified Mail (DKIM) Signatures*. <http://www.ietf.org/rfc/rfc4871.txt?number=4871>

[b-IETF RFC 4880] IETF RFC 4880 (2007), *OpenPGP Message Format*. <http://www.ietf.org/rfc/rfc4880.txt?number=4880>

[b-IETF RFC 4981] IETF RFC 4981 (2007), *Survey of Research towards Robust Peer-to-Peer Networks: Search Methods*. <http://www.ietf.org/rfc/rfc4981.txt?number=4981>

[b-IETF RFC 5039] IETF RFC 5039 (2008), *The Session Initiation Protocol (SIP) and Spam*. <http://www.ietf.org/rfc/rfc5039.txt?number=5039>

[b-IETF RFC 5090] IETF RFC 5090 (2008), *RADIUS Extension for Digest Authentication*. <http://www.ietf.org/rfc/rfc5090.txt?number=5090>

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 (ISDN)
السلسلة J	الشبكات الكبلية وإرسال إشارات تلفزيونية وبرامج صوتية وإشارات أخرى متعددة الوسائط
السلسلة K	الحماية من التداخلات
السلسلة L	بناء الكبلات وغيرها من عناصر المنشآت الخارجية وإنشاؤها وحمايتها
السلسلة M	إدارة الاتصالات، بما في ذلك شبكة إدارة الاتصالات وصيانة الشبكات
السلسلة N	صيانة الدارات الإذاعية الدولية لإرسال البرامج الصوتية والتلفزيونية
السلسلة O	مواصفات أجهزة القياس
السلسلة P	جودة الإرسال الهاتفي والمنشآت الهاتفية وشبكات الخطوط المحلية
السلسلة Q	التبديل والتشوير
السلسلة R	التراسل الإبراقي
السلسلة S	التجهيزات الانتهائية لخدمات الإبراق
السلسلة T	تجهيزات مطرافية للخدمات التلماتية
السلسلة U	التبديل الإبراقي
السلسلة V	اتصالات البيانات على الشبكة الهاتفية
السلسلة X	**شبكات البيانات والاتصالات بين الأنظمة المفتوحة ومسائل الأمن**
السلسلة Y	البنية التحتية العالمية للمعلومات وملامح بروتوكول الإنترنت وشبكات الجيل التالي
السلسلة Z	اللغات والجوانب العامة للبرمجيات في أنظمة الاتصالات

طُبعت في سويسرا
جنيف، 2009