الاتحـــــــــاد الدولـــــــــي للاتصـــــــــالات

ITU-T

قطـــاع تقييس الاتصـــالات
في الاتحاد الدولي للاتصالات

X.1245

(2010/12)

السلسلة X: شبكات البيانات والاتصالات بين الأنظمة المفتوحة ومسائل الأمن

أمن الفضاء السيبراني – مكافحة البريد الاقتحامي

إطار مكافحة البريد الاقتحامي في تطبيقات الوسائط المتعددة القائمة على بروتوكول الإنترنت

التوصيـــة ITU-T X.1245

الاتحاد الدولي للاتصالات

توصيات السلسلة X الصادرة عن قطاع تقييس الاتصالات

شبكات البيانات والاتصالات بين الأنظمة المفتوحة ومسائل الأمن

الشبكات العمومية للبيانات	X.199–X.1
التوصيل البيني للأنظمة المفتوحة	X.299–X.200
التشغيل البيني للشبكات	X.399–X.300
أنظمة معالجة الرسائل	X.499–X.400
الدليـــل	X.599–X.500
التشغيل البيني لأنظمة التوصيل OSI ومظاهر النظام	X.699–X.600
إدارة التوصيل البيني للأنظمة المفتوحة (OSI)	X.799–X.700
الأمن	X.849–X.800
تطبيقات التوصيل البيني للأنظمة المفتوحة (OSI)	X.899–X.850
المعالجة الموزعة المفتوحة	X.999–X.900
أمن المعلومات والشبكات	
الجوانب العامة للأمن	X.1029–X.1000
أمن الشبكة	X.1049–X.1030
إدارة الأمن	X.1069–X.1050
الخصائص البيومترية	X.1099–X.1080
تطبيقات وخدمات آمنة	
أمن البث المتعدد	X.1109–X.1100
أمن الشبكة المحلية	X.1119–X.1110
أمن الخدمات المتنقلة	X.1139–X.1120
أمن الويب	X.1149–X.1140
بروتوكولات الأمن	X.1159–X.1150
الأمن بين جهتين نظيرتين	X.1169–X.1160
أمن معرفات الهوية عبر الشبكات	X.1179–X.1170
أمن التلفزيون القائم على بروتوكول الإنترنت	X.1199–X.1180
أمن الفضاء السيبراني	
الأمن السيبراني	X.1229–X.1200
مكافحة البريد الاقتحامي	**X.1249–X.1230**
إدارة الهوية	X.1279–X.1250
تطبيقات وخدمات آمنة	
اتصالات الطوارئ	X.1309-X.1300
أمن شبكات المحاسيس واسعة الانتشار	X.1339–X.1310
تبادل معلومات الأمن السيبراني	
تبادل مواطن الضعف/الحالة	X.1539–X.1520
تبادل الأحداث/الأحداث العارضة/المعلومات الحدسية	X.1549–X.1540
تبادل السياسات	X.1559–X.1550
طلب المعلومات الحدسية والمعلومات الأخرى	X.1569–X.1560
تعرف الهوية والاكتشاف	X.1579–X.1570
التبادل المضمون	X.1589–X.1580

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

التوصيـــة ITU-T X.1245

إطار مكافحة البريد الاقتحامي في تطبيقات الوسائط المتعددة القائمة على بروتوكول الإنترنت

ملخص

تقدم هذه التوصية الإطار العام لمكافحة البريد الاقتحامي في تطبيقات الوسائط المتعددة القائمة على بروتوكول الإنترنت، مثل المهاتفة باستعمال بروتوكول الإنترنت (IP) والمراسلة اللحظية والمؤتمرات متعددة الوسائط وما إلى ذلك. ويشمل الإطار أربع وظائف لمكافحة الاقتحام، أي الوظائف المركزية لمكافحة الاقتحام (CASF) ووظائف مكافحة الاقتحام جهة المتلقي (RASF) ووظائف مكافحة الاقتحام جهة المرسل (SASF) ووظائف متلقي البريد الاقتحامي (SRF). وتصف هذه التوصية الوظائف والسطوح البينية المحددة لكل وظيفة مكافحة اقتحام الوسائط المتعددة العاملة ببروتوكول الإنترنت.

التسلسل التاريخي

الصيغة	التوصية	تاريخ الموافقة	لجنة الدراسات
1.0	ITU-T X.1245	2010/12/17	17

الكلمات الرئيسية

وظائف مكافحة الاقتحام، اقتحام الوسائط المتعددة العاملة ببروتوكول الإنترنت، والبريد الاقتحامي.

تمهيـــد

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

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

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

وفي بعض مجالات تكنولوجيا المعلومات التي تقع ضمن اختصاص قطاع تقييس الاتصالات، 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/.

جـــدول المحتـــويات

الصفحة

التوصيـــة ITU-T X.1245

إطار مكافحة البريد الاقتحامي في تطبيقات الوسائط المتعددة القائمة على بروتوكول الإنترنت

1 مجال التطبيق

تقدم هذه التوصية الإطار العام لمكافحة البريد الاقتحامي للوسائط المتعددة العاملة ببروتوكول الإنترنت (IP). ويمكن استخدام الإطار في تطبيقات الوسائط المتعددة القائمة على البروتوكول IP، مثل المهاتفة باستعمال بروتوكول الإنترنت والمراسلة اللحظية والمؤتمرات متعددة الوسائط وما إلى ذلك. ويضم الإطار أربع وظائف لمكافحة الاقتحام هي: الوظائف الأساسية لمكافحة الاقتحام (CASF)، ووظائف مكافحة الاقتحام جهة المتلقي (RASF)، ووظائف مكافحة الاقتحام جهة المرسل (SASF)، ووظائف متلقي البريد الاقتحامي (SRF). وتصف التوصية الوظائف والسطوح البينية المحددة لكل وظيفة محاربة البريد الاقتحامي للوسائط المتعددة العاملة ببروتوكول الإنترنت. أما الوسائل التقنية الخاصة بتنفيذ الإطار فيقع خارج مجال تطبيق هذه التوصية.

وينبغي مراعاة الامتثال لكافة القوانين والتشريعات ذات الصلة قبل اعتماد طرائق مكافحة البريد الاقتحامي الواردة في هذه التوصية.

2 المراجع

لا يوجد.

3 التعاريف

1.3 المصطلحات المعرّفة في مواضع أخرى

تستعمل هذه التوصية المصطلحات التالية المعرفة في مواضع أخرى:

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

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

2.3 المصطلحات المعرّفة في هذه التوصية

تعرف هذه التوصية المصطلحات التالية:

1.2.3 وظيفة مكافحة الاقتحام (ASF): وظيفة منطقية لمكافحة الاقتحام في تطبيقات الوسائط المتعددة القائمة على بروتوكول الإنترنت. ويمكن وضع وظيفة مكافحة الاقتحام في عناصر الشبكة مثل المخدِّم الوكيل ومخدِّم التطبيق وما إلى ذلك.

2.2.3 القائمة السوداء: قائمة تحدد أشخاصاً أو مصادر تستعمل خدمات الاتصالات يُرفض النفاذ إلى بعض موارد الاتصالات فيها.

3.2.3 الوظيفة المركزية لمكافحة الاقتحام (CASF): شكل من أشكال وظائف مكافحة الاقتحام يتم فيها تعرّف البريد الاقتحامي للوسائط المتعددة العاملة ببروتوكول الإنترنت ومنعه. كما تتميز بالقدرة على إدارة سياسات مكافحة الاقتحام ومراقبة الوظيفتين RASF وSASF.

4.2.3 اقتحام الوسائط المتعددة العاملة ببروتوكول الإنترنت: رسائل أو نداءات غير مرغوبة تمر عبر تطبيقات الوسائط المتعددة القائمة على بروتوكول الإنترنت وتتميّز عادة بخصائص البريد الاقتحامي مثل الإرسال بالجملة. وخلافاً للاقتحام التقليدي عبر البريد الإلكتروني يدل اقتحام الوسائط المتعددة العاملة ببروتوكول الإنترنت على اقتحام طرائق الاتصالات التي تستعمل بروتوكول الإنترنت، مثل خدمة المراسلة اللحظية أو المهاتفة عبر الإنترنت.

5.2.3 وظيفة مكافحة الاقتحام جهة المتلقي (RASF): مرحلة من مراحل وظيفة مكافحة الاقتحام يتم فيها تعرّف البريد الاقتحامي للوسائط المتعددة IP الذي يسلم إلى مقاصد البريد عبر حدود الشبكة الداخلية. ويمكن وضع الوظيفة RASF في عناصر الشبكة، حيث ترسل طلبات الاتصال الداخلة في مرحلتها الأخيرة إلى مقاصد البريد الاقتحامي.

6.2.3 وظيفة مكافحة الاقتحام جهة المرسل (SASF): مرحلة من مراحل وظيفة مكافحة الاقتحام يتم فيها تعرّف البريد الاقتحامي للوسائط المتعددة IP الذي أرسل من المقتحمين إلى حدود الشبكة الخارجية. ويمكن وضع الوظيفة SASF في عناصر الشبكة، حيث ترسل طلبات الاتصال الخارجة في مرحلتها الأولى والواردة من المقتحمين.

7.2.3 متلقي البريد الاقتحامي: كيان أو شخص يتلقى بريداً اقتحامياً.

8.2.3 وظيفة متلقي البريد الاقتحامي (SRF): إحدى وظائف مكافحة اقتحام يتمثل دورها في تعرّف بريد اقتحامي للوسائط المتعددة IP يصل إلى المقصد ومنعه. ويمكن وضع الوظائف SRF في الشبكة المحلية أو في مطاريف مقاصد البريد الاقتحامي.

9.2.3 القائمة البيضاء: قائمة تحدد هويات أشخاص أو مصادر تستعمل خدمات الاتصالات، وهي معرفة أو موثوقة أو مسموحة علنياً.

4 المختصرات

تستعمل هذه التوصية المختصرات التالية:

ARS نظام استجابة أوتوماتي *(Automated Response System)*

ASF وظائف مكافحة الاقتحام *(Anti-Spam Functions)*

CA سلطة إصدار شهادات *(Certification Authority)*

CAS مكافحة اقتحام مركزية *(Core Anti-Spam)*

CASF وظائف مكافحة اقتحام مركزية *(Core Anti-Spam Functions)*

CRL قائمة إلغاء الشهادات *(Certificate Revocation List)*

DAC مراقبة النفاذ استنسابياً *(Discretionary Access Control)*

HBAC مراقبة النفاذ على أساس السجلات *(History-based Access Control)*

IM مراسلة لحظية *(Instant Messaging)*

IP بروتوكول الإنترنت *(Internet Protocol)*

IPSec أمن بروتوكول الإنترنت *(Internet Protocol Security)*

L2TP بروتوكول أنفاق الطبقة 2 *(Layer 2 Tunneling Protocol)*

MAC مراقبة النفاذ الإلزامية *(Mandatory Access Control)*

MTA وكيل نقل البريد *(Mail Transfer Agent)*

NDAC مراقبة النفاذ غير الاستنسابية *(Non-Discretionary Access Control)*

OTP كلمة مرور لمرة واحدة *(One Time Password)*

PBAC مراقبة النفاذ على أساس القصد *(Purpose-based Access Control)*

PKI بنية تحتية أساسية عمومية *(Public Key Infrastructure)*

RAS مكافحة الاقتحام جهة المتلقي *(Recipient-side Anti-Spam)*

RASF وظائف مكافحة الاقتحام جهة المتلقي *(Recipient-side Anti-Spam Functions)*

RBAC مراقبة النفاذ على أساس الدور *(Role-based Access Control)*

RuBAC مراقبة النفاذ على أساس القاعدة *(Rule-based Access Control)*

SAS مكافحة الاقتحام جهة المرسل *(Sender-side Anti-Spam)*

SASF وظائف مكافحة الاقتحام جهة المرسل *(Sender-side Anti-Spam Functions)*

SPF إطار سياسة المرسل *(Sender Policy Framework)*

SR متلقي البريد الاقتحامي *(Spam Recipient)*

SRF وظائف متلقي البريد الاقتحامي *(Spam Recipient Functions)*

SSL طبقة مقابس الأمن *(Secure Socket Layer)*

TCAC مراقبة نفاذ قائمة على قيود مؤقتة *(Temporal Constraints Access Control)*

TTP طرف ثالث موثوق *(Trusted Third Party)*

TTS من النص إلى الكلام *(Text To Speech)*

VoIP نقل الصوت عبر بروتوكول الإنترنت *(Voice over Internet Protocol)*

VPN شبكة خاصة تقديرية *(Virtual Private Network)*

5 الاصطلاحات

الوظائف: تتحدد "الوظائف" في سياق إطار مكافحة اقتحام الوسائط المتعددة العاملة ببروتوكول الإنترنت بوصفها مجموعة كيانات وظيفية، ويُرمز إليها بالشكل التالي:

الفِدرة الوظيفية: تتحدد "الفدرة الوظيفية" في سياق إطار مكافحة اقتحام الوسائط المتعددة العاملة ببروتوكول الإنترنت بوصفها مجموعة كيانات وظيفية قبل تجزئتها على مستوى التفاصيل الواردة في هذه التوصية. ويُرمَز إليها بالشكل التالي:

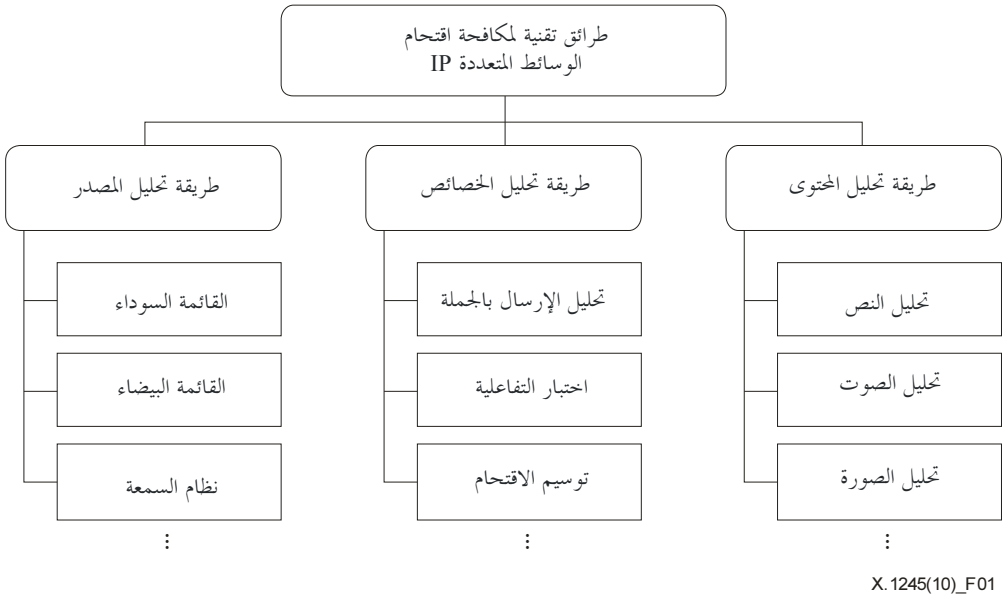
6 الطرائق التقنية لمكافحة اقتحام الوسائط المتعددة العاملة ببروتوكول الإنترنت

يمكن تحديد اقتحام الوسائط المتعددة IP بأنه مجموعة رسائل أو نداءات غير مطلوبة عبر تطبيقات الوسائط المتعددة القائمة على أساس بروتوكول الإنترنت. ولتمييز اقتحام الوسائط المتعددة IP عن اقتحام البريد الإلكتروني، فإن اقتحام الوسائط المتعددة IP يعني اقتحام طرائق الاتصالات التي تستعمل البروتوكول IP مثل المهاتفة باستعمال بروتوكول الإنترنت والمراسلة اللحظية وما إلى غير ذلك. ولاقتحام الوسائط المتعددة IP عادة خصائص مميزة يمكن رصدها في تطبيقات الوسائط المتعددة العادية القائمة على بروتوكول الإنترنت. ويمكن استعمال هذه الخصائص في وظائف مكافحة الاقتحام من أجل تحديد البريد الاقتحامي ومنعه من خلال تطبيق الوظائف على العناصر المناسبة للشبكة IP.

ويمكن تصنيف الطرائق التقنية لمكافحة اقتحام الوسائط المتعددة IP وفقاً للفئات الثلاث التالية:

- مكافحة اقتحام الوسائط المتعددة IP بتحليل المصدر،
- مكافحة اقتحام الوسائط المتعددة IP بتحليل الخصائص،
- مكافحة اقتحام الوسائط المتعددة IP بتحليل المحتوى.

ويبين الشكل 1 الطرائق التقنية الثلاث لمكافحة اقتحام الوسائط المتعددة IP ويقدم أمثلة لتقنيات مكافحة الاقتحام.



الشكل 1 – يبين الطرائق التقنية الثلاث لمكافحة اقتحام الوسائط المتعددة IP ويقدم أمثلة لتقنيات مكافحة الاقتحام

وقد استخدم العديد من تقنيات مكافحة الاقتحام الواردة في الشكل 1 لمكافحة اقتحام البريد الإلكتروني، وهي قابلة للاستخدام أيضاً لمكافحة اقتحام الوسائط المتعددة IP. ولا تقتصر تقنيات مكافحة الاقتحام للوسائط المتعددة IP على هذه الأمثلة.

ولا بدّ من تفاعل وظائف مكافحة الاقتحام فيما بينها على الشبكة من أجل الاستفادة من هذه التقنيات. ويرد وصف كيانات مكافحة الاقتحام وسطوحها البينية اللازمة لتنفيذ طرائق مكافحة الاقتحام في الفقرات التالية. وقد لا يكون استعمال تقنية مكافحة اقتحام واحدة كافياً لمكافحة اقتحام الوسائط المتعددة IP. وفي مثل هذه الحالة، قد يكون من الضروري استعمال أكثر من تقنية مكافحة واحدة في نفس الوقت على الشبكة IP للحصول على مزيد من الفعالية لترشيح البريد الاقتحامي.

1.6 طريقة تحليل المصدر

يمكن تحديد ما إذا كان تطبيق متعدد الوسائط IP قادم من مصدر ما اقتحاماً أم لا من خلال تحليل معلومات مصدر التطبيق متعدد الوسائط IP مثل معلومات السمعة أو سجلات المصدر فيما يخص الاقتحام. ويمكن استعمال عناوين بروتوكول الإنترنت واسم الميدان ورقم الهاتف ومعرّف هوية المستعمِل بوصفها معرّفات هوية المصدر.

وكأمثلة لتقنيات مكافحة الاقتحام على أساس المصدر، هنالك القائمة السوداء ونظام السمعة وغيرهما. وتستعمل هذه التقنيات على نطاق واسع لمكافحة اقتحام البريد الإلكتروني، ويمكن استخدامها أيضاً لمحاربة اقتحام الوسائط المتعددة IP. ويرد وصف إمكانية تطبيق هذه التقنيات لمكافحة اقتحام الوسائط المتعددة IP في المرجع [b-ITU-T X.1244]. غير أن طرائق تحليل المصدر قد تعاني من نقاط ضعف تحدّ من فعالية تقنيات مكافحة الاقتحام. فقد يحاول المقتحمون، على سبيل المثال، انتحال هوية المرسل أو أن يتمكّنوا من إحداث العديد من حسابات الخدمة. لذلك، يفترض أن تساعد التدابير التالية على زيادة فعالية تقنيات مكافحة الاقتحام استناداً إلى المصدر في مكافحة اقتحام الوسائط المتعددة IP:

- الاستيقان الأكيد من مصادر تطبيقات الوسائط المتعددة القائمة على بروتوكول الإنترنت،
- الإدارة الفعّالة لسياسة تعرّف الاقتحام والمعلومات المتصلة به.

وفي البداية، يتعيّن أن تتميّز المعلومات عن مصدر تطبيقات الوسائط المتعددة IP بموثوقية عالية لضمان تنقية فعالة للاقتحام، إذ إن المقتحمين يحاولون الالتفاف لتجنّب تقنيات مكافحة الاقتحام هذه من خلال استحداث عدد هائل من حسابات الخدمة أو محاولة انتحال هوية مرسل لإخفاء حقيقة أن المرسل مقتحم. لذلك، فإن استيقاناً مشدداً لمصادر تطبيق متعدد الوسائط قائم على بروتوكول الإنترنت مفيد لتوفير درجة عالية من الموثوقية للمعلومات عن المصدر.

وكما ذكر آنفاً، فإن معلومات تنقية الاقتحام (مثل القائمة البيضاء والقائمة السوداء وغيرهما) فضلاً عن مصادر تطبيقات الوسائط المتعددة IP تستعمل لتعرف هوية البريد الاقتحامي. لذلك لا بد من إدارة معلومات تنقية البريد الاقتحامي ومعايير تعرف البريد الاقتحامي إدارة فعالة.

ولهذه التقنية فائدة تكمن في إمكانية منع البريد الاقتحامي من الوصول قبل تسليمه إلى المقصد. وعلاوة على ذلك، وبافتراض أن الاعتبارات الواردة أعلاه قد استوفيت، يمكن مكافحة البريد الاقتحامي مكافحة فعالة بجهد ضئيل نسبياً مقارنة بتقنيات مكافحة الاقتحام الأخرى مثل تحليل المحتوى وتحليل الخصائص وغيرها.

2.6 طريق تحليل الخصائص

1.2.6 طرائق مكافحة الاقتحام القائمة على تحليل الخصائص

لاقتحام الوسائط المتعددة القائمة على بروتوكول الإنترنت خصائص مميزة يمكن رصدها في تطبيقات عادية للوسائط المتعددة القائمة على بروتوكول الإنترنت. فاقتحام الوسائط المتعددة IP مثلاً يصل أحياناً بكميات كبيرة وله تفاعلية محدودة مقارنة بتطبيقات الوسائط المتعددة IP العادية. ويمكن اعتبار تطبيق ما للوسائط المتعددة IP اقتحاماً يستبعده الترشيح عندما يتميّز بواحدة من هذه الخصائص أو أكثر. وفيما يلي بعض خصائص اقتحام الوسائط المتعددة IP على سبيل المثال لا الحصر؛

- إرسال بالجملة

يصل بريد اقتحام الوسائط المتعددة IP أحياناً بالجملة لأن المقتحمين يحاولون عادة إرسال هذا البريد الاقتحامي إلى عدد كبير من المقاصد في كل مرة من أجل الحد، قدر الإمكان، من تكاليف عملية الاقتحام. ويمكن اعتبار وصول كمية هائلة من تطبيقات الوسائط المتعددة IP من مصدر ما إلى العديد من المقاصد في فترة قصيرة اقتحاماً محتملاً.

- تفاعلية محدودة

لا يتيح بريد اقتحام الوسائط المتعددة IP في الكثير من الحالات إلا تفاعلية محدودة لأن المقتحمين ينزعون إلى إرسال البريد الاقتحامي باستعمال آلات بدلاً من أشخاص، وذلك للحد من تكاليف عملية الاقتحام. ففي اقتحام المراسلة اللحظية

أو في اقتحام جلسة دردشة على الخط مثلاً، لا يجيب مرسلو البريد الاقتحامي لأن الرسالة الاقتحامية مرسلة بواسطة آلات الاقتحام. واقتحام مهاتفة عبر بروتوكول الإنترنت (VoIP)، وهو شكل من أشكال الترويج التجاري على الخط، قد يتيح أيضاً تفاعلية محدودة عندما يُرسل باستعمال نظام ARS. وبالتالي، يمكن التعرّف على الاقتحام من خلال اختبار ما إذا كان مرسل تطبيق الوسائط المتعددة IP يتيح التفاعلية أم لا. أما تقنيات مكافحة الاقتحام الأكثر شيوعاً القائمة على هذه الطريقة في نظام البريد الإلكتروني فهي اختبار Turing والقائمة الرمادية التي تختبر تفاعلية المرسل والوكيل MTA على التوالي.

2.2.6 استعمال معلومات البروتوكول لمكافحة الاقتحام

إن استعمال معلومات البروتوكول أكثر فعالية من استعمال معلومات المحتوى من أجل تعرف الاقتحام باستعمال طريقة تحليل الخصائص. فجزء البروتوكول من تطبيق الوسائط المتعددة IP يمكن استعماله في تعرف هوية الاقتحام بتحليل مصدر التطبيق. كما أن تعرف الاقتحام باستعمال معلومات البروتوكول قبل تسليم المحتوى في تطبيقات الوسائط المتعددة IP المُرسلة إلى المقصد تتطلب جهداً أقل وتتميّز بفعالية أكبر مقارنة بتقنيات مكافحة الاقتحام الأخرى التي تستعمل معلومات المحتوى. وتؤكد النتائج التالية أن هذا الاستنتاج أكثر ملاءمة.

– معلومات عن توريد التطبيق

يضم جزء البروتوكول من تطبيقات الوسائط المتعددة IP معلومات تتعلق بتوريد هذه التطبيقات، مثل المصدر والمقصد ووقت التسليم وبروتوكول التسليم المستخدم، وما إلى غير ذلك. ومن الممكن استعمال بعض من هذه الأجزاء لتعرّف هوية الاقتحام.

– توقيت التحليل

تُسلَّم معلومات البروتوكول لبدء خدمة ما قبل تسليم محتوى تطبيقات الوسائط المتعددة IP. مثال في خدمة المهاتفة باستعمال بروتوكول الإنترنت (VoIP)، تجري عملية التشوير التي تستعمل خلالها معلومات البروتوكول قبل بدء عملية النداء. لذلك من الممكن تعرف الاقتحام قبل تسليمه إلى المقصد من خلال تحليل معلومات البروتوكول.

– التجفير

تُسلَّم رسائل البروتوكول عادة دون تجفير، مع أن محتوى تطبيقات الوسائط المتعددة IP قد يكون مجفراً. وتجفير الرزم IP يجعل تحليلها عسيراً جداً أو تسجيل تفكيك تجفيرها. ولذلك، فإن تحليل جزء البروتوكول أسهل من تحليل جزء المحتوى في تطبيقات الوسائط المتعددة IP.

– نمط الوسائط

لا يستعمل جزء البروتوكول من تطبيقات الوسائط المتعددة IP إلا نمطاً واحداً من الوسائط بينما يستعمل جزء المحتوى منها أحياناً معلومات متعددة الوسائط يصعب تحليلها.

– مسار التسليم

تمر رسائل البروتوكول الخاصة بالجلسة أو ببدء الخدمة عبر تجهيزات الشبكة، مثل مخدّم التطبيق للمراسلة اللحظية والمخدّمات الوكيلة لمكالمات المهاتفة VoIP، التي يمكنها الحصول على معلومات توريد تطبيقات الوسائط المتعددة IP من رسائل البروتوكول. ومن ناحية أخرى يمكن إرسال رسائل المحتوى مباشرة من المرسل إلى المتلقي دون المرور عبر تجهيزات الشبكة. وفي هذه الحالة قد يكون من الصعب تحليل تطبيقات الوسائط المتعددة IP.

3.6 طريق تحليل المحتوى

تستعمل نتائج تحليل محتوى تطبيقات الوسائط المتعددة IP في هذه الطبقة لتعرف هوية الاقتحام. وتستعمل هذه الطريقة على نطاق واسع لمكافحة اقتحام البريد الإلكتروني. وقد يكون تحليل محتوى تطبيقات الوسائط المتعددة القائمة على بروتوكول الإنترنت أصعب بكثير من حالة الرسائل الإلكترونية، إذ إن تطبيقات الوسائط المتعددة IP يمكنها أن تكون في الوقت الفعلي

و/أو أن تستعمل معلومات متعددة الوسائط، بينما تقوم الرسائل الإلكترونية على أساس النص وليست في الوقت الفعلي. وفيما يلي بعض الاعتبارات التي من شأنها مكافحة اقتحام الوسائط المتعددة IP بصورة فعالة في إطار طريقة تحليل المحتوى.

– مدة تحليل المحتوى

يتعين تحليل المحتوى في غضون فترة معقولة من الوقت لتمكين مستعملي تطبيقات الوسائط المتعددة IP من التعرف على هوية الاقتحام. وقد يكون من الممكن في تطبيقات الوسائط المتعددة IP في الوقت الفعلي إجراء تحليل المحتوى قبل بدء التطبيق.

– دقة تحليل المحتوى

يتعين أن يتسم تحليل محتوى تطبيقات الوسائط المتعددة IP بدرجة مناسبة من الجودة للتمكّن من تعرف الاقتحام بصورة فعالة. وستساعد تكنولوجيات تعرف الصوت والصورة المتطورة جداً على ذلك، إذ إن تحليل المحتوى متعدد الوسائط فائق الصعوبة مقارنة بتحليل النص.

– تجفير المحتوى

قد يكون تحليل محتوى تطبيقات الوسائط المتعددة IP صعباً جداً أو يستحيل تفكيك تجفيره عندما تكون الرزم IP مجفرة.

– مسار تسليم المحتوى

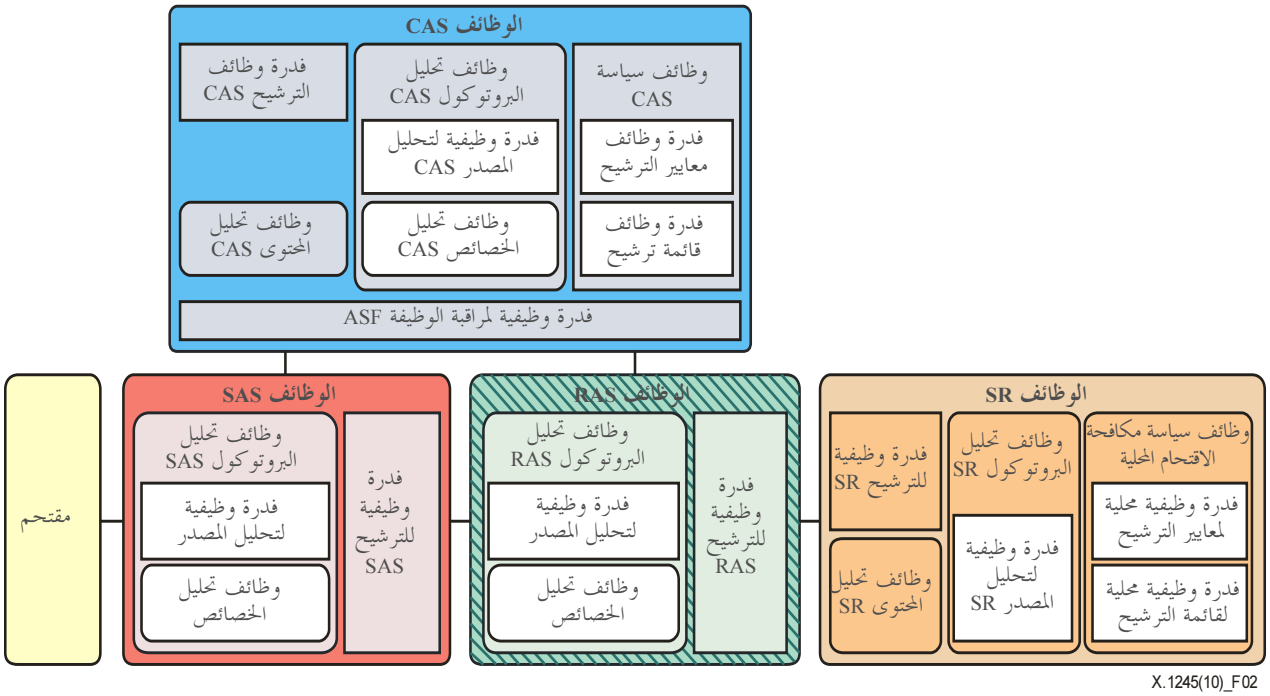
يتم تحليل محتوى تطبيقات الوسائط المتعددة IP عندما يمر عبر تجهيزات شبكة ما مثل مخدّم تطبيق أو مخدم وسائط مزوّد بوظيفة تحليل المحتوى.

وفي العديد من الحالات قد لا تستوفي تطبيقات الوسائط المتعددة IP المعايير المطلوبة. وفي حالة تطبيقات الوسائط المتعددة IP في الوقت الفعلي مثل المهاتفة VoIP، قد يتعذّر كشف الاقتحام وترشيحه باتباع طريقة تحليل المحتوى في غضون فترة زمنية معقولة بالنسبة لمستعملي الخدمة، لأنه لا يمكن تحليل المحتوى إلا بعد إقامة دورة الاتصال بين طالب النداء ومتلقيه. ومن ناحية أخرى، قد يُتاح وقت كاف لتحليل المحتوى في حالة تطبيقات الوسائط المتعددة IP في غير الوقت الفعلي مثل حالة الرسائل الصوتية المسجلة. ومع هذا قد تتخلل تحليل المحتوى صعوبات في الحصول على معلومات وافية لتعرف هوية الاقتحام بسبب التكنولوجيات غير المكتملة لتعرف الكلام والصورة أو بسبب الكمية غير الكافية من المحتوى. وعند تحليل محتوى تطبيقات الوسائط المتعددة IP النصية مثل خدمات المراسلة اللحظية وخدمات الرسائل النصية، قد يكون تعرف الاقتحام صعباً أيضاً إذا كان المحتوى مجفراً أو إذا أرسل مباشرة بين مستعملي الخدمة دون المرور عبر تجهيزات الشبكة ليخضع لتحليل المحتوى.

7 إطار مكافحة الاقتحام للوسائط المتعددة العاملة ببروتوكول الإنترنت

يتعيّن على كيانات شبكات بروتوكول الإنترنت المزوّدة بوظائف مكافحة الاقتحام أن تتفاعل مع بعضها البعض لمكافحة اقتحام الوسائط المتعددة IP. ويرد في هذه الفقرة وصف وظائف كيانات مكافحة الاقتحام وتفاعلاتها الضرورية لتطبيق طرائق مكافحة الاقتحام. وقد لا يكون استخدام تقنية واحدة فقط لمكافحة الاقتحام فعالاً إلى درجة تكفي لمكافحة اقتحام الوسائط المتعددة. لذلك قد يتعيّن استخدام أكثر من تقنية واحدة في نفس الوقت في شبكات بروتوكول الإنترنت من أجل ترشيح البريد الاقتحامي ترشيحاً أكثر فعالية.

وتصف هذه الفقرة إطار مكافحة اقتحام الوسائط المتعددة IP. وهو مصمم بحيث يمكن توسيعه بسهولة ليشمل مختلف الوسائل التقنية لمكافحة الاقتحام في مختلف التطبيقات والشبكات. كما أنه مصمَّم لحماية المستعملين والشبكات من اقتحام الوسائط المتعددة IP. ويمكن للاقتحام أن يظهر في أي مكان؛ لذا ينبغي توفير آليات كشف مختلف أنواع الاقتحام وترشيحها في كامل الشبكة.



الشكل 2 – إطار مكافحة اقتحام الوسائط المتعددة IP

يتكون إطار مكافحة اقتحام الوسائط المتعددة IP من خمسة عناصر على النحو المبيّن في الشكل 2. وتصف الفقرات التالية الوظائف والسطوح البينية في كل عنصر.

1.7 المقتحم

يولد المقتحم اقتحاماً وينشره عبر الشبكة. فهو مصدر الاقتحامات. ووظائف مكافحة الاقتحام لا تطبّق في كيان المقتحم.

2.7 وظائف مكافحة الاقتحام جهة المرسل (SAS)

وظائف مكافحة الاقتحام جهة المرسل (SASF) هي مجموعة وظائف مكافحة الاقتحام دورها تعرف الاقتحام الذي يولده المقتحمون في الوسائط المتعددة IP ومنعه. ويمكن تطبيق الوظائف SASF على عناصر الشبكة من قبيل مخدم الوكيل، حيث يرسل المقتحمون طلبات الاتصال الخارجة في مرحلتها الأخيرة. وتتفاعل الوظيفة SASF مع الوظائف المركزية لمكافحة الاقتحام (CASF) من أجل تنفيذ وظائف مكافحة الاقتحام في الوظيفة SASF. والطريقة الأكثر فعالية هي منع الاقتحام في المصدر قبل أن ينتشر في الشبكة، مع أن الوظيفة SASF قد تؤدي دوراً أقل نشاطاً من المكوّنات الأخرى في بيئة الاتصالات الفعلية.

وتتألف الوظيفة SASF من وظائف تحليل البروتوكول SAS وفدرة وظائف الترشيح SAS لمراقبة ترشيح الاقتحام. وتصف الفقرات التالية مختلف التقنيات التي يمكن للوظائف SASF اعتمادها لمكافحة اقتحام الوسائط المتعددة IP.

1.2.7 فدرة وظائف الترشيح SAS

تحدد فدرة وظائف الترشيح SAS ما إذا كان تطبيق الوسائط المتعددة القائم على بروتوكول الإنترنت والذي يتم تحليله اقتحاماً أم لا، وذلك استناداً لنتائج تحليل وظائف تحليل البروتوكول SAS وسياسة مكافحة الاقتحام. ولهذا السبب تعمل هذه الفدرة مع الوظائف CASF ووظائف مكافحة الاقتحام الأخرى أو مع الفِدر الوظيفية في الوظائف SASF.

2.2.7 وظائف تحليل البروتوكول SAS

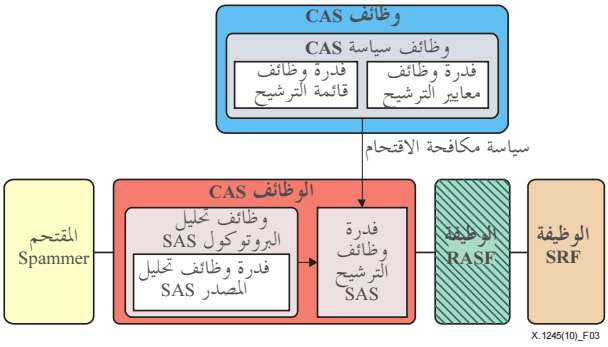
تحلل وظائف تحليل البروتوكول SAS معلومات بروتوكول تطبيقات الوسائط المتعددة IP الواصلة. وهي تتألف من فدرة وظيفية لتحليل المصدر SAS ووظائف تحليل الخصائص SAS التي تحلل معلومات مصدر تطبيقات الوسائط المتعددة القائمة على بروتوكول الإنترنت وخصائصها على التوالي.

i) فدرة وظيفية لتحليل المصدر SAS

تستطيع الوظائف SASF أن تميّز اقتحام الوسائط المتعددة IP عن التطبيقات غير الاقتحامية للوسائط المتعددة IP، وذلك استناداً إلى معلومات مصدر هذه التطبيقات. وللوظائف SASF وجهان يتصلان بمصدر تطبيقات الوسائط المتعددة IP؛ أحدهما ترشيح المصدر باتباع سياسة مكافحة الاقتحام التي توفرها الوظيفة CASF، والآخر استيقان المرسل.

– سياسة مكافحة الاقتحام

تحدد الوظيفة SASF هوية الاقتحام وتستبعده بالترشيح باستعمال عنوان مصدر رزم بيانات الوسائط المتعددة IP. ولا يجري الترشيح عن طريق عنوان المصدر فحسب بل عن طريق معلومات بروتوكول أخرى متوفرة في الوظيفة SASF. ويبيّن الشكل 3 وظائف مكافحة الاقتحام والتفاعلات بين وظائف مكافحة اقتحام الوسائط المتعددة IP من خلال تحليل المصدر في الوظيفة SASF.

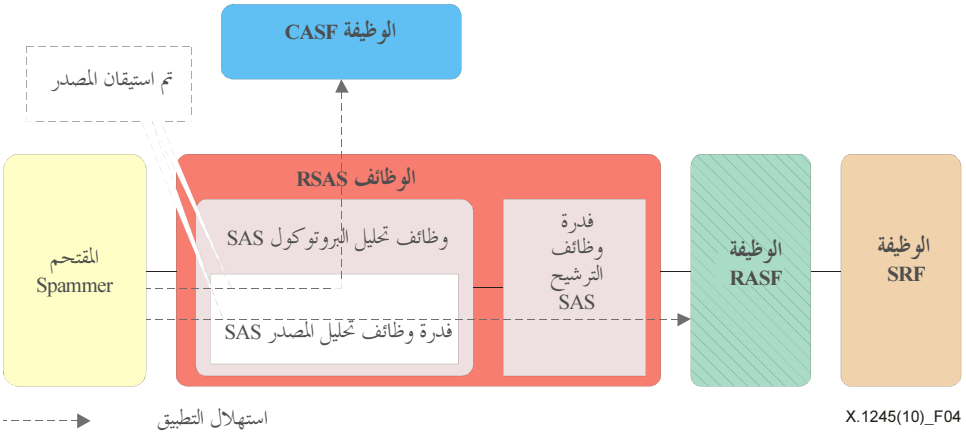


الشكل 3 – مكافحة اقتحام الوسائط المتعددة IP من خلال تحليل المصدر في الوظائف SASF

تستطيع فدرة وظائف الترشيح SAS أن تحصل على سياسة مكافحة الاقتحام من وظائف السياسات CAS، وتقوم فدرة وظائف الترشيح SAS بترشيح الرزم IP التي يرسلها المقتحم عندما يتم تحديدها بأنها اقتحاماً، وذلك استناداً إلى نتائج التحليل.

– استيقان المرسل

تزوّد الوظائف SASSF بمعلومات استيقان المرسلين، ويمكنها أن تقوم باستيقان مستعمل الحركة المرسلة. ويجوز للوظيفة SASF أن تمنع الكيانات غير المرخّص لها من استعمال تطبيقات الوسائط المتعددة IP حسب الاقتضاء.



الشكل 4 – استيقان المصدر في الوظائف SASF

يبين الشكل 4 نظام استيقان المصدر في الوظائف SASF. وقدرة تحليل المصدر في الوظائف SASF مزوّدة بوظيفة استيقان قادرة على استيقان حركة المقتحم قبل إرسالها إلى الوظيفة CASF أو RASF (ووظائف مكافحة الاقتحام جهة المتلقي). وتستبعد الوظيفة SASF الحركة التي تخفق في الاستيقان، إن اقتضت الحاجة. ولا يمكن إرسال سوى الحركة المستيقنة إلى الوظائف ASF الأخرى. ويساعد استبعاد الحركة غير المستيقنة على الحيلولة دون وصول المقتحمين الذين يحاولون انتحال الهويات.

– إجراء الترشيح

يتم إجراء الترشيح في الوظيفة SASF لاقتحام الوسائط المتعددة IP من خلال تحليل المصدر على النحو التالي:

1) إرسال سياسة مكافحة الاقتحام: تتلقى الوظيفة SASF سياسة مكافحة الاقتحام من الوظيفة CASF. ويمكن إرسال سياسة مكافحة الاقتحام إلى الوظيفة SASF على شكل تبليغ أو بطريقة الطلب/الرد.

2) استقبال تطبيقات الوسائط المتعددة IP: تستقبل الوظيفة SASF طلب البدء في تطبيقات الوسائط المتعددة IP.

3) استيقان المصدر: تستيقن الوظيفة SASF مصدر التطبيقات. وإذا أخفقت عملية الاستيقان رفضت الوظيفة SASF طلب البدء الوارد من المقتحم.

4) تعرف الاقتحام وترشيحه: تقرر الوظيفة SASF بشأن تطبيق الوسائط المتعددة IP المستقبِل استناداً إلى سياسة مكافحة الاقتحام المستقبلة من الوظيفة CASF ومصدر الطلب. وترفض الوظيفة SASF الحركة التي تتحدد كاقتحام أو تهملها.

ii) وظائف تحليل خصائص الاقتحام SAS

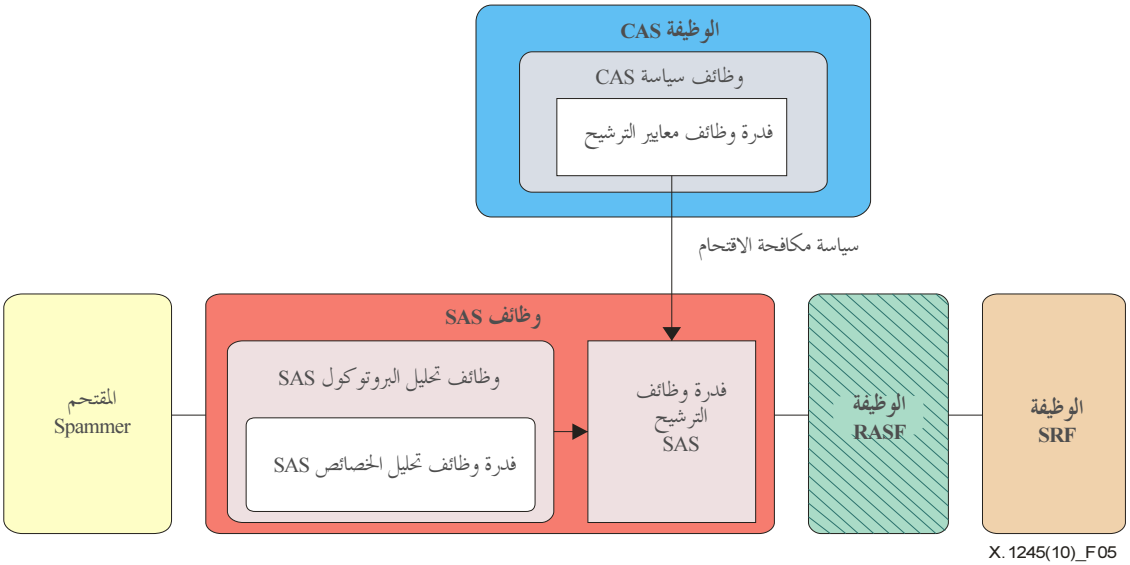
تستطيع الوظيفة SASF أن تميّز الاقتحام باستعمال خصائص التطبيقات مثل الخدمة بالجملة. ويمكن للوظيفة SASF أن تستعمل قيمة عتبة للتحقق من الإرسال بالجملة. وتضم وظائف تحليل الخصائص SAS عدة فدر وظيفية لتحليل الخصائص المميزة. أما وظيفة كل فدرة وظيفية وسطحها البيني فيشكل كل منهما وسيلة تقنية خاصة لمكافحة اقتحام الوسائط المتعددة IP، ولا يدخلان في مجال تطبيق هذه التوصية. وفيما يلي قوائم ببعض أمثلة الخصائص التي يمكن أن ترصدها الوظيفة SASF من أجل تطبيق طريقة مكافحة الاقتحام.

– الإرسال بالجملة

تتمتع وظائف تحليل الخصائص SAS بالقدرة على تحليل مقدار طلب الخدمة من مصدر واحد وتحليل معدّل طلب الخدمة. وتحدد فدرة وظائف الترشيح SAS هوية اقتحام الوسائط المتعددة IP استناداً إلى نتائج تحليل الخصائص SAS وإلى سياسة مكافحة الاقتحام التي وردت من فدرة وظائف معايير الترشيح CAS.

– التفاعلية المحدودة

تتمتع الوظيفة SASF بالقدرة على اختبار تفاعلية خدمة المقتحم، على الرغم من أن اختبار تفاعلية مصدر تطبيقات الوسائط المتعددة IP تقوم به عادة الوظيفة CASF. وينزع المقتحمون إلى استعمال الآلات في بدء تطبيقات الوسائط المتعددة IP، ذلك لأن تكاليفها أقل من تكاليف الموارد البشرية. لذلك، فإن اختبار التفاعلية يعد إحدى طرائق التحقق من اقتحام الوسائط المتعددة IP.



الشكل 5 – مكافحة اقتحام الوسائط المتعددة IP بتحليل الخصائص في الوظيفة SASF

وفيما يلي كيفية إجراء ترشيح اقتحام الوسائط المتعددة IP من خلال تحليل الخصائص في الوظيفة SASF:

1) إرسال سياسة مكافحة الاقتحام: تتلقى فدرة وظائف الترشيح SAS سياسة مكافحة الاقتحام بشأن تحليل الخصائص المرسلة من الوظيفة CASF. ويمكن إرسال سياسة مكافحة الاقتحام إلى الوظيفة SASF على شكل تبليغ أو بطريقة الطلب/الرد.

2) استقبال تطبيقات الوسائط المتعددة IP: تستقبل الوظيفة SASF طلب البدء في تطبيقات الوسائط المتعددة IP.

3) تحليل الخصائص: تستخرج وظائف تحليل الخصائص SAS الخصائص المتعلقة بالاقتحام في تطبيقات الوسائط المتعددة IP المستقبَلة.

4) معالجة النتائج: ترسل نتائج تحليل الخصائص من وظائف تحليل الخصائص SAS إلى فدرة وظائف الترشيح SAS.

5) ترشيح الاقتحام: تعالج فدرة وظائف الترشيح SAS الاقتحام وفقاً لسياسة مكافحة الاقتحام. وإذا أفضت النتيجة عن أن الاتصال اقتحام، ترفض الوظيفة SASF الحركة المحددة كاقتحام للوسائط المتعددة IP أو تهملها.

وترتبط سياسة إدارة اقتحام الوسائط المتعددة IP بمورّدي الخدمة ومستعملي الخدمة وتطبيقات الوسائط المتعددة IP واللوائح الوطنية وما إلى غير ذلك. لذا ينبغي أن تتفاعل الوظيفتان SASF وRASF مع الوظيفة CASF من أجل الحصول على معلومات عن سياسة مكافحة الاقتحام لمكافحته استناداً إلى خصائص تطبيق الوسائط المتعددة IP.

3.7 الوظائف RAS

RASF هي مجموعة وظائف يتمثل دورها في تعرّف اقتحام الوسائط المتعددة IP المفترض تسليمها إلى متلقي الاقتحام ومنع هذا التسليم. ويمكن تطبيق الوظائف RASF في عناصر الشبكة مثل مخدّم الوكيل، حيث ترسل طلبات الاتصال الداخلة إلى متلقي الاقتحام في مرحلتها الأخيرة. وتتفاعل الوظائف RASF مع الوظائف CASF لتنفيذ وظائف مكافحة الاقتحام في المجموعة RASF.

ويمكن استخدام الوظائف CASF وRASF في تجهيزات نفس الشبكة التي تشمل المقتحمين ومتلقي الاقتحامات في الوقت ذاته. غير أن وظائف مكافحة الاقتحام التي تعمل في التجهيزات تختلف باختلاف تدفق الحركة. وبصيغة أخرى، فإن وظائف مكافحة الاقتحام في التجهيزات تعمل كوظيفة SASF عندما تكون الحركة واردة من مستعملي تطبيقات الوسائط المتعددة IP الذين تشملهم التجهيزات. وتعمل كوظيفة RASF عندما تكون الحركة ذاهبة إلى مستعملي تطبيقات الوسائط المتعددة IP الذين تشملهم التجهيزات.

وتتألف المجموعة RASF من وظائف تحليل البروتوكول RAS وفدرة وظائف الترشيح RAS لمراقبة ترشيح الاقتحامات.

وعلى الرغم من تمكّن الوظيفتين SASF وRASF تقنياً من تحليل محتوى الحركة المرسَلة لمكافحة الاقتحام، فإنهما غير متناولتين من خلال وظائف تحليل المحتوى الواردة في هذه التوصية، لأن هذا الأمر يستوجب فرض قيود إضافية على معالجتهما. فعندما لا يمر تطبيق الوسائط المتعددة IP عبر الوظيفة CASF بالتغيّب، يجوز للوظيفة RASF أن تسلم التطبيق المذكور إلى الوظيفة CASF وتطلب منها تحليل محتواه لأغراض تعرّف الاقتحام.

وتصف الفقرات التالية تقنيات مختلفة من شأن الوظيفة RASF أن تعتمدها من أجل مكافحة اقتحام الوسائط المتعددة IP.

1.3.7 فدرة وظائف الترشيح RAS

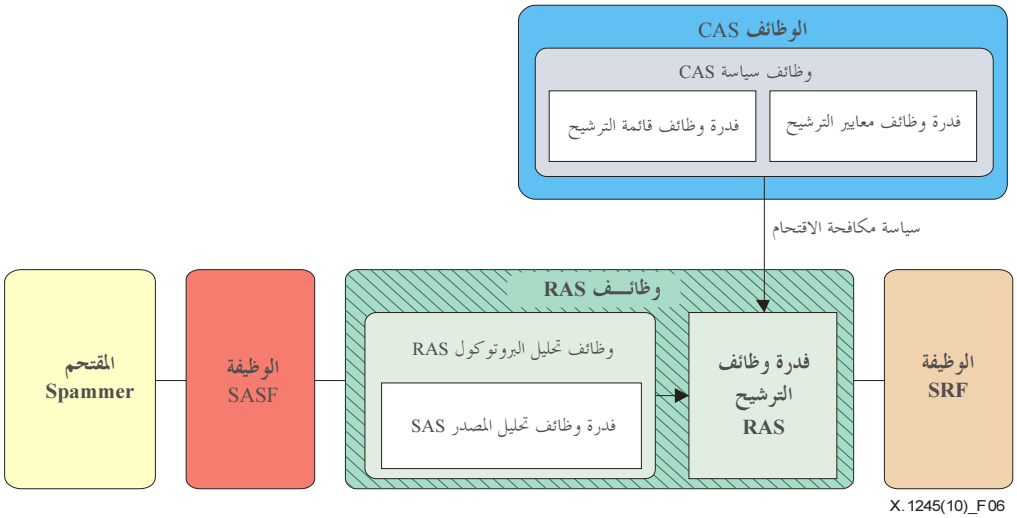
تحدد فدرة وظائف الترشيح RAS ما إذا كان تطبيق الوسائط المتعددة IP اقتحاماً أم لا، وذلك استناداً إلى نتيجة تحليل سياسة مكافحة الاقتحام. لذا تتفاعل هذه الفدرة مع الوظائف CASF وغيرها من وظائف مكافحة الاقتحام أو الفِدر الوظيفية الموجودة في المجموعة RASF.

2.3.7 وظائف تحليل البروتوكول RAS

تحلل وظائف تحليل البروتوكول RAS معلومات بروتوكول تطبيقات الوسائط المتعددة IP المستقبَلة. وتتألف من فدرة وظائف تحليل المصدر RAS ووظائف تحليل الخصائص RAS التي تحلل معلومات مصدر تطبيقات الوسائط المتعددة IP المستقبَلة وخصائصها على التوالي.

i) فدرة وظائف تحليل المصدر RAS

تستطيع الوظائف RASF التمييز بين الاقتحام وعدم الاقتحام لتطبيقات الوسائط المتعددة IP استناداً إلى المعلومات عن مصدر هذه التطبيقات. وفيما يتعلق بتعرّف الاقتحام، تحدد الوظائف RASF خصائص سياسات مكافحة الاقتحام المتصلة بالمصدر المتوفر في الوظيفة CASF من قبيل القائمة السوداء والقائمة البيضاء وعلامة السمعة وغيرها. ويقدم الشكل 6 وظائف مكافحة الاقتحام وتفاعلات الوظائف لمكافحة اقتحام الوسائط المتعددة IP من خلال تحليل المصدر.



الشكل 6 – مكافحة اقتحام الوسائط المتعددة IP استناداً إلى تحليل المصدر

تحدد الوظيفة RASF ما إذا كان تطبيق الوسائط المتعددة IP اقتحاماً أم لا، وذلك استناداً إلى المعلومات عن مصدر التطبيق المذكور، وتعالجه تبعاً للنتيجة. ونظراً لضرورة أن تكون معلومات المصدر موثوقة بدرجة فائقة من أجل ضمان فعالية تقنية مكافحة الاقتحام القائمة على المصدر، يُفترض أن يكون تطبيق الوسائط المتعددة IP الذي تستقبله الوظيفة RASF من الوظيفة SASF جديراً بالثقة أي مستيقناً. وتحدد الوظيفة RASF هوية اقتحام الوسائط المتعددة IP طبقاً لمعايير ترشيح الاقتحام أو قائمة ترشيح الاقتحام المتوفرة في الوظيفة CASF. وتحتفظ الوظيفة CASF بقائمة الترشيح ومعايير الترشيح من أجل دعم الوظيفة RASF أو SASF أو الوظيفة CASF ذاتها لتعرف الاقتحام. وفيما يلي عمليات تحديد هوية الاقتحام وترشيحه في الوظيفة RASF باستعمال طريقة تحليل المصدر؛

1) إرسال سياسة مكافحة الاقتحام من الوظيفة CASF: تستقبل الوظيفة RASF سياسة مكافحة الاقتحام من الوظيفة CASF. ويمكن إرسال سياسة مكافحة الاقتحام إلى الوظائف RASF على شكل تبليغ أو بطريقة الطلب/الرد.

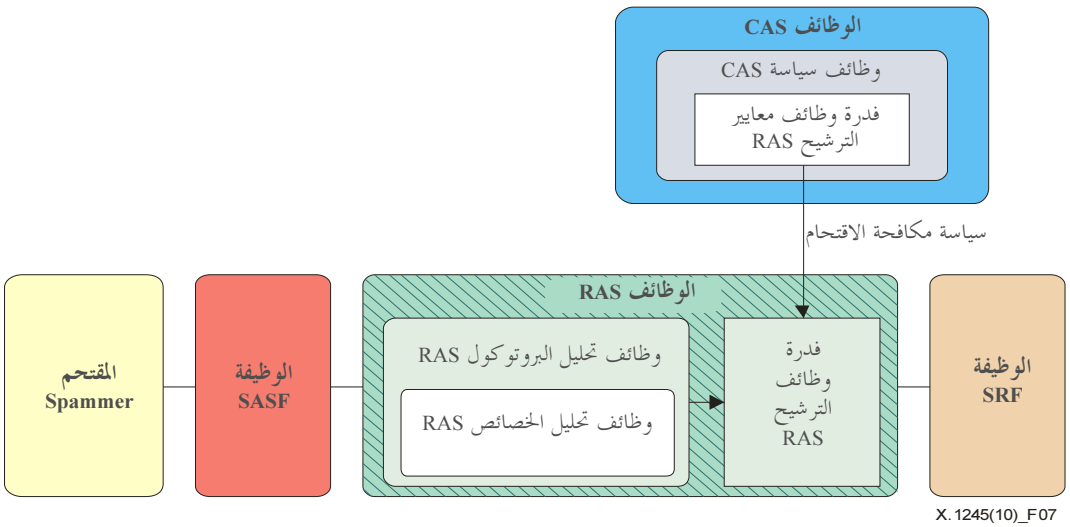
2) استقبال تطبيقات الوسائط المتعددة: تستقبل الوظيفة RASF تطبيق الوسائط المتعددة IP وتتحقق من مصدره.

3) تعرف الاقتحام وترشيحه: تقرر الوظيفة RASF بشأن تطبيق الوسائط المتعددة IP المستقبَل استناداً إلى معلومات المصدر وإلى سياسة إدارة مكافحة الاقتحام التي تلقتها في المرحلة السابقة. وترفض الوظيفة RASF الحركة المحددة بأنها اقتحام للوسائط المتعددة IP أو تهملها تبعاً لسياسة مكافحة الاقتحام التي يتبعها مورّد الخدمة أو مستعملوها.

عندما تحدد الوظيفة RASF هوية اقتحام استناداً إلى قائمة سوداء أو بيضاء يمكن استعمال قائمة الترشيح التي تلقتها من الوظيفة CASF. وعندما تحدد الوظيفة RASF هوية الاقتحام استناداً إلى علامة السمعة، يمكن استعمال معايير الترشيح مثل علامة العتبة للسمعة التي يتحدد عندها تطبيق وسائط متعددة IP بأنه اقتحام.

ii) وظائف تحليل الخصائص RAS

يمكن للوظيفة RASF أن تحدد الاقتحام من خلال استعمال تطبيق الوسائط المتعددة IP للتحقق مما إذا كان الاقتحام يتميز بخصائص اقتحام الوسائط المتعددة IP من عدمه. وتضم وظائف تحليل الخصائص RAS عدة فدر وظيفية خاصة لتحليل الخصائص. ولا تدخل الوسائل التقنية لمكافحة اقتحام الوسائط المتعددة IP في مجال تطبيق هذه التوصية.



الشكل 7 – مكافحة اقتحام الوسائط المتعددة IP استناداً إلى تحليل الخصائص

يبيّن الشكل 7 وظائف مكافحة الاقتحام والتفاعلات بين وظائف مكافحة اقتحام الوسائط المتعددة IP من خلال تحليل الخصائص في الوظيفة RASF. وفيما يلي كيفية إجراء تحديد الوظيفة RASF لهوية اقتحام الوسائط المتعددة IP من خلال تحليل الخصائص؛

1) إرسال سياسة مكافحة الاقتحام: تتلقى فدرة وظائف الترشيح RAS سياسة مكافحة الاقتحام القائمة على أساس تحليل الخصائص من الوظيفة CASF. ويمكن إرسال سياسة مكافحة الاقتحام إلى الوظيفة RASF على شكل تبليغ أو بطريقة الطلب/الرد.

2) استقبال تطبيقات الوسائط المتعددة IP: تستقبل الوظيفة RASF إشارة بدء تطبيقات الوسائط المتعددة IP.

3) تحليل الخصائص: تستخرج وظائف تحليل الخصائص RAS الخصائص المتصلة بالاقتحام في تطبيق الوسائط المتعددة IP.

4) معالجة النتائج: تزود وظائف تحليل الخصائص RAS فدرة وظائف الترشيح RAS بنتيجة التحليل.

5) ترشيح الاقتحام: تعالج فدرة وظائف الترشيح RAS الاقتحامات وفقاً لسياسة مكافحة الاقتحام. وإذا خَلُصت نتيجة التحليل إلى تحديد اقتحام، يمكن للوظيفة RASF أن ترفض الحركة المحددة بأنها اقتحام للوسائط المتعددة IP أو أن تهملها.

4.7 الوظائف CAS

تتمتع الوظيفة CASF بمقدرات إدارة سياسات مكافحة الاقتحام ومراقبة الوظيفتين PASF وSASF. كما لديها مقدرة تحليل مصدر تطبيقات الوسائط المتعددة IP أو خصائصها من أجل تحديد وجود اقتحام ومنعه عندما توجد على مسار الرزم IP بين المقتحمين ومتلقّي الاقتحام لتزويد تطبيقات الوسائط المتعددة IP تبعاً لنمط هذه التطبيقات. وتتمتع الوظيفة CASF بوظائف تحليل البروتوكول CAS ووظائف تحليل المحتوى CAS وفدرة وظائف الترشيح CAS ووظائف سياسة مكافحة الاقتحام CAS وفدرة وظائف مراقبة الوظيفة ASF. ويرد في هذه الفقرة وصفاً لوظائف وتفاعلات كل كيان في الوظائف CASF من أجل مكافحة اقتحام الوسائط المتعددة IP.

1.4.7 فدرة وظائف الترشيح CAS

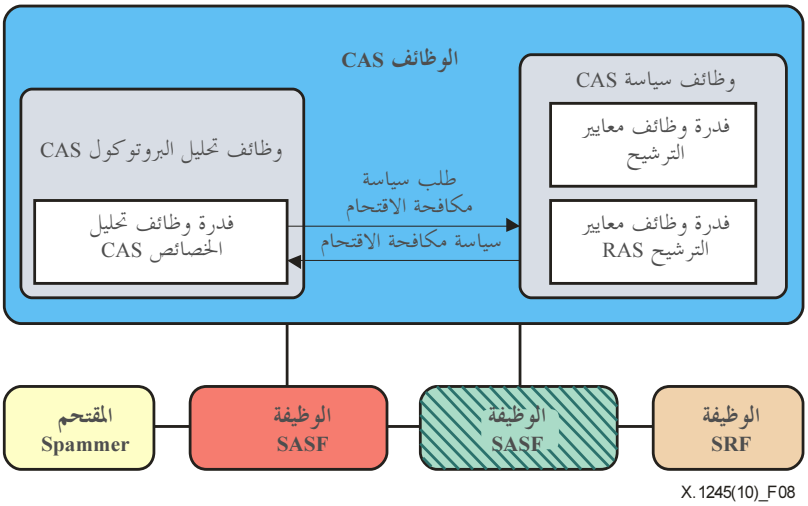
تحدد فدرة وظائف الترشيح CAS ما إذا كان تطبيق الوسائط المتعددة IP الخاضع للتحليل اقتحاماً أم لا، وذلك استناداً إلى نتائج التحليل وسياسة مكافحة الاقتحام. ولذلك تتفاعل هذه الفدرة مع وظائف أو فدر وظائف مكافحة الاقتحام الأخرى القائمة في الوظيفة CASF.

2.4.7 وظائف تحليل البروتوكول CAS

تحلل هذه الوظائف معلومات بروتوكول تطبيقات الوسائط المتعددة IP التي جرى استقبالها. وهي تتألف من فدرة وظيفية لتحليل المصدر CAS ووظيفة تحليل الخصائص CAS اللتين تحللان معلومات المصدر والخصائص في تطبيقات الوسائط المتعددة IP الواصلة على التوالي.

i) فدرة وظائف تحليل المصدر CAS

عندما يرد تطبيق وسائط متعددة IP تحت مراقبة مكوّنة الشبكة التي تضم الوظيفة CASF – مثال: عندما يصل مستعمل نفسه بخدمة مراسلة لحظية أو بخدمة مهاتفة عبر بروتوكول الإنترنت تحت مراقبة مخدّمات التطبيق – يمكن أن تكون الوظيفة CASF كياناً وظيفياً لتعرف الاقتحام من خلال تحليل المصدر. ويبين الشكل 8 وظائف مكافحة الاقتحام وتفاعلاتها مع وظائف مكافحة اقتحام الوسائط المتعددة IP من خلال تحليل المصدر في الوظيفة CASF.



الشكل 8 – مكافحة اقتحام الوسائط المتعددة IP استناداً إلى تحليل المصدر

وفيما يلي وصف لإجراء مكافحة اقتحام الوسائط المتعددة IP استناداً إلى معلومات مصدر تطبيق الوسائط المتعددة IP في الوظيفة CASF؛

1) الاستيقان: استيقان مستعمِل يرغب في استعمال تطبيق متعدد الوسائط IP (مثل خدمة مراسلة لحظية) وذلك من خلال مكوّنة من الشبكة مثل مخدّم تطبيقات مزوّد بوظيفة CASF.

2) استقبال تطبيقات وسائط متعددة IP: يرسل المستعمل طلب تسليم رسالة IP إلى الوظيفة CASF، وتتحقق فدرة وظائف تحليل المصدر CAS من مصدر المستعمِل.

3) الحصول على سياسة مكافحة الاقتحام: تطلب فدرة وظائف تحليل المصدر CAS سياسة مكافحة الاقتحام وتتلقاها من وظائف السياسة CAS.

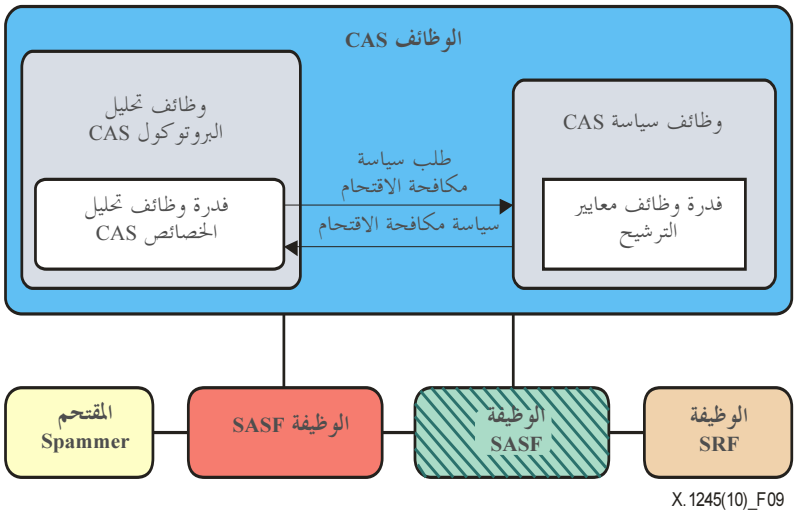
4) تعرف الاقتحام وترشيحه: تقرر الوظيفة CASF بشأن تطبيق الوسائط المتعددة IP المستقبَلة استناداً إلى معلومات المصدر وإلى سياسة مكافحة الاقتحام التي تلقتها في مراحل سابقة. وتستطيع الوظيفة CASF أن ترفض أو أن تهمل الحركة التي تحددت بأنها اقتحام وسائط متعددة IP، وأن تعالج هذه الحركة بعد ذلك وفقاً لسياسة مكافحة الاقتحام لمورد الخدمة أو مستعمِل الخدمة عندما تتحدد بأنها اقتحام.

ii) وظائف تحليل الخصائص CAS

يمكن أن تكون الوظيفة CASF نقطة تحليل خصائص لمحاربة الاقتحام عندما يصل تطبيق وسائط متعددة IP بمراقبة كيان من شبكة الوظيفة CASF. وتحلل الوظيفة CASF تطبيق وسائط متعددة IP لمعرفة ما إذا كان له خصائص الاقتحام وتستعمل معايير الترشيح الواردة في سياسة مكافحة الاقتحام من أجل تحديد ما إذا كان هذا التطبيق اقتحاماً أم لا. ويبيّن الشكل 9 المعمارية الإجمالية والسطوح البينية لطريقة تحليل الخصائص من أجل مكافحة اقتحام الوسائط المتعددة IP في الوظيفة CASF.

ووظائف السياسة CASF مزوّدة بفدرة وظيفية لمعايير الترشيح تضم معايير ترشيح الاقتحامات الضرورية لتحديد هوية اقتحام الوسائط المتعددة IP وإرسال المعايير إلى الوظيفة SASF أو RASF بغية دعمهما في تعرّف الاقتحام. مثال على ذلك، عندما تحاول وظائف تحليل الخصائص CAS تعرف الاقتحام في حالة إرسال تطبيق الوسائط المتعددة IP بالجملة، تقدم فدرة وظائف معايير الترشيح CASF معيار الكمية الذي يحدد مستوى كمية تطبيقات الوسائط المتعددة IP باعتباره اقتحاماً.

ويعرض الشكل 9 وظائف مكافحة الاقتحام وتفاعلاتها مع وظائف محاربة اقتحام الوسائط المتعددة IP من خلال تحليل الخصائص في الوظيفة CASF.



الشكل 9 – مكافحة اقتحام الوسائط المتعددة IP استناداً إلى تحليل الخصائص

وفيما يلي إجراءات تحليل الخصائص لمكافحة اقتحام الوسائط المتعددة IP في الوظيفة CASF.

1) تحليل خصائص الاقتحام: عندما يشرع تطبيق وسائط متعددة IP بمحاولة التوصيل بمراقبة كيان الشبكة الذي ترتبط به الوظيفة CASF، تبدأ هذه الوظيفة بتحليله لمعرفة ما إذا كان له خصائص الاقتحام مثل الإرسال بالجملة أو التفاعلية المحدودة وغيرهما.

2) الحصول على سياسة مكافحة الاقتحام: تطلب وظائف تحليل الخصائص وظائف السياسة CAS لمكافحة الاقتحام المتعلقة بتحليل الخصائص وذلك من أجل ترشيح الاقتحام. وترسل فدرة سياسة مكافحة الاقتحام المعلومات المطلوبة إلى وظائف تحليل الخصائص CAS.

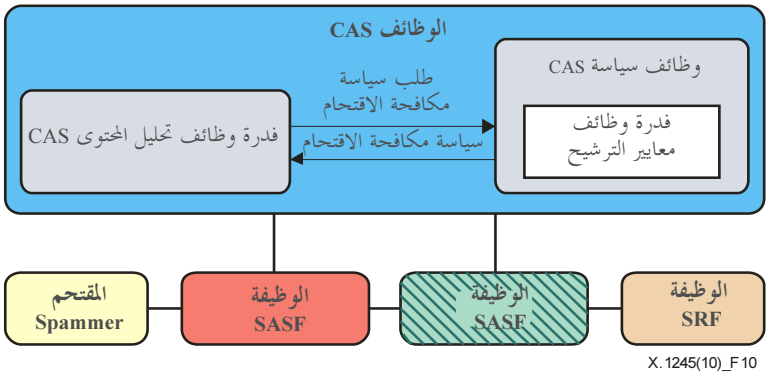
3) تعرف الاقتحام وترشيحه: تحدد وظائف تحليل الخصائص CAS ما إذا كان تطبيق الوسائط المتعددة IP اقتحاماً أم لا، استناداً إلى نتيجة تحليل وظائف تحليل الخصائص وإلى سياسة مكافحة الاقتحام التي استلمتها سابقاً.

3.4.7 وظائف تحليل المحتوى CAS

يتمتع الكيان CASF بوظائف تحليل المحتوى CAS وتحلل هذه الوظائف محتوى تطبيق متعدد الوسائط IP بهدف رصد الاقتحام عندما يرسل التطبيق إلى المتلقي عبر تجهيزات الشبكة التي تضم الكيان CASF مثل مخدّم التطبيق أو مخدّم الوسائط.

وتعريف الاقتحام باستعمال معلومات بروتوكول تطبيقات الوسائط المتعددة IP، مثل معلومات المصدر أو خصائص الاقتحام، يمكن أن يقوم بالتحليل فيه أي وظيفة CASF أو SASF أو RASF. ومن جهة أخرى، ففي تعريف الاقتحام باستعمال تحليل المحتوى، تكون الوظيفة CASF التي يمرّ عبرها محتوى تطبيقات الوسائط المتعددة IP هي الكيان الوظيفي المسؤول عن تحليل المحتوى عند استعمال تقنيات مكافحة الاقتحام القائمة على المحتوى من أجل مكافحة اقتحام الوسائط المتعددة IP.

ويعرض الشكل 10 وظائف مكافحة الاقتحام وتفاعلاتها مع وظائف مكافحة اقتحام الوسائط المتعددة IP من خلال تحليل المحتوى في الوظيفة CASF.



الشكل 10 – مكافحة اقتحام الوسائط المتعددة IP استناداً إلى تحليل المحتوى

وفيما يلي إجراءات تحليل المحتوى لمكافحة اقتحام الوسائط المتعددة IP في الكيان CASF:

1) استقبال تطبيقات الوسائط المتعددة IP: يصل محتوى تطبيق الوسائط المتعددة IP إلى الوظائف CASF.

2) تحليل المحتوى: تحلل وظائف التحليل CAS محتوى التطبيق IP.

3) الحصول على سياسة مكافحة الاقتحام: تطلب الوظيفة CASF وظائف السياسة CAS الخاصة بسياسة مكافحة الاقتحام، وتستلم السياسة من فدرة وظائف معايير الترشيح.

4) تعرف الاقتحام وترشيحه: تقرر الوظائف CASF ما إذا كان تطبيق الوسائط المتعددة IP اقتحاماً أم لا، وذلك استناداً إلى نتيجة التحليل وإلى سياسة مكافحة الاقتحام.

وكما ورد في الفقرة 6 قد تكون قابلية تطبيق طريقة تحليل المحتوى محدودة تبعاً لخصائص تطبيق الوسائط المتعددة القائمة على بروتوكول الإنترنت، مثل، ما إذا كانت تطبيقات الوسائط المتعددة IP في الوقت الفعلي أم لا؟ وما إذا كانت متعددة الوسائط أم لا: وما إذا كان محتوى تطبيقات الوسائط المتعددة IP مجفراً أم لا؟

4.4.7 وظائف السياسة CAS

تضم وظائف السياسة CAS السياسات المضادة للاقتحام لأغراض مكافحة اقتحام الوسائط المتعددة IP وتتألف من فدرة وظائف معايير الترشيح وفدرة وظائف قائمة الترشيح.

i) فدرة وظائف معايير الترشيح

تضم فدرة وظائف معايير الترشيح معايير الترشيح المضادة للاقتحام من أجل تعرّف اقتحام الوسائط المتعددة IP. وقد توجد أنواع مختلفة من معايير الترشيح تبعاً لتقنيات مكافحة الاقتحام المستخدمة. فمثلاً عند تحليل الإرسال بالجملة يمكن أن تكون عتبة كمية تطبيقات الوسائط المتعددة IP التي أرسلت في نفس الوقت من نفس المصدر معياراً للترشيح. أما آليات وضع معايير الترشيح وإدارتها، فإنها تقع خارج مجال تطبيق هذه التوصية.

ii) فدرة وظائف قوائم الترشيح

تقوم فدرة وظائف قوائم الترشيح بإدارة قوائم الترشيح سعياً لتعرّف اقتحام الوسائط المتعددة IP استناداً إلى تحليل المصدر. وقد توجد أنواع مختلفة من قوائم ترشيح الاقتحام تبعاً لتقنيات مكافحة الاقتحام المستخدمة. فمثلاً، يمكن استعمال القائمة السوداء والقائمة البيضاء، ودرجة السمعة كقوائم ترشيح. وقد تكون قائمة الترشيح إما قائمة عمومية للعديد من مستعملي الخدمة المتماثلين، وهي قائمة شخصية تُدار شخصياً أو مزيجاً من النوعين. أما آليات إنشاء قائمة الترشيح وإدارتها فلا تدخل في مجال تطبيق هذه التوصية.

5.4.7 فدرة وظائف المراقبة ASF

تتفاعل فدرة وظائف المراقبة ASF مع الوظائف SASF وRASF لدعمها في عملية تعرف الاقتحام وترشيحه. وهي ترسل السياسات المضادة للاقتحام من وظائف السياسة CAS إلى RASF وSASF.

5.7 الوظائف SR

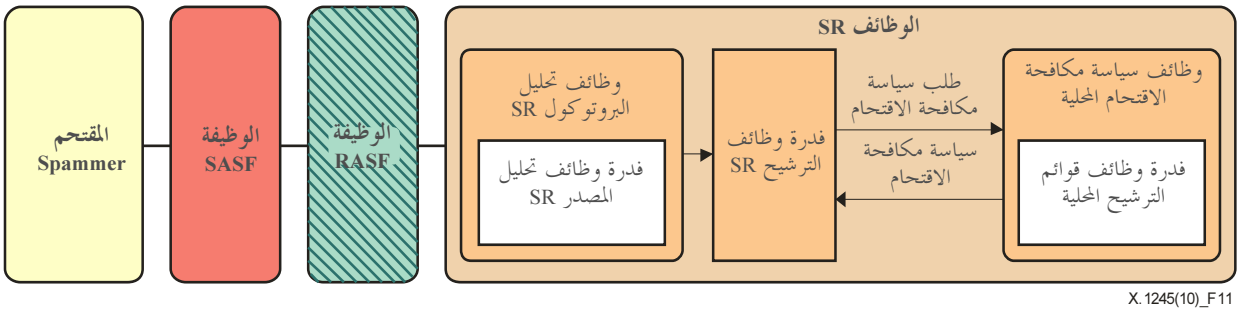
متلقي الاقتحام (SR) هو النقطة النهائية لاقتحام الوسائط المتعددة IP. وقد يتأثر المستعملون ويتكبّدون الخسائر جراء اقتحام الوسائط المتعددة IP إن لم توجد آلية لمكافحة الاقتحام.

ومتلقي الاقتحام مزوّد بوظائف SR لحماية نفسه من اقتحام الوسائط المتعددة IP. ويستطيع المستعملون اقتناء سياسة مكافحة اقتحام أو الحصول عليها من مزوّدي الخدمة بغية ترشيح اقتحامات الوسائط المتعددة IP. وتتألف الوظائف SR من وظائف تحليل البروتوكول SR ووظائف تحليل المحتوى SR وفدرة وظائف الترشيح SR ووظائف سياسة مكافحة الاقتحام المحلية. وتصف هذه الفقرة وظائف وتفاعلات كل وظيفة مكافحة اقتحام يمكن اعتمادها من قِبل متلقي الاقتحام لمكافحة الاقتحام.

1.5.7 وظائف تحليل البروتوكول SR

تزوّد وظائف تحليل البروتوكول SR بفدرة وظائف تحليل المصدر SR القادرة على تعرّف الاقتحام استناداً إلى معلومات المرسل. وعلى الرغم من إمكانية ترشيح الاقتحام في الوظائف CASF وSASF وRASF في حالة التوصيل المباشر لتطبيقات الوسائط المتعددة IP، يمكن أيضاً استخدام الوظائف المضادة للاقتحام وسياسة مكافحة الاقتحام في الكيان SRF من أجل مكافحة اقتحام الوسائط المتعددة IP.

وبإمكان متلقي الاقتحام أن يحدد قائمة ترشيح محلية ومعايير ترشيح محلية أو أن يتلقى القائمة من وظائف مكافحة الاقتحام الأخرى مثل CASF. ولا تدخل الآليات الخاصة بتحديد سياسة مكافحة الاقتحام في مجال تطبيق هذه التوصية. ويعرض الشكل 11 وظائف مكافحة الاقتحام وتفاعلاتها بين الوظائف لمكافحة اقتحام الوسائط المتعددة IP من خلال تحليل المصدر في الوظيفة SRF.



الشكل 11 – مكافحة اقتحام الوسائط المتعددة IP من خلال تحليل المصدر في وظيفة متلقي الاقتحام

فيما يلي وصف لإجراء ممكن لمكافحة اقتحام وسائط متعددة IP استناداً إلى معلومات مصدر تطبيق الوسائط المتعددة IP في كيان متلقي اقتحام:

1) استقبال تطبيقات وسائط متعددة IP: تستقبل الوظيفة SRF إشارة بدء تطبيقات الوسائط المتعددة IP وتتحقق من مصدر التطبيق IP.

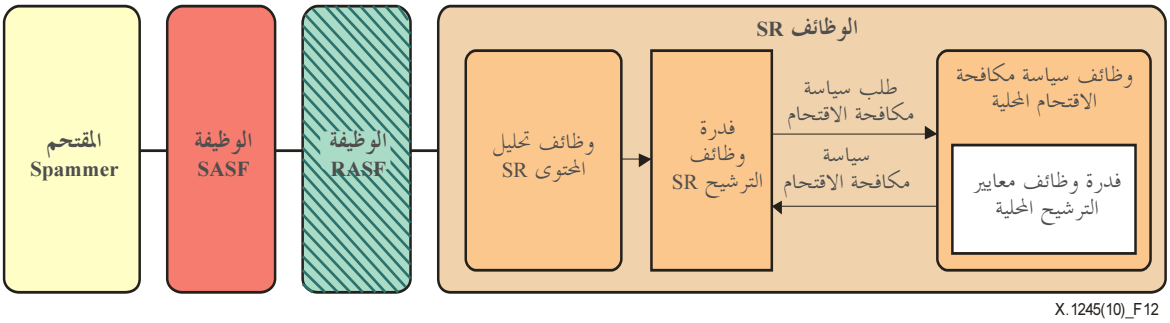
2) الحصول على سياسة مكافحة الاقتحام: تطلب وظائف تحليل البروتوكول SR سياسة مكافحة اقتحام وتتلقاها من وظائف سياسة مكافحة الاقتحام المحلية.

3) تعرف الاقتحام وترشيحه: تقرر فدرة وظائف الترشيح SR بشأن تطبيق الوسائط المتعددة IP الواصل استناداً إلى سياسة مكافحة الاقتحام، وإلى نتيجة تحليل المصدر. وإذا تحددت بأن اقتحام وسائط متعددة IP، يستطيع متلقي الاقتحام أن يرفضها أو يتجاهلها.

وبإمكان وظائف متلقي الاقتحام تقنياً أن تميز الاقتحام باستعمال تحليل الخصائص. لكن وظائف تحليل البروتوكول SR غير مزوّدة بفدرة وظائف تحليل خصائص نظراً لخطورة اعتمادها على متلقي الاقتحام في تنفيذ وظائف محاربة اقتحام متطورة كالمتبع في طريقة تحليل الخصائص، إذ إن وظائف تحليل البروتوكول RS موجودة بتصرّف جماعات متنوعة جداً من المستعملين.

2.5.7 وظائف تحليل المحتوى SR

بإمكان متلقي الاقتحام أن يتصدى للاقتحام باستعمال تحليل المحتوى. وبإمكانه أن يحتفظ بآلياته لتحليل المحتوى التي قد تكون خاصة بالمستعمِل أو صادرة عن مورّدي الخدمة. وتوضع سياسة مكافحة الاقتحام بشأن تحليل المحتوى في وظائف سياسة مكافحة الاقتحام المحلية باعتبارها جزءاً من الفِدرة الوظيفية لمعايير الترشيح المحلية. ويعرض الشكل 12 وظائف مكافحة الاقتحام وتفاعلاتها بين الوظائف لمكافحة اقتحام الوسائط المتعددة IP من خلال تحليل المحتوى في الوظيفة SRF.



الشكل 12 – مكافحة اقتحام الوسائط المتعددة IP استناداً إلى تحليل المحتوى في كيان متلقي الاقتحام

وفيما يلي الإجراء الذي يستعمله متلقي الاقتحام لترشيح اقتحام الوسائط المتعددة IP باستعمال تحليل المحتوى.

1) استقبال تطبيقات متعددة الوسائط IP: تستقبل الوظيفة SRF إشارة بدء تطبيقات الوسائط المتعددة IP. وتنفذ وظائف تحليل المحتوى SR تحليل المحتوى من أجل تعرّف الاقتحام.

2) الحصول على سياسة مكافحة الاقتحام/ترسل نتيجة تحليل المحتوى إلى فدرة وظائف الترشيح SR التي تطلب وتستقبل سياسة مكافحة الاقتحام من وظائف سياسة مكافحة الاقتحام المحلية.

3) تعرف الاقتحام وترشيحه: تقرر فدرة وظائف الترشيح SR بشأن التطبيق IP الواصل استناداً إلى سياسة مكافحة الاقتحام وإلى نتيجة تحليل المحتوى. وبإمكان متلقي الاقتحام أن يرفض أو يتجاهل الحركة التي تتحدد بأنها اقتحام وسائط متعددة IP.

3.5.7 فدرة وظائف الترشيح SR

تحدد فدرة وظائف الترشيح SR ما إذا كان تطبيق الوسائط المتعددة IP موضوع التحليل اقتحاماً أم لا، وذلك استناداً إلى نتيجة التحليل وإلى سياسة مكافحة الاقتحام. لذلك فإنها تتفاعل مع الوظائف أو فِدر الوظائف الأخرى لمكافحة الاقتحام في الكيان SRF.

4.5.7 وظائف سياسة مكافحة الاقتحام المحلية

تحتفظ وظائف سياسة مكافحة الاقتحام المحلية بسياسات مكافحة الاقتحام الخاصة بالمستعمل لأغراض مكافحة اقتحام الوسائط المتعددة IP. وتتألف الوظائف من فدرة وظائف معايير الترشيح المحلية وفدرة وظائف قوائم الترشيح المحلية.

i) فدرة وظائف معايير الترشيح المحلية

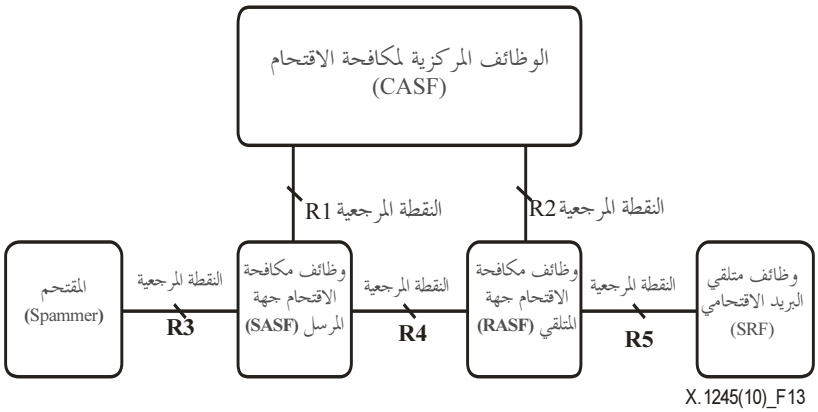
تحتفظ فدرة وظائف معايير الترشيح المحلية بمعايير ترشيح الاقتحام الخاصة بالمستعمِل من أجل تعرف اقتحام الوسائط المتعددة IP. وتعتمد أنواع معايير الترشيح على وظائف مكافحة الاقتحام التي تدعمها الوظيفة SRF.

ii) فدرة وظائف قوائم الترشيح المحلية

تدير فدرة وظائف قوائم الترشيح المحلية قائمة ترشيح خاصة بالمستعمِل لأغراض تعرف اقتحام الوسائط المتعددة IP استناداً إلى تحليل المصدر. وتعتمد أنواع القوائم على وظائف تحليل المصدر التي تدعمها الوظيفة SRF.

6.7 نقاط مرجعية في الإطار

تحدد هذه الفقرة النقاط المرجعية بين مختلف العناصر المكوّنة للإطار. ويبين الشكل 13 هذه النقاط.



الشكل 13 – النقاط المرجعية في إطار مكافحة الاقتحام

1.6.7 النقطة المرجعية R1

تقع R1 بين الوظيفتين CASF وSASF، وتستعمل للحصول على سياسة الترشيح من CASF وإرسالها إلى SASF. وتراقب الوظيفة CASF الوظيفة SASF عبر النقطة R1.

2.6.7 النقطة المرجعية R2

تقع R2 بين الوظيفتين CASF وRASF وتستعمل للحصول على سياسة الترشيح من CASF وإرسالها إلى RASF. وتراقب الوظيفة CASF الوظيفة RASF عبر النقطة R2.

3.6.7 النقطة المرجعية R3

تقع R3 بين المقتحمين وSASF وتستعمل في بروتوكول تطبيق الوسائط المتعددة IP و/أو في إرسال حركة البيانات.

4.6.7 النقطة المرجعية R4

تقع R4 بين SASF وRASF وتستعمل في بروتوكول تطبيق الوسائط المتعددة P و/أو في إرسال حركة البيانات.

5.6.7 النقطة المرجعية R5

تقع R5 بين الوظائف RASF ومقاصد الاقتحام، وتستعمل في بروتوكول تطبيق الوسائط المتعددة IP و/أو إرسال حركة البيانات.

التذييل I

مكافحة الاقتحام بفرض صعوبات على عمليات الاقتحام

(لا يشكل هذا التذييل جزءاً أساسياً من هذه التوصية)

يمكن أن يمثل فرض الصعوبات في وجه الاقتحام إحدى الطرائق التقنية لمكافحة اقتحام الوسائط المتعددة IP. غير أن هذه الطريقة تختلف بعض الشيء عن الطرائق الأخرى التي تعرف الاقتحام وترشحه مباشرة. ويساعد فرض صعوبات على الاقتحام على الحد من كمية الاقتحامات بصورة غير مباشرة، غير أن هذه الطريقة تحتاج إلى مجهود ووقت فضلاً عن أنها مكلفة. وهناك طريقة يمكنها تحقيق خفض كمية اقتحامات الوسائط المتعددة IP بزيادة صعوبات إرسال الاقتحامات، بالنسبة للمقتحمين، وذلك بزيادة التكلفة والجهود المطلوبة من أجل إعداد رسالة اقتحامية وإرسالها. وتتكون رسوم الاقتحام بالنسبة للمقتحمين من رسوم التنظيم، بما فيها رسوم العقوبة المتوقعة للاقتحام غير المشروع ورسوم استعمال تطبيقات الوسائط المتعددة IP التي تدفع إلى مورد الخدمة أو مورد الشبكة، ورسوم لتوزيع الاقتحامات، أي اختبار التفاعلية وغيرها. وفيما يلي الطرائق التي من شأنها زيادة الصعوبات في وجه عمليات الاقتحام:

- تعقيد الحصول على نفاذ إلى العناوين IP: زيادة الجهد المطلوب لجمع المعلومات عن أهداف إرسال الاقتحام، مثل العناوين IP وحسابات خدمة تطبيقات الوسائط المتعددة IP وزيادة صعوبة إرسال اقتحام وسائط متعددة IP على المقتحمين.
- نظام الدفع: فرض رسوم على اقتحام الوسائط المتعددة IP يساعد على الحدّ من كمية الاقتحامات. غير أن اعتماد نظام دفع لقاء احتمال الاقتحام، مثل الرسائل IP بالجملة، ليس حلا تقنياً.
- منع الإرسال بالجملة: نظراً لأن البريد الاقتحامي يرسل في العديد من الحالات بالجملة، فإن منع هذا النمط من الإرسال قد يساعد على خفض كمية الاقتحامات.
- اختبار التفاعلية: يمكن أن يزيد اختبار تفاعلية المقتحم من رسوم إرسال الاقتحام بالنسبة للمقتحمين. لكن ذلك قد يكون له تأثير سلبي، إذ إنه قد يسيء إلى مستعملي تطبيقات الوسائط المتعددة IP العاديين.

ولا تقتصر طرائق مكافحة الاقتحام من خلال فرض الصعوبات في وجه الاقتحام على الأمثلة آنفة الذكر.

ويمكن للوظيفة CASF في اختبار الفعالية أن تؤدي دور المختبر. ويمكن للوظائف CASF أو SASF أو RASF في طريقة منع الإرسال بالجملة، أن تكشف الإرسال بالجملة، أي تحدد مستوى الكمية وأن تمنع مرور تطبيقات الوسائط المتعددة IP ذات الإرسال بالجملة. وفرض رسوم على اتصالات أو رسائل الجملة بمراقبة الوظيفة CASF طريقة ممكنة أيضاً لزيادة الصعوبات في وجه الاقتحام.

وتحلل الوظيفتان SASF وRASF أحياناً معلومات البروتوكول لكنهما لا تتخذان عادة إجراءات إضافية لزيادة صعوبات الاقتحام مثل منع الإرسال بالجملة أو الدفع أو اختبار التفاعلية. وبإيجاز يتوقع أن تتخذ الوظيفة SASF أو RASF إجراءات لازمة لدعم الوظيفة CASF في معالجة الاقتحام وأن تؤدي الوظيفة CASF دوراً رئيسياً في زيادة الصعوبات أمام عمليات الاقتحام.

التذييل II

الأمن واعتبارات عملية في استعمال الإطار

(لا يشكل هذا التذييل جزءاً أساسياً من هذه التوصية)

1.II اعتبارات أمنية

فيما يلي بعض الاعتبارات الأمنية لمكافحة اقتحام الوسائط المتعددة IP.

– الاستيقان

الاستيقان عملية يؤكد فيها كيان ما، سواء كان متلقي اقتحام أم الوظيفة CASF، هويته بتقديم أوراق ثبوتية من الصعب لأيٍّ كان، باستثناء المستعمل الفعلي، أن يقدمها.

ومن الضروري استيقان المستعمل لتحديد مرسل رسائل تطبيقات الوسائط المتعددة IP التي تساعد على منع العديد من أنواع الاقتحامات الناجمة عن هجمات انتحال الهوية. وإذا لم يجر الاستيقان بصورة صحيحة يتعذر تتبّع مواقع المقتحمين، لأن المقتحمين قادرون على تزوير عناوين IP بالقيام بعمليات الانتحال.

ويمكن إجراء الاستيقان في طرق عديدة. وتطبّق بعض طرائق الاستيقان، مثل استيقان كلمة مرور واضحة، بسهولة، ولكنها تبقى عموماً ضئيلة الفعالية وبدائية. وهنالك طرائق استيقان أخرى مثل Secure Socket Layer (SSL) وIPSec وSecure Shell وKerberos وقد تكون أكثر تعقيداً، ويتطلّب استعمالها والمحافظة عليها مزيداً من الوقت، لكنها تقدم استيقاناً قوياً وموثوقاً.

وثمة تكنولوجيات ناشئة أخرى، مثل طرائق التوقيع المحفر، تعِد بحلول أفضل. ولكن الطريقة الأكثر انتشاراً من الطرائق المتوفرة حالياً تبقى الطريقة التقليدية إطار سياسة المرسل (SPF) وdomain keys.

– التحكم في النفاذ

التحكم في النفاذ هي وسيلة استخدام وإنفاذ سياسات الترخيص. وتمنح عملية التحكم في النفاذ لمستعمل ما التصريح بالقيام بإجراء ما في مقصد الاقتحام والوظائف ASF أو تمنعه من ذلك وفقاً لسياسة الأمن.

ويطبق التحكم في النفاذ عادة بعد إجراء الاستيقان. وهنالك عموماً صنفان للتحكم في النفاذ هما التحكم التمييزي في النفاذ (DAC) والتحكم غير التمييزي في النفاذ (NDAC). في التحكم DAC يحدد صاحب الغرض الجهات التي يجوز لها النفاذ إلى الغرض أو يحدد السياسات. وتصنّف سائر سياسات النفاذ التي لا تنتمي إلى الفئة DAC في الفئة NDAC. أما في التحكم NDAC، فالسياسات قواعد غير محددة تبعاً لرغبة المستعمل (على سبيل المثال التحكم الإلزامي في النفاذ (MAC) والتحكم في النفاذ القائم على الدور (RBAC) والتحكم في النفاذ القائم على الغرض (PBAC) والتحكم في النفاذ القائم على السجلات (HBAC) والتحكم في النفاذ القائم على قيود مؤقتة (TCAC) والتحكم في النفاذ القائم على قواعد (RuBAC)).

– السرية

السرية هي الآليات التي تضمن ألا يصل إلى الاتصالات الأمينة إلا المستعملون المرخّص لهم بذلك. وهنالك آليتان رئيسيتان لتوفير السرية فيما يتعلق بالمعلومات المرسلة إلكترونياً، هما: التجفير أو النقل عبر بنية تحتية أمينة، مثل شبكة افتراضية خاصة (IPN) أو وصلات مجفرة أخرى.

وIPSec هو البروتوكول المستعمل في معظم الشبكات VPN لإنشاء توصيل أمين عبر الإنترنت. والبروتوكول IPSec معيار مقبول على نطاق واسع للإرسال الأمين، ويتميّز بالمرونة وأقل تكلفة من طرائق تجفير أخرى. ويقدم البروتوكول IPSec تجفيراً منيعاً وتكاملية واستيقاناً، وهو مفيد تحديداً في المنظمات التي تحتاج إلى نقل البيانات عبر الإنترنت بصورة أمينة.

أما بروتوكول أنفاق الطبقة (L2TP) فهو بروتوكول أنفاق يستعمل في الشبكات VPN. وهو يغلف بروتوكول الطبقة في شبكة ما بالبروتوكول PPP لحماية تجفير الأرتال PPP ولتغليف البيانات داخل بروتوكول أنفاق ما.

– سلامة البيانات

تعني السلامة عدم تغير المعلومات عند نقلها بين مقصد الاقتحام والمقتحم. ومن دون حماية وافية يتمكن المقتحمون من الإساءة إلى متحدّي رسائل الوسائط المتعددة IP أو خلطها.

وعند استعمال ملخصات الرسائل الناتجة عن وظيفة التقطيع التجفيرية يمكن لإدارة النظام أن تكشف التغيّرات غير المسموح بها في الرسائل. كما يمكن مزج وظائف التقطيع مع طرائق تجفيرية عادية أخرى من أجل التحقق من مصدر البيانات. وعند إضافة خوارزميات التقطيع إلى التجفير تنتج ملخصات رسائل خاصة تعرف مصدر البيانات.

وعند استعمال التوقيع الرقمي لتوفير سلامة البيانات، قد يكون من الضروري الحصول على بنية تحتية للمفتاح العمومي (PKI) من أجل إدارة مفاتيح التجفير. وتحتفظ البنية التحتية PKI في ذاكرتها بمسار تخصيص مفاتيح التجفير العمومية وإلغائها للمستعملين وللمنظمات.

وفضلاً عن التوقيع الرقمي والبنية PKI، يمكن استعمال التجفير السري للحفاظ على سلامة البيانات. وتطبيق المفتاح السري أسهل من حيث إنه لا يستعمل إلا مفتاحاً واحداً فقط، ويجب أن يكون بحوزة كل من المرسل والمتلقي من أجل إعمال التجفير وفك التجفير. وأنظمة المفاتيح السرية منتشرة الاستعمال على نطاق واسع، لكنها مشوبة بصعوبات تتعلق بوظيفة توزيع المفاتيح السرية بطريقة أمينة.

– عدم الرفض

عدم الرفض طريقة لا يتمكن فيها مرسل رسالة أو مصدر معاملة من أن ينفي لاحقاً إرسال الرسالة أو المعاملة.

وتجري عملية عدم الرفض من خلال وثائق قانونية ملزمة والالتزام بآليات الأمن والعمليات الموثوقة التالية لإدارة المخدّمات: SSL وأذنة البروتوكول OTP للتحري–الاستجابة، والتقطيع الأمين وبيانات التدقيق.

وهنالك استعمال شائع لاستخدام طريقة عدم الرفض، وهو الاستفادة من التواقيع الرقمية التي يمكن اعتبارها إحدى أفضل الطرق البديلة لاستبدال التواقيع القديمة في معالجة البيانات الإلكترونية. ومن أجل إعمال التواقيع الرقمية ينبغي وجود طرف ثالث موثوق (TTP) أو بنية PKI. ويمكن أن توفر الوظيفة TTP أو PKI سلطة إصدار شهادات (CA) واحدة على الأقل لإصدار شهادات رقمية وقوائم رفض مصدقة (CRL) للتحقق من الشهادات الباطلة.

2.II اعتبارات عملية

من أهم الأهداف في هذا الإطار هو التأكد من الحد من الآثار السلبية على الأعمال التجارية قدر الإمكان. وينبغي توضيح أن الامتثال لتدابير مكافحة الاقتحام تؤدي إلى نتائج إيجابية بالنسبة للأفراد وللمنشآت.

وتقوم الاعتبارات العملية التالية على أساس عمليات المعالجة. وهي تعتبر بأنها إرشادات لاستخدام نظام مكافحة الاقتحام وتوفير مورّدين محتملين بأعلى قدر من المعلومات.

– توفير دقة عالية وأداء جيد
– إمكانية نشر النظام على نطاق الإنترنت
– إدراج النظام في أنظمة تطبيقات الوسائط المتعددة القائمة على بروتوكول الإنترنت

- إتاحة الاستخدام في قواعد متنوعة للمخدّم الزبون: UNIX أو Windows، أو إلى ما غير ذلك.
- ترشيح اقتحام الوسائط المتعددة IP الداخلي والخارجي على حد سواء.
- إتاحة المرونة للتمشي مع سياسات المنظمات وأفضلياتها
- إتاحة القدرة للمستعمِل على استحداث مراشيح فردية أو خاصة
- السماح للمستعملين النهائيين إدارة مصنفاتهم الخاصة لاقتحام التطبيقات IP ووضع مجموعة بسيطة للأفضليات
- إتاحة القدرة على إدارة وظيفة القائمة السوداء والقائمة البيضاء
- إتاحة القدرة على التزوّد بترشيح المحتوى بما في ذلك القدرة على إضافة ترشيح المحتوى جهة المخدم مع مستويات إدارة الرسوم ووصولاً إلى مستوى المستعمل.

ثبت المراجع

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

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

سلاسل التوصيات الصادرة عن قطاع تقييس الاتصالات

السلسلة A	تنظيم العمل في قطاع تقييس الاتصالات
السلسلة D	المبادئ العامة للتعريفة
السلسلة E	التشغيل العام للشبكة والخدمة الهاتفية وتشغيل الخدمات والعوامل البشرية
السلسلة F	خدمات الاتصالات غير الهاتفية
السلسلة G	أنظمة الإرسال ووسائطه والأنظمة والشبكات الرقمية
السلسلة H	الأنظمة السمعية المرئية والأنظمة متعددة الوسائط
السلسلة I	الشبكة الرقمية متكاملة الخدمات
السلسلة J	الشبكات الكبلية وإرسال إشارات تلفزيونية وبرامج صوتية وإشارات أخرى متعددة الوسائط
السلسلة K	الحماية من التداخلات
السلسلة L	إنشاء الكبلات وغيرها من عناصر المنشآت الخارجية وتركيبها وحمايتها
السلسلة M	إدارة الاتصالات بما في ذلك شبكة إدارة الاتصالات (TMN) وصيانة الشبكات
السلسلة N	الصيانة: الدارات الدولية لإرسال البرامج الإذاعية الصوتية والتلفزيونية
السلسلة O	مواصفات تجهيزات القياس
السلسلة P	المطاريف وطرائق التقييم الذاتية والموضوعية
السلسلة Q	التبديل والتشوير
السلسلة R	الإرسال البرقي
السلسلة S	التجهيزات المطرافية للخدمات البرقية
السلسلة T	المطاريف الخاصة بالخدمات التلماتية
السلسلة U	التبديل البرقي
السلسلة V	اتصالات البيانات على الشبكة الهاتفية
السلسلة X	**شبكات البيانات والاتصالات بين الأنظمة المفتوحة ومسائل الأمن**
السلسلة Y	البنية التحتية العالمية للمعلومات وملامح بروتوكول الإنترنت وشبكات الجيل التالي
السلسلة Z	اللغات والجوانب العامة للبرمجيات في أنظمة الاتصالات

طُبعت في سويسرا
جنيف، 2011