الاتحـــــــــاد الدولـــــــــي للاتصـــــــــالات

ITU-T X.1243

(2010/12)

قطـــاع تقييس الاتصـــالات
في الاتحاد الدولي للاتصالات

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

أمن الفضاء السيبراني – مكافحة الرسائل الاقتحامية

نظام بوابي تفاعلي لمكافحة البريد الاقتحامي

التوصيـــة ITU-T X.1243

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 الرسائل الاقتحامية	**X.1249–X.1230**
إدارة الهوية	X.1279–X.1250
تطبيقات وخدمات آمنة	
اتصالات الطوارئ	X.1309-X.1300
أمن شبكات المحاسيس واسعة الانتشار	X.1339–X.1310
تبادل معلومات الأمن السيبراني	
نظرة عامة على الأمن السيبراني	X.1519–X.1500
تبادل مواطن الضعف/الحالة	X.1539–X.1520
تبادل الأحداث/الأحداث العارضة/المعلومات الحدسية	X.1549–X.1540
تبادل السياسات	X.1559–X.1550
طلب المعلومات الحدسية والمعلومات الأخرى	X.1569–X.1560
تعرف الهوية والاكتشاف	X.1579–X.1570
التبادل المضمون	X.1589–X.1580

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

التوصيـــة ITU-T X.1243

نظام بوابي تفاعلي لمكافحة البريد الاقتحامي

ملخص

تحدد التوصية ITU-T X.1243 النظام البوابي التفاعلي لمكافحة البريد الاقتحامي باعتباره وسيلة تقنية لمكافحة البريد الاقتحامي بين الميادين. ويتيح النظام البوابي إمكانية التبليغ عن البريد الاقتحامي بين الميادين المختلفة ويمنع مروره من ميدان لآخر.

كما تضع هذه التوصية مواصفات معمارية النظام البوابي، وتصف الكيانات الأساسية لنظام البوابة وبروتوكولاته ووظائفه، وتوفر آليات كفيلة بكشف البريد الاقتحامي وتقاسم المعلومات وإجراءات خاصة في النظام البوابي لمكافحة البريد الاقتحامي.

التسلسل التاريخي

الصيغة	التوصية	تاريخ الموافقة	لجنة الدراسات
1.0	ITU-T X.1243	2010-12-17	17

تمهيـــد

الاتحاد الدولي للاتصالات وكالة متخصصة للأمم المتحدة في ميدان الاتصالات وتكنولوجيا 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).

ملاحظـــة

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

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

حقوق الملكية الفكرية

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

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

جـــدول المحتويـــات

الصفحة

1 مجال التطبيق 1
2 المراجع 1
3 التعاريف 1
1.3 المصطلحات المعرفة في وثائق أخرى 1
2.3 المصطلحات المعرفة في هذه التوصية 1
4 المختصرات 2
5 الاصطلاحات 3
6 المعمارية 3
1.6 الكيانات والوظائف في نظام مكافحة البريد الاقتحامي 3
2.6 التعرّف على البريد الاقتحامي 4
3.6 إجراءات مكافحة البريد الاقتحامي 4
4.6 اكتشاف البريد الاقتحامي 4
5.6 التبليغ عن البريد الاقتحامي باستعمال بروتوكول النظير لمكافحة الاقتحام 5
7 تقنيات الترشيح في مكافحة البريد الاقتحامي 5
1.7 اعتبارات محايدة تقنياً 5
2.7 التقنيات المتوفرة لمكافحة الاقتحام 6
8 عملية بروتوكول النظام النظير لمكافحة الاقتحام 9
1.8 اكتشاف النظير 9
2.8 إقامة علاقة النظير 10
3.8 تبادل رسائل مكافحة البريد الاقتحامي 10
4.8 تحرير النظير 10
9 تنفيذ نموذج أنظمة بوابية لمكافحة البريد الاقتحامي 10
1.9 النموذج المدمج 10
2.9 النموذج القائم على أساس الميدان 11
3.9 نموذج النشر بالتحويل 12
البيبليوغرافيا 15

نظام بوابي تفاعلي لمكافحة البريد الاقتحامي

1 مجال التطبيق

النظام البوابي التفاعلي لمكافحة البريد الاقتحامي هو آلية تفاعلية عامة لمكافحة مختلف الرسائل الاقتحامية بين الميادين، بما فيها البريد الإلكتروني الاقتحامي والرسائل القصيرة الاقتحامية وغيرها، وهي تقاسم المعلومات من أجل مكافحة البريد الاقتحامي بين ميادين مختلفة، ولمنع إرسال هذا البريد واستقباله على حدٍ سواء. وتقدم هذه التوصية أنواعاً متعددة لتقنيات الترشيح من البريد الاقتحامي وتوفر المرونة اللازمة للتقنيات القادمة.

ينبغي قبل اعتماد تطبيق هذه التوصية مراعاة الامتثال للقوانين واللوائح الوطنية ذات الصلة.

2 المراجع

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

[ITU-T X.509] التوصية ITU-T X.509 (2000) | ISO/IEC 9594-8:2001، *Information technology – Open Systems Interconnection – The Directory: Public-key and attribute certificate frameworks.*

3 التعاريف

1.3 المصطلحات المعرفة في وثائق أخرى

تستعمل هذه التوصية المصطلحات التالية المعرفة في وثائق 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. ويتطور معنى الكلمة ويتسع خصوصاً مع تطور أنواع التكنولوجيا وتوفيرها فرصاً جديدة لإساءة استخدام الاتصالات الإلكترونية. وعلى الرغم من عدم وجود أي تعريف متفق عليه عالمياً 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 المعرفة في هذه التوصية

تعرف هذه التوصية المصطلحات التالية:

1.2.3 النظام البوابي التفاعلي لمكافحة البريد الاقتحامي (IGCS): هو كيان مسؤول عن كشف الاقتحام والتصدي له. وله وظيفتان، وظيفة بوابة المرسل (SGF) ووظيفة بوابة المستقبل (RGF). وينبغي أن يعمل النظام IGCS مع النظراء الآخرين لتطبيق كامل وظائف مكافحة الاقتحام.

2.2.3 قاعدة بيانات محلية لمكافحة البريد الاقتحامي: وهي قاعدة بيانات تستعمل لتخزين معلومات تتصل بالاقتحام وقوائم سوداء وقواعد مكافحة الاقتحام للوظائف المحلية لبوابة المستقبل وبوابة المرسل.

3.2.3 الأسلوب: يشير مصطلح الأسلوب إلى تشفير المعلومات التي تشتمل على معلومات يدركها الإنسان.

4.2.3 رسالة متعددة الأساليب: تدل على رسالة متعددة الوسائط تشتمل على معلومات مشفرة بأساليب مختلفة للتفاعل معها عبر أساليب متعددة.

5.2.3 وكيل المستقبل: هو مخدم يستقبل رسائل لمتلقيها. وفي تطبيقات البريد الإلكتروني، يعمل مخدم ببروتوكول مكتب البريد (POP) باعتباره وكيل مستقبل.

6.2.3 وظيفة بوابة المستقبل: وهي وظيفة الطرف المستقبل لمكافحة الاقتحام التي تكشف الاقتحام وتوقفه خلال عملية استقبال الرسالة.

7.2.3 وكيل المرسِل: هو مخدم يرسل رسائل لمرسليها. وفي تطبيقات البريد الإلكتروني، يعمل مخدم ببروتوكول النقل البسيط للإرسال (SMTP) باعتباره وكيل مرسل.

8.2.3 وظيفة بوابة المرسل: هي وظيفة الطرف المرسل لمكافحة الاقتحام التي تكشف الاقتحام وتوقفه خلال عملية إرسال الرسالة.

9.2.3 النظام النظير لمكافحة الاقتحام: خلال عملية مكافحة البريد الاقتحامي، هنالك نظامان IGCS يعملان سوية على رصد البريد الاقتحامي وتوقيفه، وهكذا يكون أحد النظامين IGCS نظام مكافحة الاقتحام النظير للنظام الآخر.

10.2.3 البروتوكول النظير لمكافحة الاقتحام: يتحدد البروتوكول بتبادل رسائل الإنذار بالاقتحام والقوائم السوداء بين بوابات مكافحة البريد الاقتحامي.

11.2.3 بروتوكول الإبلاغ عن الاقتحام: يتحدد البروتوكول بأن يُبلغ متلقو الرسائل البوابة عن البريد الاقتحامي.

4 المختصرات

تستعمل هذه التوصية المختصرات والأسماء المختصرة التالية:

E-mail بريد إلكتروني *(Electronic Mail)*

FE كيان وظيفي *(Functional Entity)*

IGCS نظام بوابي تفاعلي لمكافحة البريد الاقتحامي *(Interactive Gateway system for Countering Spam)*

IM رسالة لحظية *(Instant Message)*

IRC خدمة الدردشة على الإنترنت *(Internet Relay Chat)*

LscDB قاعدة بيانات محلية لمكافحة البريد الاقتحامي *(Local Spam-Countering Database)*

POP بروتوكول مكتب البريد *(Post Office Protocol)*

RA وكيل المستقبِل *(Receiver Agent)*

RBL قائمة سوداء في الوقت الفعلي *(Real-time Blackhole List)*

RGF وظيفة بوابة المستقبِل *(Receiver Gateway Function)*

SA وكيل المرسل *(Sender Agent)*

SCPP بروتوكول مكافحة البريد الاقتحامي النظير *(Spam-Countering Peering Protocol)*

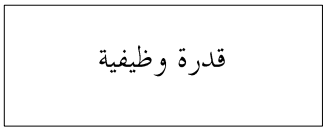
SGF وظيفة بوابة المرسل *(Sender Gateway Function)*

SMTP بروتوكول النقل البسيط للبريد *(Simple Mail Transfer Protocol)*

WPF مرشاح معلمات مرجحة *(Weighted Parameter Filter)*

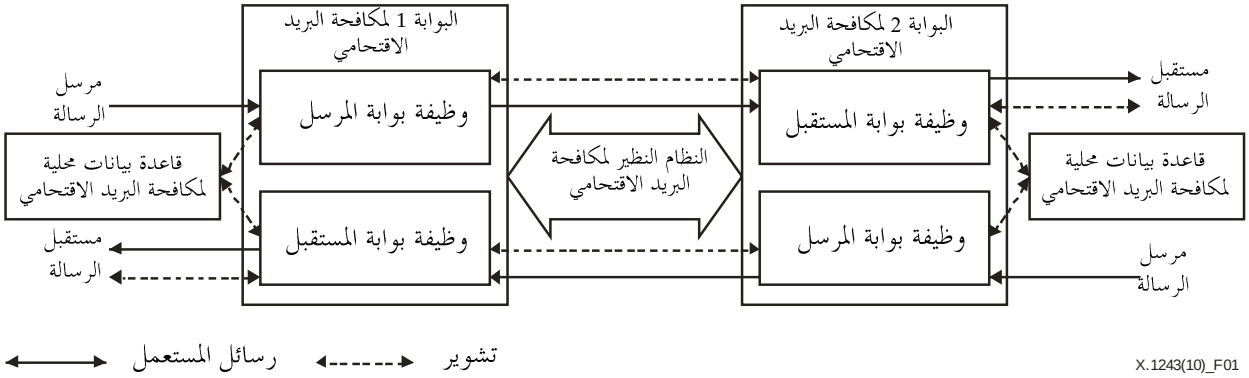
5 الاصطلاحات

قدرة وظيفية: تتحدد القدرة الوظيفية في إطار نظام بوابي تفاعلي لمكافحة البريد الاقتحامي باعتبارها مجموعة وظائف. ويُرمز إليها بالشكل التالي:



6 المعمارية

1.6 الكيانات والوظائف في نظام مكافحة البريد الاقتحامي



الشكل 1 – معمارية النظام البوابي التفاعلي لمكافحة البريد الاقتحامي

النظام البوابي التفاعلي لمكافحة البريد الاقتحامي (IGCS)

يتألف النظام IGCS من بوابة مكافحة الاقتحام وقاعدة بيانات محلية لمكافحة الاقتحام. ولبوابة مكافحة الاقتحام كيانان وظيفيان فرعيان هما: وظيفة بوابة المرسِل (SGF) ووظيفة بوابة المستقبِل (RGF). ويُعمل كلا هذين الكيانين الوظيفيين بوصفهما نقاط إقرار السياسة ونقاط إنفاذ السياسة. وتستخدم الوظيفة SGF في معالجة البريد الاقتحامي الخارج والوظيفة RGF لمعالجة البريد الاقتحامي الداخل. وتوفر قاعدة البيانات المحلية لمكافحة الاقتحام (IcsDB) قواعد مكافحة الاقتحام من أجل تحديد البريد الاقتحامي وإجراءات مكافحته. كما تقوم البوابة المحلية لمكافحة الاقتحام بتحديث قواعد مكافحة البريد الاقتحامي في قاعدة البيانات المحلية للمكافحة.

أما مسؤوليات الوظيفتين RGF وSGF فتتحدد على النحو التالي:

للوظيفة RGF بصورة أساسية ثلاث مسؤوليات هي:

- اتخاذ إجراءات مكافحة الاقتحام (السد أو العزل أو الإنذار إلى ما غير ذلك) بشأن البريد الاقتحامي المعروف الداخل؛
- كشف اقتحام جديد من خلال تقارير المستقبِل عن الاقتحام وتحديث قواعد مكافحة البريد الاقتحامي محلياً في القاعدة LcsDB؛
- تبليغ وظيفة بوابة المُرسل جهة مُرسل البريد الاقتحامي وذلك بإرسال التبليغ عند كشف الاقتحام.

وللوظيفة SGF مسؤوليتان هما:

- اتخاذ إجراءات مكافحة الاقتحام (السد أو العزل أو الإنذار وإلى ما غير ذلك) بشأن البريد الاقتحامي المعروف الخارج؛
- معالجة التبليغات بشأن البريد الاقتحامي الواردة من وظيفة بوابة المستقبِل جهة المستقبِل وتحديث قواعد مكافحة البريد الاقتحامي محلياً في القاعدة LcsDB.

قاعدة البيانات المحلية لمكافحة البريد الاقتحامي (LcsDB)

تستخدم القاعدة LcsDB في تخزين معلومات مكافحة الاقتحام. ويمكن أيضاً تصنيف هذه المعلومات إلى ثلاثة أنواع:

- معلومات التعرّف على البريد الاقتحامي: مثل عنوان مصدر بريد اقتحامي وكلمات مفتاحية في مجال موضوع الاقتحام؛
- قواعد مكافحة الاقتحام: مثل إعداد قائمة سوداء وقائمة بيضاء للبريد؛
- سجل البريد الاقتحامي المشبوه: عيّنات من البريد المشبوه الذي يرسله الكيانان الوظيفيان SGF وRGF.

2.6 التعرّف على البريد الاقتحامي

يتعرّف الكيانان الوظيفيان SGF وRGF على البريد الاقتحامي المعروف استناداً إلى المعلومات المخزنة في قاعدة البيانات LcsDB. ويصنف البريد الاقتحامي بعد ذلك في عدة مستويات ويعالج بالإجراءات المكافئة لهذه المستويات.

3.6 إجراءات مكافحة البريد الاقتحامي

بعد التعرّف على البريد الاقتحامي تقوم الوظيفة المعنية RGF أو SGF باتخاذ الإجراءات استناداً إلى المستوى المحدد للبريد الاقتحامي. وتشمل إجراءات مكافحة البريد الاقتحامي على سبيل المثال لا الحصر ما يلي:

- إنذار بالبريد الاقتحامي: ترسل الوظيفة SGF/RGF إنذاراً إلى مستقبِل/مُرسِل الرسالة؛
- عزل البريد الاقتحامي: تعزل الوظيفة SGF/RGF رسالة الاقتحام وترسل دورياً موجزاً عن العزل لمستقبِل/مرسِل الرسالة؛
- سد طريق البريد الاقتحامي: تسد الوظيفة SGF/RGF رسالة الاقتحام.

4.6 اكتشاف البريد الاقتحامي

1.4.6 اكتشاف الوظيفة RGF للبريد الاقتحامي

يرسل المستقبِل قواعد محاربة الاقتحام إلى الوظيفة RGF في الخدمة. وتشتمل قواعد محاربة الاقتحام على سبيل المثال لا الحصر على قائمة سوداء بعناوين المصدر/المقصد والكلمات المفتاحية في مجال البريد الإلكتروني. وتحدِّث الوظيفة RGF معلومات التعرّف على البريد الاقتحامي وقواعده في قاعدة البيانات LcsDB. وعند دخول رسالة مشبوهة تبدأ الوظيفة RGF عملية تقييم تحدد من خلالها ما إذا كانت الرسالة تشكل اقتحاماً، وذلك استناداً إلى قواعد مكافحة الاقتحام المخزنة في القاعدة LcsDB. وفي حال اعتبار الرسالة بريداً اقتحامياً، تتخذ الوظيفة RGF الإجراءات اللازمة.

2.4.6 اكتشاف الوظيفة SGF للبريد الاقتحامي

عملية اكتشاف البريد الاقتحامي في الوظيفة SGF مماثلة لتلك الموصوفة في الوظيفة RGF. وتتلقى الوظيفة SGF أيضاً تبليغات من الوظيفة RGF جهة المستقبِل، ثم تقيم هذا التبليغ وتحدِّث قواعد البريد الاقتحامي المؤكدة في القاعدة LcsDB.

5.6 التبليغ عن البريد الاقتحامي باستعمال بروتوكول النظير لمكافحة الاقتحام

1.5.6 اكتشاف النظير

عندما يحاول عنوان المرسل SA أن يرسل رسالة إلى عنوان مستقبل RA، يبدأ إجراء الاكتشاف النظير بكشف نظام IGCS نظير في الخدمة على طول مسار تسليم الرسالة. ويمكن لأحد النظامين IGCS تفعيل إجراء الاكتشاف. وبذلك تنشأ علاقة نظير بعد عملية استيقان النظير.

2.5.6 التبليغ عن البريد الاقتحامي بين النظراء

يمكن للنظام IGCS بعد إقامة علاقة نظير أن يتبادل التبليغات عن البريد الاقتحامي مع نظيره باستعمال بروتوكول النظير لمكافحة البريد الاقتحامي. وبما أن المستقبِل هو الذي يتعرّف أساساً على البريد الاقتحامي، فإن الوظيفة RGF لدى المستقبل تكون هي المسؤولة عن تحديد البريد الاقتحامي وتوفير معلومات عنه للوظيفة SGF جهة المرسل. وبعد أن تكشف الوظيفة RGF رسالة اقتحامية تبلغ الوظيفة SGF جهة المرسل عنها باستعمال عملية التبليغ عن الاقتحام. وينبغي أن تقرر الوظيفة SGF بعد تلقي التبليغ عن الاقتحام إمكانية قبول الرسالة تبعاً للسياسة المحلية لمكافحة الاقتحام.

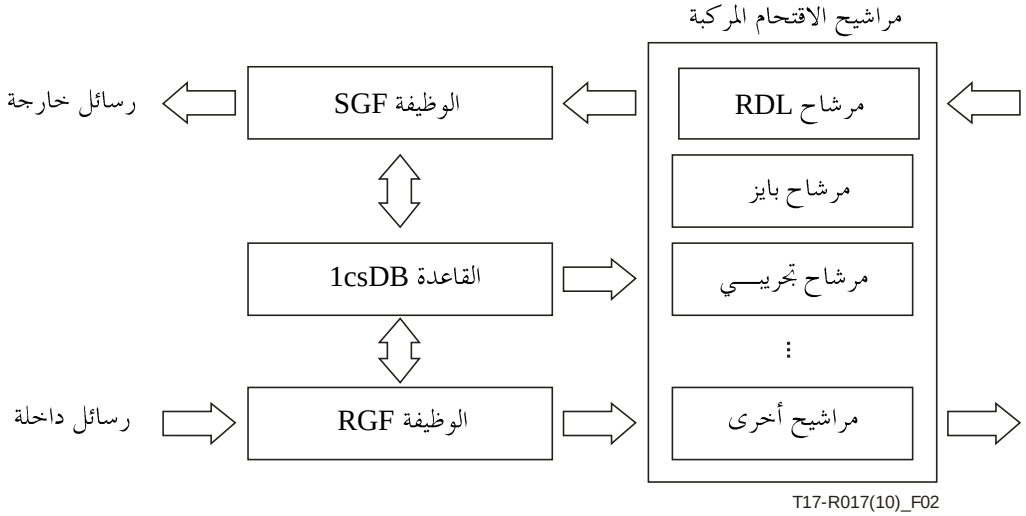
3.5.6 الجانب الأمني

يُوصى بإدراج آلية إصدار الشهادة المحددة في التوصية ITU-T X.509 في عملية التبليغ عن البريد الاقتحامي لاستيقان النظير. ويُوصى بالحصول على توقيع الكيان RGF رقمياً لرسالة التبليغ. كما يُوصى بعدم قبول رسائل التبليغ إلاّ من مصدر RGF موثوق.

7 تقنيات الترشيح في مكافحة البريد الاقتحامي

1.7 اعتبارات محايدة تقنياً

ينبغي للنظام IGCS أن يوفر عدداً من التقنيات المختلفة لمكافحة البريد الاقتحامي ومرونة تخوّله إدراج تقنيات ترشيح مكافحة البريد الاقتحامي الحالية والقادمة. ويمكن استخدام كل تقنية ترشيح خيارياً. ومن أجل كشف رسائل اقتحامية بصورة فعالة يمكن للنظام IGCS أن يوفر عدة تقنيات ترشيح ويجمعها في جهاز واحد في الشبكة المادية. أما تطبيق تقنيات ترشيح محدد فيقع خارج إطار هذه التوصية. ولا تحدد هذه التوصية إلا السطوح البينية وأنساق بيانات كل تقنية ترشيح لضمان إمكانية التشغيل البيني عند تبادل معلومات مكافحة البريد الاقتحامي بين نظراء النظام IGCS.



الشكل 2 – نظام IGCS مزوّد بمراشيح اقتحام متعددة

2.7 التقنيات المتوفرة لمكافحة الاقتحام

1.2.7 قائمة العناوين

قائمة سوداء بالوقت الفعلي (RBL): تتوفر القوائم RBL في عدة من المنظمات التي تضطلع بدراسة ظاهرة الاقتحام وتضع قوائم بعناوين مصدره. ويستطيع نظام ما لمكافحة الاقتحام أن يشترك في القائمة ويحدد وجود اقتحام أم لا من خلال التحقق من القائمة.

القوائم السوداء: وهي آلية أساسية لمراقبة النفاذ تتيح نفاذ أي كان ما عدا المصادر المُدرجة في القوائم السوداء. ويمكن تحديث هذه القوائم بصورة مستمرة، شأنها شأن القوائم RBL. كما أن النظام يعاني من أن العديد من الرسائل الاقتحامية لا تحمل عناوين مصدرها. وتتيح بعض الأنظمة للمستعملين أن يضعوا قوائم بيضاء بالمرسلين المسموح لهم لكنها قد تحذر المستعملين من استلام رسائل مشوّقة واردة من مصادر غير معروفة سابقاً.

2.2.7 الترشيح التجريبي

تستند هذه المراشيح إلى مبدأ اختبار وجود بعض الخصائص النمطية للبريد الاقتحامي في الرسالة، مثل الاستعمال الحصري للغة HTML أو نمط الزبون الذي ترسل إليه الرسالة. ويقيم الاختبار في عملية تعليم استناداً إلى مجموعة رسائل ومجموعة رسائل إلكترونية معروفة بأنها مشروعة.

وهنالك احتمال أن تصنف هذه المراشيح رسالة تستعمل أساليب المقتحمين، مثل الرسائل المثيرة في اللغة HTML، بوصفها رسائل اقتحامية.

ويمكن أن تكشف هذه المراشيح جزءاً كبيراً من الرسائل ولا تحتاج إلى ترتيب أو تشكيل. لكن نظراً لأنها تستعمل عدداً كبيراً من الاختبارات من الأفضل تغيير التشكيلة التي تجري بها الاختبارات والنتائج التي تحصل من أجل تصنيف الرسائل الاقتحامية.

3.2.7 ترشيح بايز

المبدأ الذي يقوم عليه مِرشاح بايز هو تدريب جهاز مكافحة البريد الاقتحامي على مجموعة من الرسائل الاقتحامية المعروفة بأنها اقتحامية ومجموعة من الرسائل المعروفة بأنها مشروعة. وبعد عملية التدريب تجمع خصائص المفردات المستخدمة في الرسائل الاقتحامية. ويستعمل ترشيح بايز احتمالات بايز لتقييم رسالة جديدة وتحديد ما إذا كانت اقتحامية أم لا. وفي حالة الترشيح الخاص بالمجموعات، يتم التدريب عادة من قِبل مدير النظام.

ويقوم ترشيح بايز الذي يستند إلى خوارزمية احتمالات بايز، بعمليات حسابية معقدة كثيرة ويطرح مشاكل على نطاق النظام الواسع لمكافحة الاقتحام. وقد يكون ذلك مقبولاً في بيئة صغيرة وشديدة الانتظام (مثل شبكة مؤسسة أو جامعة). غير أن ذلك غير ممكن في حالة مورد خدمة كبير خاصة إذا كان مورداً عمومياً.

وعلى الرغم من أن ترشيح بايز استعمل لمكافحة الاقتحام، لكن هنالك بعض القيود عندما يضع المقتحمون معلوماتهم.

4.2.7 الترشيح متعدد الأساليب

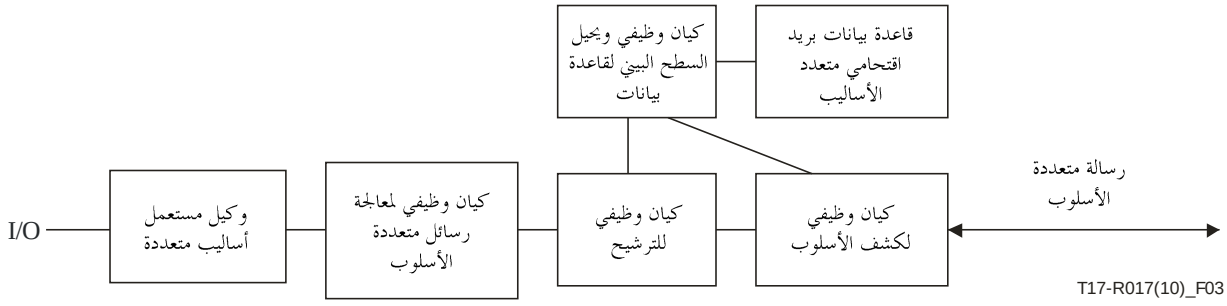
عندما يقوم النظام IGCS بترشيح متعدد الأساليب تنفذ الوظيفتان SGF وRGF ترشيحاً متعدد الأساليب عن طريق كيانين وظيفيين على التوالي هما: كيان وظيفي (FE) لكشف الأسلوب، وكيان وظيفي (FE) للترشيح وغيرها من الكيانات الوظيفية مثل كيان معالجة الرسائل متعددة الأساليب. ولا بد من تحديد مجموعات بيانات المعلومات عن مكافحة البريد الاقتحامي متعدد الأساليب من أجل التمكن من تخزين المعلومات وتبادلها. وتقوم قاعدة البيانات LcsDB بتخزين المعلومات متعددة الأساليب لمكافحة الاقتحام التي تحمل فئات (ومواضيع) رسائل متعددة الأساليب ومناسبة إلى جانب معايير ترشيح (يدخلها المستعملون أو المشغلون، أو مكتسبة من أنظمة IGCS نظراء).

إذا توفر وصف البيانات الشرحية متعددة الأساليب واعتبر هذا الوصف جديراً بالثقة يمكن للتطبيقات متعددة الأساليب أن تقوم بترشيح المعلومات متعددة الأساليب استناداً إلى وصف البيانات الشرحية للمحتوى متعدد الأساليب. وإلاّ يُفضل ترشيح كامل المعلومات متعددة الأساليب حيث يتعين على الكيانات الوظيفية التالية القيام بمهمات على النحو التالي:

- تحتفظ قاعدة بيانات أو مستودع بفئات الرسائل متعددة الأساليب المناسبة وبمعايير الترشيح. ويمكن تواجد القاعدة أو المستودع في نفس مكان/ميدان الكيان الوظيفي وكيل السطح البيني لقاعدة البيانات والكيان الوظيفي لكشف الأسلوب والكيان الوظيفي للمعالجة متعددة الأساليب وكيان مستعمل الأسلوب المتعدد، وفي حالات أخرى يمكن استضافة قاعدة البيانات أو المستودع في أمكنة أو ميادين أخرى غير الكيان الوظيفي للترشيح؛
- يفحص كيان وظيفي لكشف الأسلوب رسالة متعددة الأسلوب مرسلة أو مستقبلة من أجل تحديد الأساليب الواردة فيها؛
- يستخرج كيان وظيفي لوكيل السطح البيني لقاعدة البيانات معايير الترشيح من قاعدة بيانات واردة في أساليب وفئات رسائل معينة؛
- يرشح كيان وظيفي للترشيح رسالة متعددة الأسلوب ومعيار ترشيحها. وقد يسد هذا الكيان كلياً أو جزئياً الأجزاء متعددة الأساليب المنتقاة من رسالة متعددة الأساليب تجري معالجتها.

ويشرح الشكل 3 المعمارية العامة لرسائل الترشيح متعددة الأساليب والكيانات الوظيفية اللازمة. وتضم معمارية الترشيح الكيان الوظيفي لكشف الأسلوب والكيان الوظيفي للترشيح والكيان الوظيفي الوكيل للسطح البيني لقاعدة البيانات وقاعدة البيانات متعددة الأساليب كما يعرض الشكل 3 كيانات وظيفية أخرى لا تقوم عادة بأي مهمة ترشيح متعدد الأساليب مثل كيان وظيفي لمعالجة رسالة متعددة الأساليب أو وكيل مستعمل متعددة الأساليب.

ويعالج الكيان الوظيفي لمعالجة الرسائل متعددة الأساليب الرسائل متعددة الأساليب (المرشحة) ويضبط زمن وصول هذه الرسائل من وكلاء مستعملي الأساليب المتعددة ويرسلها أو يوزع الرسائل متعددة الأسلوب المرشحة على وكلاء مستعملي الأساليب المتعددة. ويعالج كل من وكلاء مستعملي الأساليب المتعددة المختلفين الأساليب الخاصة مثل مدخل و/أو منتج أسلوبي (محدد الجهاز).



الشكل 3 – معمارية ترشيح متعدد الأساليب

ويبين الشكل 4 تفاصيل المعمارية النوعية للترشيح متعدد الأساليب من خلال مقابلة الكيانات الوظيفية مع وظيفة بوابة المستقبِل (RGF). وتصف الخطوات التالية الإجراءات التي تقوم بها الكيانات الوظيفية عند تلقّيها رسالة متعددة الأساليب:

1) مستقبل الوظيفة RGF رسالة متعددة الأساليب.

2) يحدد الكيان الوظيفي لكشف الأسلوب الأساليب الواردة والنمط (الأنماط) الواردة في الرسالة متعددة الأسلوب الواصلة.

3) يمكن تشكيل الكيان الوظيفي للترشيح بصورة ساكنة مع قواعد ترشيح لجميع الرسائل متعددة الأسلوب الممكنة (مثل منعزل عن حالة خاصة لتلقي رسالة متعددة الأسلوب) أو بصورة دينامية مع رسالة و/أو قاعدة متعلقة بأسلوب لكل رسالة متعددة الأساليب مستلمة.

أ) ويمكن للكيان الوظيفي لكشف الأسلوب إما أن يقدم الأساليب التي تم التعرّف عليها ومعلمات نمط الرسالة إلى وكيل سطح بيني لقاعدة بيانات. وإما أن يربط المعلمات بالرسالة الواصلة.

ب) يُرسل الكيان الوظيفي لكشف الأسلوب الرسالة متعددة الأساليب بعد الإشارة إلى الأساليب التي تتضمنها ومعلمات نمطها إن أمكن، إلى الكيان الوظيفي للترشيح.

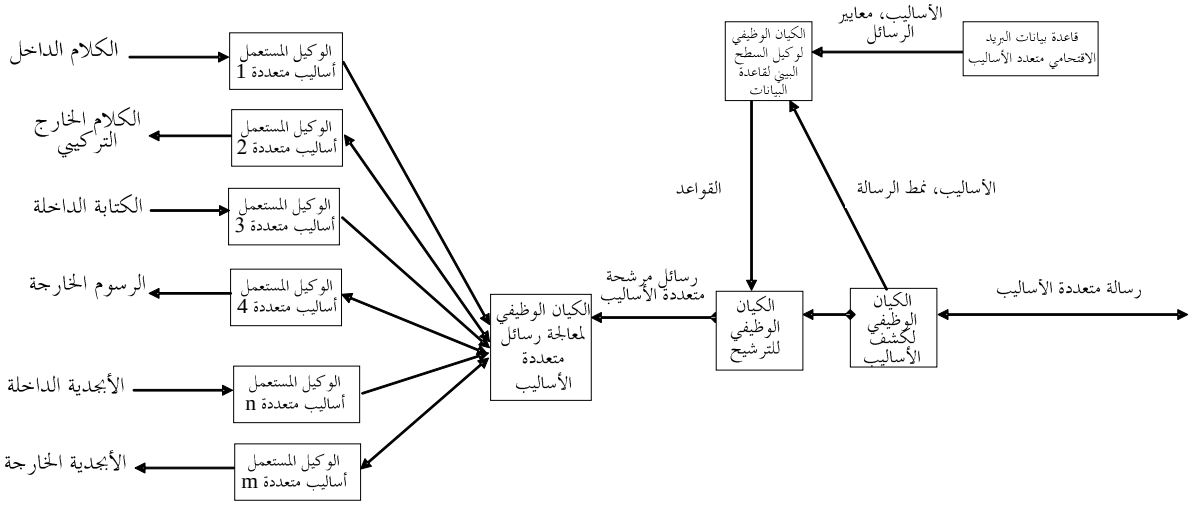
4) يُرسل الكيان الوظيفي للترشيح، في حال عدم تشكيله مع القواعد، الأساليب ومعلمات نمط الرسالة إلى وكيل السطح البيني لقاعدة البيانات إن لم يكن هذا الوكيل قد حصل على هذه المعلمات مباشرة من الكيان الوظيفي لكشف الأسلوب.

5) يطلب الكيان الوظيفي الوكيل للسطح البيني لقاعدة البيانات من قاعدة البيانات متعددة الأساليب الحصول على أساليب ومعايير رسائل مقابلة. ويجمع الكيان الوظيفي المذكور هذه القيم في قواعد محددة ويرسلها إلى الكيان الوظيفي للترشيح.

6) يطبق الكيان الوظيفي للترشيح القواعد المتوفرة ويجري الترشيح للرسائل متعددة الأساليب الواصلة. وتبعاً للقواعد والسياسات المتبعة، تمر الرسائل متعددة الأساليب أو تستبعد كلياً أو جزئياً عندما يعترض سبيل بعض الأساليب فقط في الرسالة متعددة الأساليب.

7) يرسل الكيان الوظيفي للترشيح الرسالة متعددة الأساليب المرشحة إلى الكيان الوظيفي لمعالجة الرسائل متعددة الأساليب مع الإشارة إلى بعض نتائج الترشيح إن أمكن (معلومات عن التسجيل أو إنذارات أمنية).

8) يعالج الكيان الوظيفي لمعالجة الرسائل متعددة الأساليب الرسائل الواصلة متعددة الأساليب (الناتجة عن الترشيح). ويزامن الكيان الوظيفي المدخلات الواردة من مختلف وكلاء مستعملي الأساليب المتعددة للدخل المختلفين. ويصنف الرسائل حسب مكوّناتها الأسلوبية ويرسل هذه الأجزاء الخاصة بالأسلوب إلى وكلاء مستعملي الأساليب المتعددة للخَرج.



الشكل 4 – ترشيح متعدد الأساليب في وظيفة بوابة المستقبِل (RGF)

ملاحظة: يصف الشكل 4 عدة وكلاء مستعملي الأساليب المتعددة. وقد لا تتطلب الوظيفة RGF تواجد جميع الوكلاء الواردين في الشكل.

5.2.7 مِرشاح تجميد البريد الاقتحامي

يُستعمل مرشاح تجميد البريد الاقتحامي لمراقبة معدل وصول الرسائل. ومعلمة الدخل الهامة لمرشاح التخميد هي معامل تجميد البريد الاقتحامي. وتتمثل هذه المعلمة في قياس الرسائل المشبوهة وتراقب معدلات وصول الرسائل. فعندما تصل كمية كبيرة من الرسائل المشبوهة يزداد المعامل بالتالي ويُخفض مرشاح تجميد البريد الاقتحامي معدل وصول الرسائل الإلكترونية المشبوهة. وتنتج هذه المعلمة عادة عن نظام خارجي لمكافحة البريد الاقتحامي مثل الخبرة أو قاعدة بيانات ذات شهرة. وقد

يؤثر مرشاح تجميد البريد الاقتحامي على مهلة استجابة البريد الإلكتروني وحجم نوافذ النقل ومدة دورة التخميد وإلى ما غير ذلك.

6.2.7 مِرشاح رأسية البريد الإلكتروني

يراقب مِرشاح رأسية البريد الإلكتروني (EHF) محادثات البروتوكول SMTP ويتأكد من امتثالها للبروتوكولات ذات الصلة. ويمكن استعماله لتحديد مدى عدم اتساق البروتوكول ورأسيات البريد الإلكتروني المزوّرة. وقد يطلب المِرشاح EHF من أجل إعادة إقامة الجلسات SMTP وتتبع حالات البروتوكولات تجميع الرزم وجمع تدفقات البروتوكول TCP، إلى ما غير ذلك. ويركّز المِرشاح EHF على تحليل مستوى البروتوكول ويوفر مزيداً من المعلومات في سبيل تحسين دقة التعرّف على البريد الاقتحامي بشكل عام. ويُدرج المرشاح EHF عادة في العديد من أنظمة محاربة البريد الاقتحامي المطروحة في الأسواق إلى جانب بعض أنظمة محاربة البريد الاقتحامي مفتوحة المصدر.

7.2.7 مِرشاح المعلمات المرجحة (WPF)

يستعمل مرشاح المعلمات المرجحة (WPF) لكشف البريد الاقتحامي من خلال تحليل معلمات متعددة. فالمعلمات تستند إلى معلومات إحصائية تضم عدد دورات البريد وعدد الخدمات المرسل إليها وعدد محاولات البريد الإلكتروني ومدة إرسال الرسائل ومعدل إرسالها ومعدل المحاولات والرسائل الناجحة وإلى ما غير ذلك. ولكل معلمة عتبة وقيمة ترجيح يتم تحديدها. وإلى جانب ذلك، فإن كامل مجموعة قيمة الترجيح التي قد يطلب تبريرها عدة مرات مسبقاً عند التجريب، مطلوبة أيضاً. ويتم التحقق من جميع المعلمات في كل رسالة حسب القواعد. ولا يضاف ترجيح إلا للمعلمات التي تتجاوز العتبة المحددة. وإذا تجاوز مجموع المعلمات العتبة المحددة مسبقاً يمكن للمرشاح WPF أن يميّز بين الرسائل الإلكترونية الاقتحامية والرسائل العادية.

8 عملية بروتوكول النظام النظير لمكافحة الاقتحام

1.8 اكتشاف النظير

عملية اكتشاف النظير هي إقامة علاقة نظير بين نظامين IGCS. وتبدأ هذه العملية عندما يحاول نظام IGCS اكتشاف نظام IGCS صالح بموازاة مسار تسليم الرسالة. وعندما تكشف وظيفة RGF رسالة مشبوهة تبدأ عملية اكتشاف النظير.

يُوصى برسالة اكتشاف النظير لإدراج المعلومات التالية:

- قائمة عناوين الوظيفتين SGF/RGF في النظام الأول: عنوان المصدر (مثال، عنوان IP للمصدر وزوج المنفذين). للحماية من أعطال النقطة الواحدة، يمكن لنظام IGCS أن يدرج عدة وظائف RGF وSGF للتعويض. وقد تحتوي قائمة العناوين على عناوين وظائف RGF/SGF للنظام IGCS الأول.
- عنوان النظام IGCS النظير: @IGCS {عنوان حاسوب الطرف المقابل}.
- مصدر البريد الاقتحامي: عنوان مرسل البريد الاقتحامي.
- نوع البريد الاقتحامي المشبوه: WELL_KNOWN, USER_REPORTED u OTHER.
- البريد الاقتحامي المشبوه المرفق: البريد الاقتحامي المشبوه الذي يُرفق بالرسالة.

وعند إرسال رسالة اكتشاف نظير يبدأ عمل مؤقت النظام IGCS الأول. وفي حال عدم استلام رسالة استجابة بعد انقضاء المهلة المحددة، لكون النظام IGCS الأول أخفق في اكتشاف نظام IGCS نظير. وقد تتضمن رسالة الرد على اكتشاف النظير المعلومات التالية:

- قائمة عناوين الوظائف RGF/SGF للنظام الذي يرسل الرد.
- تأكيد بشأن البريد الاقتحامي المشبوه: للتأكيد على ما إذا كان النظام IGCS الذي يرسل الرد يعتبر البريد الاقتحامي المشبوه بريداً اقتحامياً.

2.8 إقامة علاقة النظير

عندما يتلقى النظام IGCS الأول قبل انقضاء المهلة رسالة رد على اكتشاف النظير، يمكنه الشروع بإقامة علاقة النظير. وتنطوي العملية على إجراءين رئيسيين هما:

- يحدِّث النظام IGCS قائمة النظراء: يضيف قائمة عناوين نظام الطرف الآخر IGCS إلى قائمة النظير.
- قائمة أسماء مراشيح البريد الاقتحامي المتوفرة: المراشيح المتوفرة في كل نظام IGCS.

3.8 تبادل رسائل مكافحة البريد الاقتحامي

يبدأ النظام IGCS بعد عملية إقامة العلاقة مع النظير، تبادل رسائل مكافحة البريد الاقتحامي. وفي هذه العملية يتبادل نظاما IGCS نظيرا المعلومات عن مراشيح البريد الاقتحامي المشتركة المتوفرة. ويحدث كل نظام IGCS قاعدة بياناته المحلية من خلال تبادل رسائل لهذا الغرض.

4.8 تحرير النظير

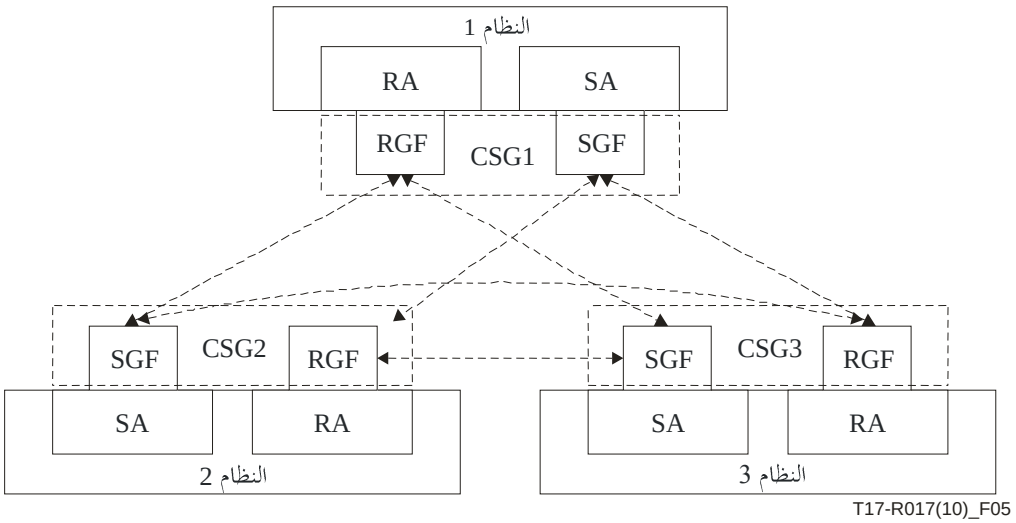
في حال عدم كشف أي بريد اقتحامي خلال فترة من الزمن، يمكن لأحد النظامين IGCS أن يُنهي علاقة النظير وذلك بإرسال رسالة تحرير النظير. وبعد أن يتلقى النظام IGCS رسالة تحرير النظير يلغي معلومات النظير ذات الصلة أو يعيد استعمالها وفقاً للسياسة المحددة.

9 تنفيذ نموذج أنظمة بوابية لمكافحة البريد الاقتحامي

1.9 النموذج المدمج

1.1.9 وصف النموذج

يُدرج في النظام المدمج نظام IGCS مع نظام رسائل يضم عنوان مستقبِل (RA) وعنوان مرسل (SA). وكل نظام له بوابة (وظيفة RGF ووظيفة SGF) وقاعدة بيانات محلية. وعلى سبيل المثال، يمكن أن يكون عنوان المستقبِل في نظام بريد إلكتروني مخدّم ببروتوكول POP3 ويكون عنوان المرسل مخدم ببروتوكول SMTP. ويمكن استخدام وظيفة RGF/SGF باعتبارها مخدم مدمج يتيح خدمات البروتوكولين POP3 وSMTP على حد سواء. ويشترط وجود قاعدة بيانات LcsDB أيضاً في نظام البريد الإلكتروني كيما توفر قواعد مكافحة البريد الاقتحامي. ويبين الشكل 5 نموذجاً مدمجاً.



الشكل 5 – نموذج مدمج للنظام IGCS

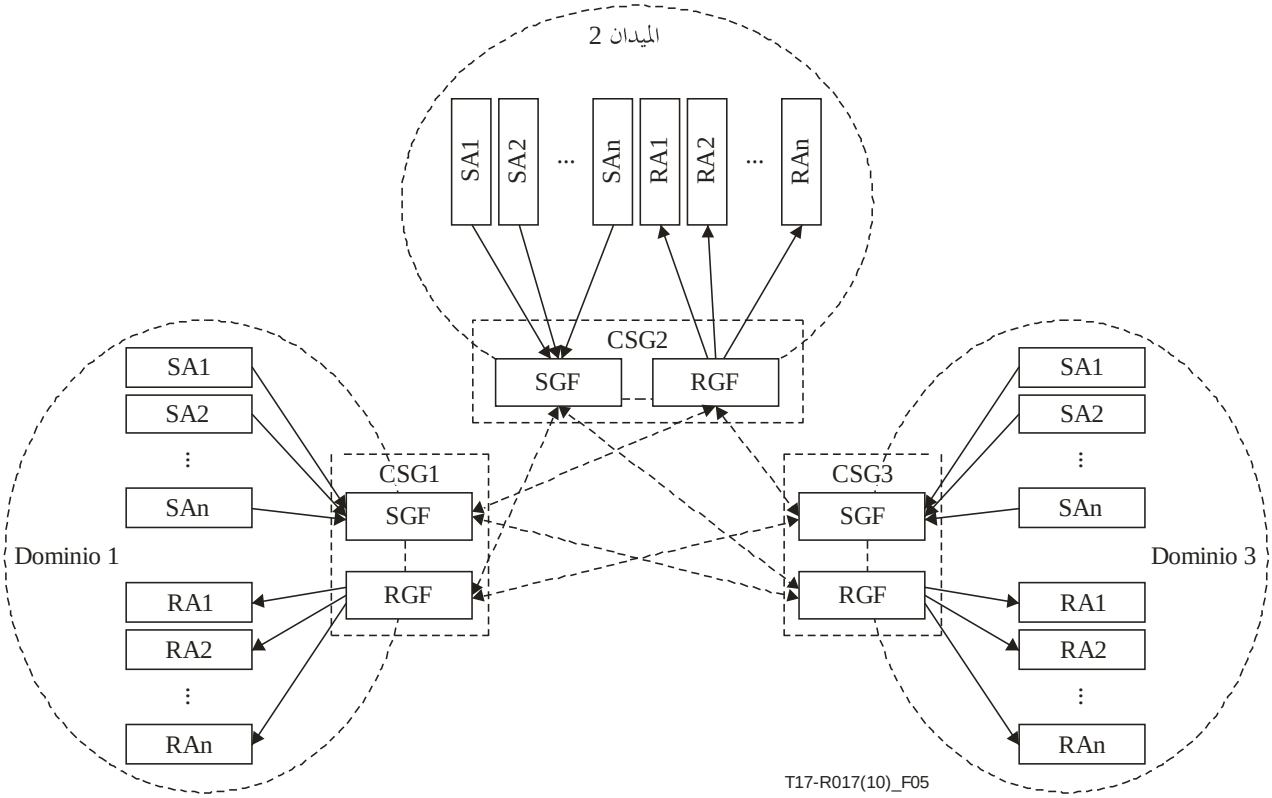
2.1.9 حالات الاستعمال

يناسب النموذج المدمج نموذج الزبون/المخدم الذي يقوم بخدمة إرسال/استقبال رسائل للعديد من الزبائن. وفي هذه الحالة يعمل المخدّم كنقطة قرار ونقطة إنفاذ سياسات في الأنشطة المضادة للبريد الاقتحامي.

2.9 النموذج القائم على أساس الميدان

1.2.9 وصف النموذج

في النموذج القائم على أساس الميدان، يعمل النظام IGCS كحاسوب تسليم رسائل في ميدان قد يكون له عدة عناوين SA وRA لمتطلبات توازن الحمولة. وقد تكون للوظيفة RGF/SGF عدة حالات موزعة في ميدان ما. وكل حالة RGF/SGF مكلفة بعدة عناوين SA/RA في ميدان ما ومسؤولة عن مكافحة الرسائل الاقتحامية في الميدان المحلي والميدان الداخلي على حدّ سواء.



الشكل 6 – النموذج القائم على أساس الميدان

2.2.9 حالات الاستعمال

يمكن استعمال النموذج القائم على الميدان لأغراض مكافحة البريد الاقتحامي القائمة على الميدان. وهو يتماشى بشكل خاص مع أنظمة الاتصال بين النظراء مثل العديد من تطبيقات الرسائل الإلكترونية الرائجة شعبياً: مثل خدمة الدردشة على الإنترنت (IRC). وفي نموذج الاتصال بين النظراء يعمل نظام جهة المستعمل ذاته كعنوان مستقبِل وعنوان مُرسِل في نفس الوقت. وسيكون من الصعب جداً تشغيل عدد كبير من العناوين RA وSA جهة المستعمل في نَموذج IGCS مُدمج. لكن النموذج القائم على الميدان قادر على حل المشكلة بطريقة التوزيع.

3.9 نموذج النشر بالتحويل

1.3.9 وصف النموذج

يمكن أيضاً نشر نظام IGSC في شبكة لا سلكية باستعمال نقاط نفاذ لا سلكية. وتحوِّل نقطة النفاذ اللاسلكية جميع الرسائل إلى النظام IGSC. ويقرر النظام IGCS بشأن الرسائل الداخلة استناداً إلى القواعد المخزنة في القاعدة LcsDB ويبعث بالرسائل السليمة إلى الشبكة اللاسلكية.

2.3.9 حالات الاستعمال

يمكن استعمال نموذج النشر بالتحويل في شبكة لا سلكية. ويمكن ترشيح البريد الاقتحامي خارجاً قبل وصوله إلى الشبكة اللاسلكية بحيث يمكن تخفيف التكاليف غير الضرورية الناجمة عن إيصال حركة البريد الاقتحامي إلى المستعملين النهائيين.

التذييل الأول

مثال لتعريف رسالة SCPP

(يعتبر هذا التذييل جزءاً أساسياً من التوصية)

يرد مثال رسالة CSPP معرّفة في لغة الترميز ASN.1 على النحو التالي، وقد تحقق مجمِّع الترميز ASN.1 منه:

An example of SCPP messages defined in ASN.1 language is listed as follows and has been checked by the ASN.1 compiler:

```
SCPP-MESSAGES {itu-t(0) recommendation(0) x(24) igscs(1243)
asn1-module(0) scpp-messages(1)}
DEFINITIONS AUTOMATIC TAGS ::=
BEGIN

-- SCPP Message body definition
SCPP-PDU ::= SEQUENCE {
     sourceAddress        IGCS-Address,
     destAddress          IGCS-Address,
     igcs-message-body    CHOICE {
               peerDiscovery   PeerDiscoveryDEF,
               peerSetup       PeerSetupDEF,
               dataExchange    DataExchangeDEF,
               peerKeepAlive   PeerKeepAliveDEF,
               peerRelease     PeerReleaseDEF},
     nonStandardData      OCTET STRING OPTIONAL,
     ...
}

-- PeerDiscovery Message definition
PeerDiscoveryDEF::=SEQUENCE {
     setupRequest    BOOLEAN,
     igcsSignature   IGCS-Signature
}

-- PeerSetup Message definition
PeerSetupDEF::=SEQUENCE {
     setupResponse        BOOLEAN,
     sgfList              SEQUENCE OF IGCS-Address,
     rgfList              SEQUENCE OF IGCS-Address,
     supportedFilters     SupportedSpamFilters,
     igcsSignature        IGCS-Signature
}

-- Countering Spam Data Exchange Message definition
DataExchangeDEF::=SEQUENCE {
     csData               SET OF SpamFilterData,
     ...
}

-- Peer Keep Alive Message definition
PeerKeepAliveDEF::=SEQUENCE {
     sgfUpdates      GF-Updates,
     rgfUpdates      GF-Updates,
     filtersUpdates  SupportedSpamFilters
}
-- Peer Release Message definition
PeerReleaseDEF::=SEQUENCE {
     peerRelease     ENUMERATED{request(0), confirm(1)},
     nonStandardData OCTET STRING OPTIONAL,
     ...
}
```

```
-- IGCS supported addresses, include IGCS,SGF,RGF address definition
-- Support IP address, Email ID and other types of address
IGCS-Address::=CHOICE{
     ipAddress
     SEQUENCE { ip OCTET STRING(SIZE(4)),
                port INTEGER(0..65535) },
                ip6Address
                SEQUENCE { ip OCTET STRING(SIZE(16)),
                           port INTEGER(0..65535) },

     emailAddress         IA5String(SIZE(1..512)),
     nonStandardAddress   OCTET STRING,
     ...
}

-- Signature data for authentication
IGCS-Signature::=SEQUENCE {
     igcsID          INTEGER(0..65535),
     signatureData   OCTET STRING,
     ...
}

-- RGF/SGF status update information
GF-Updates::=SEQUENCE {
     gateType        ENUMERATED {sgf(0),rgf(1)},
     gateAdd         IGCS-Address,
     gateRemove      IGCS-Address
}

-- IGCS Supported Spam filters and related data

SupportedSpamFilters::= SEQUENCE {
     supportedFilter SEQUENCE OF SpamFilters

}

SpamFilters::=SEQUENCE{
     filterID        INTEGER(0..128),
     filterName      IA5String(SIZE(1..512))
}

SpamFilterData::=SEQUENCE {
     filterID        INTEGER(0..128),
     filterData      OCTET STRING,
     ...
}

END
```

البيبليوغرافيا

[b-ITU-T X.680] Recommendation ITU-T X.680 (2008) | ISO/IEC 8824-1:2008, *Information technology – Abstract Syntax Notation One (ASN.1): Specification of basic notation.*

[b-ITU-T X.681] Recommendation ITU-T X.681 (2008) | ISO/IEC 8824-2:2008, *Information technology – Abstract Syntax Notation One (ASN.1): Information object specification.*

[b-ITU-T X.682] Recommendation ITU-T X.682 (2008) | ISO/IEC 8824-3:2008, *Information technology – Abstract Syntax Notation One (ASN.1): Constraint specification.*

[b-ITU-T X.683] Recommendation ITU-T X.683 (2008) | ISO/IEC 8824-4:2008, *Information technology – Abstract Syntax Notation One (ASN.1): Parameterization of ASN.1 specifications.*

[b-ITU-T X.1231] Recommendation ITU-T X.1231 (2008), *Technical strategies for countering spam.*

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

[b-ITU-T X.1241] Recommendation ITU-T X.1241 (2008), *Technical framework for countering e-mail spam*.

[b-IETF RFC 1869] IETF RFC 1869 (1995), *SMTP Service Extensions*.

[b-IETF RFC 1939] IETF RFC 1939 (1996), *Post Office Protocol – Version 3*.

[b-IETF RFC 2060] IETF RFC 2060 (1996), *Internet Message Access Protocol – Version 4rev1*.

[b-IETF RFC 2505] IETF RFC 2505 (1999), *Anti-Spam Recommendations for SMTP MTAs*.

[b-IETF RFC 2635] IETF RFC 2635 (1999), *DON'T SPEW A Set of Guidelines for Mass Unsolicited Mailings and Postings (spam*).*

[b-IETF RFC 2821] IETF RFC 2821 (2001), *Simple Mail Transfer Protocol*.

[b-IETF RFC 2822] IETF RFC 2822 (2001), *Internet Message Format*.

[b-IETF RFC 3685] IETF RFC 3685 (2004), *SIEVE Email Filtering: Spamtest and VirusTest Extensions.*

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	نوعية الإرسال الهاتفي والمنشآت الهاتفية وشبكات الخطوط المحلية
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