الاتحـــــــــاد الدولـــــــــي للاتصـــــــــالات

ITU-T

قطـــاع تقييس الاتصـــالات
في الاتحاد الدولي للاتصالات

X.1241

(2008/04)

السلسلة X: شبكات البيانات والاتصالات بين الأنظمة المفتوحة والأمن

أمن الاتصالات

الإطار التقني لمكافحة الرسائل الاقتحامية عبر البريد الإلكتروني

التوصيـــة ITU-T X.1241

الاتحاد الدولي للاتصالات

توصيات السلسلة X الصادرة عن قطاع تقييس الاتصالات

شبكات البيانات والاتصالات بين الأنظمة المفتوحة والأمن

الشبكات العمومية للبيانات	
الخدمات والمرافق	X.19–X.1
السطوح البينية	X.49–X.20
الإرسال والتشوير والتبديل	X.89–X.50
جوانب الشبكة	X.149–X.90
الصيانة	X.179–X.150
الترتيبات الإدارية	X.199–X.180
التوصيل البيني للأنظمة المفتوحة	
النموذج والترميز	X.209–X.200
تعاريف الخدمات	X.219–X.210
مواصفات البروتوكول بأسلوب التوصيل	X.229–X.220
مواصفات البروتوكول بأسلوب غياب التوصيل	X.239–X.230
جداول إعلان المطابقة (PICS)	X.259–X.240
تعرّف هوية البروتوكول	X.269–X.260
بروتوكولات الأمن	X.279–X.270
أشياء مسيرة على الطبقة	X.289–X.280
اختبار المطابقة	X.299–X.290
التشغيل البيني للشبكات	
اعتبارات عامة	X.349–X.300
الأنظمة الساتلية لإرسال البيانات	X.369–X.350
الشبكات القائمة على بروتوكول الإنترنت	X.399–X.370
أنظمة معالجة الرسائل	X.499–X.400
الدليل	X.599–X.500
التوصيل الشبكي في التوصيل البيني للأنظمة المفتوحة (OSI) وجوانب النظام	
التوصيل الشبكي	X.629–X.600
الفعالية	X.639–X.630
نوعية الخدمة	X.649–X.640
التسمية والعنونة والتسجيل	X.679–X.650
ترميز النظم المجرد واحد (ASN.1)	X.699–X.680
إدارة التوصيل البيني للأنظمة المفتوحة (OSI)	
الإطار والهيكل المعماري لإدارة الأنظمة	X.709–X.700
خدمة اتصالات الإدارة وبروتوكولاتها	X.719–X.710
هيكل معلومات الإدارة	X.729–X.720
وظائف الإدارة ووظائف الهيكل المعماري للإدارة الموزعة المفتوحة	X.799–X.730
الأمن	X.849–X.800
تطبيقات التوصيل البيني للأنظمة المفتوحة (OSI)	
الالتزام والتلازم والاستعادة	X.859–X.850
معالجة المعاملات	X.879–X.860
العمليات البُعدية	X.889–X.880
التطبيقات التنوعية لترميز النظم المجرد واحد (ASN.1)	X.899–X.890
المعالجة الموزعة المفتوحة	X.999–X.900
أمن الاتصالات	**X.1000–**

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

التوصيـــة ITU-T X.1241

الإطار التقني لمكافحة الرسائل الاقتحامية عبر البريد الإلكتروني

الخلاصة

توفر التوصية ITU-T X.1241 إطاراً تقنياً لمكافحة الرسائل الاقتحامية عبر البريد الإلكتروني. ويصف هذا الإطار بنية واحدة موصى بها لميدان معالجة مقاوم للرسائل الاقتحامية والوظيفة المحددة لكل وحدة من الوحدات النموذجية الرئيسية فيه. والنقطة الأساسية للإطار هي أنه يرسي آلية لتبادل المعلومات بشأن الرسائل الاقتحامية عبر البريد الإلكتروني بين مختلف مخدِّمات البريد الإلكتروني. وسوف تحسن الأنظمة التي تتبع هذا الإطار من الكفاءة من خلال التوصيل البيني.

المصدر

وافقت لجنة الدراسات 17 (2005-2008) لقطاع تقييس الاتصالات على التوصية ITU-T X.1241 بتاريخ 18 أبريل 2008 بموجب الإجراء الذي ينص عليه القرار 1 للجمعية العالمية لتقييس الاتصالات.

الكلمات المفتاحية

مقاوم للرسائل الاقتحامية، البريد الإلكتروني، التوصيل البيني، الرسائل الاقتحامية، الإطار التقني.

تمهيـــد

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

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

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

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

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/.

© ITU 2009

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

المحتويات

الصفحة

1 مجال التطبيق 1
2 المراجع 1
3 تعاريف 1
1.3 المصطلحات المعرَّفة في مواضع أخرى 1
2.3 مصطلحات معرَّفة في هذه التوصية 1
4 الاختصارات والأسماء المختصرة 2
5 اصطلاحات 2
6 البنية العامة لميدان المعالجة المقاوم للرسائل الاقتحامية 2
1.6 البنية العامة 2
2.6 نموذج مرجعي 4
7 وظائف ميدان المعالجة المقاوم للرسائل الاقتحامية 5
1.7 وظائف عميل البريد الإلكتروني 5
2.7 وظائف مخدِّم البريد الإلكتروني 5
3.7 وظائف كيان المعالجة المقاوم للرسائل الاقتحامية 6
4.7 وظائف الكيان الفرعي للمعالجة المقاوم للرسائل الاقتحامية 6
8 التعرف على الرسائل الاقتحامية 7
1.8 الخصائص الشائعة للرسائل الاقتحامية 7
2.8 المعايير المشتركة لمكافحة الرسائل الاقتحامية 8
9 طرائق مكافحة الرسائل الاقتحامية 9
1.9 إبطال وظيفة 'الترحيل المفتوح' 9
2.9 التحكم في عملية التصريح بتسليم البريد الإلكتروني 9
3.9 تقنية الترشيح 9
4.9 اختبار إمكانية تعقُّب البريد الإلكتروني 10
10 التوصيل البيني بين ميادين المعالجة المقاومة للرسائل الاقتحامية 11
1.10 التوصيل البيني بين كيانات المعالجة الرئيسية 11
2.10 التوصيل البيني بين كيان المعالجة والكيان الفرعي للمعالجة 11
3.10 التوصيل البيني بين كيان فرعي للمعالجة ومخدِّم بريد إلكتروني 12
ثبت المراجع 13

مقدمة

لقد شهد تطور شبكة الاتصالات القائمة على بروتوكول الإنترنت تبادل أعداد هائلة من البريد الإلكتروني بين المستعملين. وفي الوقت ذاته، يُرسَل المزيد ثم المزيد من الرسائل الاقتحامية إلى هؤلاء المستعملين من خلال شبكة الاتصالات القائمة على بروتوكول الإنترنت ويتسبَّب ذلك في مشاكل خطيرة.

ولقد أصبحت الرسائل الاقتحامية عبر البريد الإلكتروني وباءً يؤدي إلى تردّي مقدرة الخدمة في شبكة الاتصالات القائمة على بروتوكول الإنترنت. ويضطر مقدِّمو الخدمات إلى إنفاق مبالغ كبيرة من المال للتغلب على المشاكل التي تتسبَّب فيها ظاهرة الرسائل الاقتحامية. ويتطلب الأمر من المستعملين وقتاً طويلاً للتخلص من هذة الرسائل الاقتحامية عبر البريد الإلكتروني.

وقد طُرِحت بعض التقنيات لتحرِّي الرسائل الاقتحامية والتخلص منها. ولكن المقتحمين على درجة عالية من الابتكار في تجنب الكشف عن هويتهم. إذ باستطاعتهم مثلاً تزييف البريد الإلكتروني العادي وجعل محتواه عشوائياً لتجنب الكشف عنه من جانب أجهزة ترشيح الرسائل الاقتحامية. ولذلك أصبحت الحاجة ملحّة لوضع إطار تقني فعَّال من أجل التصدي للمشكلة العالمية للرسائل الاقتحامية.

وقد تستعمِل الحلول المختلفة المقاومة للرسائل الاقتحامية تقنيات مختلفة في مكافحتها، وما لبثت تتطوَّر هذه التكنولوجيات. ومن العسير جداً التوصل إلى وصف ثابت يشمل جميع تفاصيل التكنولوجيات المقاومة للرسائل الاقتحامية على المدى الطويل.

ولذلك، من الضروري وضع إطار مفتوح يشتمل على مختلف هذه الحلول. وينبغي أن يكون هذا الإطار متوافقاً مع جميع التكنولوجيات المقاومة للرسائل الاقتحامية، وألا يقتصر على تفصيل تقني محدَّد. ومتطلبات الإطار كما يلي:

- أن يتمكن منهجياً من أن يقدِّر ما إذا كان البريد الإلكتروني عبارة عن رسالة اقتحامية أم لا.
- أن يمكِّن مختلف أنظمة خدمات البريد الإلكتروني من تبادل معلومات مكافحة الرسائل الاقتحامية فيما بينها.
- أن يتمكن من تحسين مصداقية أدوات مكافحة الرسائل الاقتحامية في أنظمة خدمات البريد الإلكتروني.
- أن يضمن تبادل الكيانات في مختلف الميادين الإدارية للمعلومات الخاصة بمكافحة الرسائل الاقتحامية.

التوصيـــة ITU-T X.1241

الإطار التقني لمكافحة الرسائل الاقتحامية عبر البريد الإلكتروني

1 مجال التطبيق

تقدم هذه التوصية إطاراً تقنياً لمكافحة الرسائل الاقتحامية. ويصف هذا الإطار بنية واحدة موصى بها لميدان معالجة مقاوم للرسائل الاقتحامية والوظيفة المحددة لكل وحدة من الوحدات النموذجية الرئيسية فيه. والنقطة الأساسية للإطار هي أنه يؤسس الآلية لتبادل المعلومات عن الرسائل الاقتحامية بين مختلف مخدمات البريد الإلكتروني. وسوف تحسن الأنظمة التي تتبع هذا الإطار من كفاءتها من خلال التوصيل البيني.

2 المراجع

لا يوجد.

3 تعاريف

1.3 المصطلحات المعرَّفة في مواضع أخرى

تستعمل هذه التوصية المصطلحات التالية المعرَّفة في مواضع أخرى:

1.1.3 حقول الرأسية [b-IETF RFC 2822]: تتمتع حقول الرأسية بنفس البنية التركيبية العامة: اسم حقل تتبعه نقطتان يتبعه متن الحقل.

2.1.3 أغراض البريد [b-IETF RFC 2821]: يُنقَل غرض البريد بواسطة البروتوكول البسيط لنقل البريد (SMTP). وهو يشمل غلافاً ومحتوى.

2.3 مصطلحات معرَّفة في هذه التوصية

تعرِّف هذه التوصية المصطلحات التالية:

1.2.3 ميدان معالجة مقاوم للرسائل الاقتحامية: نظام مستقل يحتوي على كيان معالجة مقاوم للرسائل الاقتحامية وكيانات فرعية للمعالجة مقاومة للرسائل الاقتحامية ومخدِّمات بريد إلكتروني وعملاء بريد إلكتروني.

2.2.3 كيان المعالجة المقاوم للرسائل الاقتحامية: الكيان المركزي في ميدان المعالجة المقاوم للرسائل الاقتحامية. فهو يجمع المعلومات عن الرسائل الاقتحامية من كيانات المستويات الأدنى، ومن ثم يقوم ببناء نظام قواعد متجانس ومتكامل. وأخيراً، ينبغي تقديم نظام القواعد إلى جميع الكيانات الواقعة في المستويات الأدنى.

3.2.3 الكيان الفرعي للمعالجة المقاوم للرسائل الاقتحامية: كيان فرعي موصول بواحد أو أكثر من مقدِّمي خدمات البريد الإلكتروني. وهو يتلقَّى معلومات عن الرسائل الاقتحامية من مخدِّمات البريد الإلكتروني أو من تجهيزات مكافحة الرسائل الاقتحامية ويبلِّغ هذه المعلومات إلى الكيانات في المستوى الأعلى بعد تحليلها دورياً. كما يتلقَّى أيضاً قواعد التحديث من كيانات المستوى الأعلى دورياً ويوزِّع هذه القواعد على الكيانات الفرعية.

4.2.3 القاعدة المركَّبة: تتألف من قاعدتين بسيطتين أو أكثر.

5.2.3 البريد الإلكتروني: يُستعمَل هذا المصطلح بالدرجة الرئيسية للإشارة إلى البريد الإلكتروني المرسَل عبر شبكة اتصالات.

6.2.3 الرسائل الاقتحامية: يُستعمَل المصطلح لوصف الرسائل الإلكترونية غير المطلوبة عبر البريد الإلكتروني والتي تُرسَل عادةً لأغراض محدَّدة.

7.2.3 القاعدة: مجموعة من الشروط والإجراءات الأساسية. وتشتمل القواعد على أشكال عديدة، مثل أساليب التصرف وأجهزة الترشيح وغير ذلك.

8.2.3 عيّنة بريد إلكتروني: يُستعمَل المصطلح لوصف أي بريد إلكتروني يتم استلامه من مخدِّمات البريد الإلكتروني وفقاً لقواعد معيَّنة.

9.2.3 مرسل الرسائل الاقتحامية: يستخدم هذا المصطلح لوصف الكيان أو الشخص الذي يولد الرسائل الاقتحامية ويرسلها.

4 الاختصارات والأسماء المختصرة

تستعمل هذه التوصية الاختصارات والأسماء المختصرة التالية:

DNS نظام أسماء الميادين (*Domain Name System*)

E-mail بريد إلكتروني (*electronic mail*)

ESMTP البروتوكول البسيط الموسَّع لنقل البريد (*Extended Simple Mail Transfer Protocol*)

FTP بروتوكول نقل الملفات (*File Transfer Protocol*)

HTTP بروتوكول نقل النصوص على الشبكة (*Hypertext Transfer Protocol*)

IMAP4 الصيغة 4 من بروتوكول النفاذ إلى الرسائل عبر الإنترنت (*Internet Message Access Protocol v4*)

IP بروتوكول الإنترنت (*Internet Protocol*)

POP3 الصيغة 3 من بروتوكول مكتب البريد (*Post Office Protocol v3*)

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

SASL طبقة الاستيقان والأمن البسيطة (*Simple Authentication and Security Layer*)

SMTP البروتوكول البسيط لنقل البريد (*Simple Mail Transfer Protocol*)

URL موقع الموارد الموحد (*Uniform Resource Locator*)

5 اصطلاحات

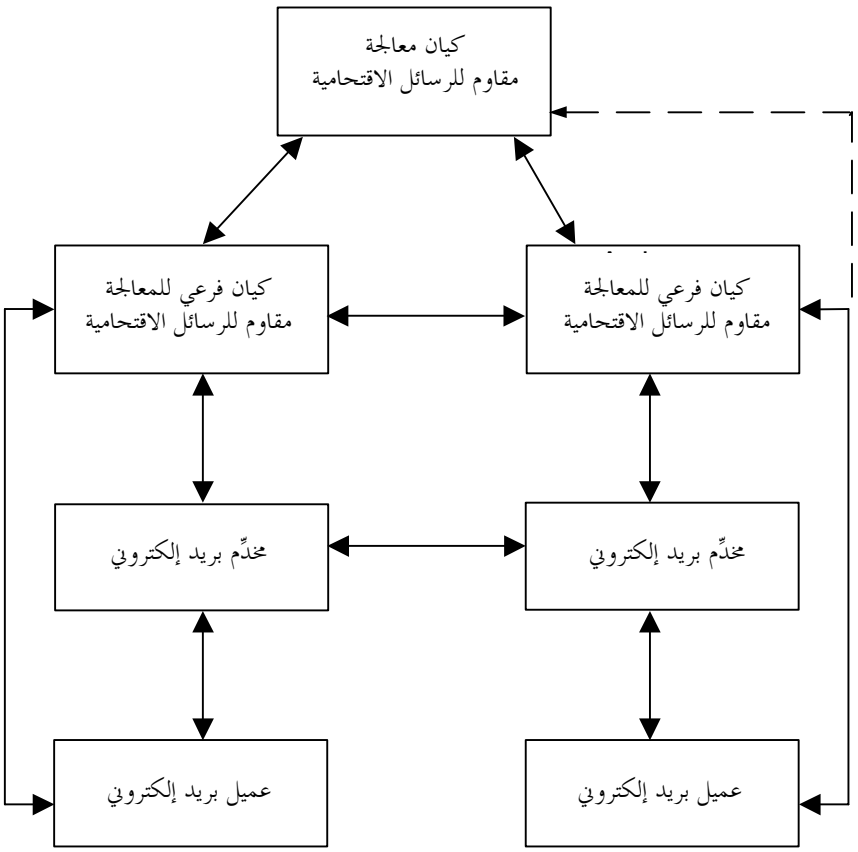
لا يوجد.

6 البنية العامة لميدان المعالجة المقاوم للرسائل الاقتحامية

1.6 البنية العامة

تصف هذه التوصية مكونات الإطار. ويشتمل الإطار على كيان معالجة مقاوم للرسائل الاقتحامية وكيانات فرعية للمعالجة مقاومة هي الأخرى للرسائل الاقتحامية ومخدِّمات بريد إلكتروني وعملاء بريد إلكتروني.

وبإمكان هذه المكونات الاتصال فيما بينها باستعمال بروتوكولات الرسائل الشائعة. ويرد أدناه في هذا القسم وصف لخصائص هذه المكونات.



ملاحظة – يمثل الخط المستمر مسير المعلومات المتبادلة بين مكونات ميدان المعالجة المقاوم للرسائل الاقتحامية.

الشكل 1 – البنية العامة

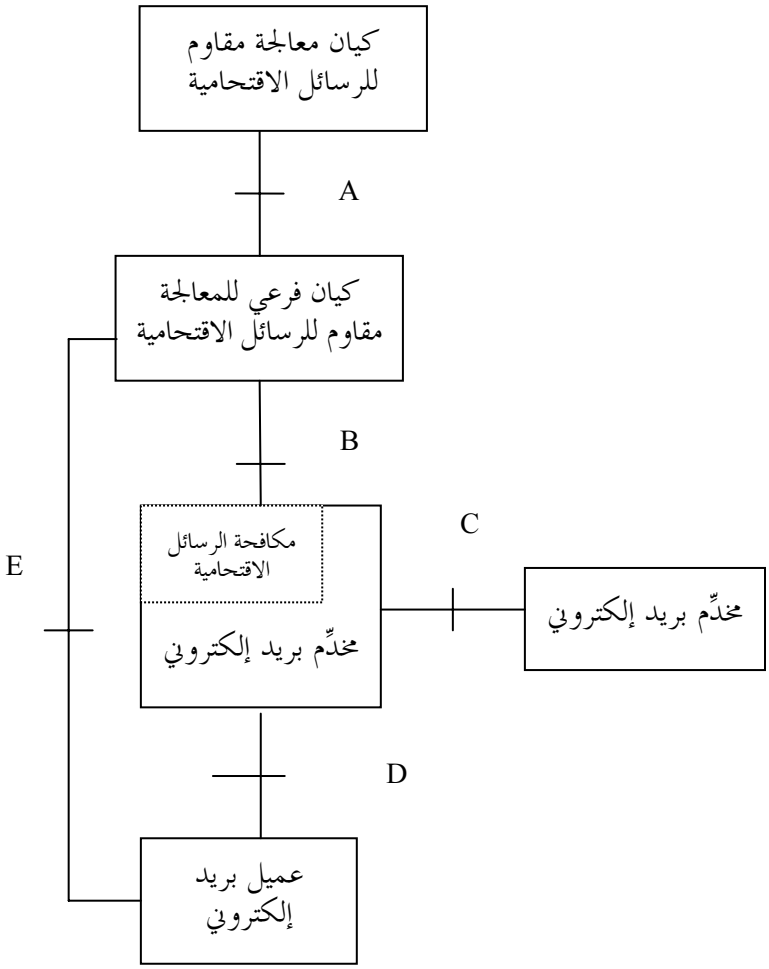
في الشكل 1، يتلقَّى كيان المعالجة المقاومة للرسائل الاقتحامية تقاريراً من الكيانات الفرعية للمعالجة المقاومة للرسائل الاقتحامية ويبعث إليها بقواعد جديدة.

ويتعيَّن على الكيانات الفرعية للمعالجة المقاومة للرسائل الاقتحامية أن تتحقق من سلامة القواعد التي تأتيها من كيان المعالجة المقاوم للرسائل الاقتحامية والعمل على صقلها.

وعميل البريد الإلكتروني هو الكيان الذي يتعامل معه العملاء مباشرة. ويقوم مخدِّم البريد الإلكتروني بتسليم هذا البريد في شبكة الاتصالات القائمة على بروتوكول الإنترنت.

ويُرسِل عميل البريد الإلكتروني الشكاوى إلى الكيان الفرعي للمعالجة المقاوم للرسائل الاقتحامية. وفي حالات محددة، يستطيع عميل البريد الإلكتروني أن يُرسِل شكاواه مباشرةً من خلال كيان المعالجة الرئيسي المقاوم للرسائل الاقتحامية.

2.6 نموذج مرجعي



الشكل 2 – نموذج مرجعي

يقع السطح البيني A بين كيان المعالجة المقاوم للرسائل الاقتحامية والكيان الفرعي. وتُرسَل تقارير الشكاوى وقواعد مكافحة الرسائل الاقتحامية عبر السطح البيني A. ويمكن أن تكون القواعد مركَّبة من قبيل "IP + URL المصدر". وينبغي للسطح البيني A أن يدعم بروتوكول FTP وبروتوكول HTTP.

ويقع السطح البيني B بين الكيان الفرعي للمعالجة المقاوم للرسائل الاقتحامية ومخدِّم البريد الإلكتروني. وهو يُستعمَل لإرسال تقارير الشكاوى والقواعد. وبالمثل، يمكن أن تكون القواعد مركَّبة من قبيل "IP + URL المصدر". وينبغي للسطح البيني B أن يدعم بروتوكول FTP وبروتوكول HTTP. وفي حالات محددة، يمكن لمخدِّم البريد الإلكتروني أن يتصل مباشرةً بكيان المعالجة الرئيسي المقاوم للرسائل الاقتحامية.

يقع السطح البيني C بين مخدمات البريد الإلكتروني وترسل الرسائل عبره باستخدام البروتوكول SMTP.

ويقع السطح البيني D بين مخدم البريد الإلكتروني وعميله. ويمكن استخدام بروتوكولات متنوعة لنقل البريد الإلكتروني، مثل POP3 وIMAP4.

ويقع السطح البيني E بين عميل البريد الإلكتروني والكيان الفرعي للمعالجة المقاوم للرسائل الاقتحامية. ويستطيع عميل البريد الإلكتروني إرسال شكاواه إلى الكيان الفرعي للمعالجة المقاوم للرسائل الاقتحامية. وفي حالات محددة، يمكن لعميل البريد الإلكتروني أن يُرسِل شكاواه مباشرةً إلى كيان المعالجة الرئيسي المقاوم للرسائل الاقتحامية. ويمكن في هذا السطح البيني استعمال الويب على الخط والهاتف والبريد الإلكتروني وبرمجية العميل.

7 وظائف ميدان المعالجة المقاوم للرسائل الاقتحامية

1.7 وظائف عميل البريد الإلكتروني

تشمل وظائف عميل البريد الإلكتروني ما يلي:

- بالإضافة إلى القيام بالوظائف العامة لإرسال البريد الإلكتروني، يوفر عميل البريد الإلكتروني آلية تساعد المستعملين على إرسال معلومات شكوى بشأن رسائل اقتحامية إلى كيان المعالجة المقاوم للرسائل الاقتحامية. والأمر منوط فقط بمتلقِّي البريد الإلكتروني لتحديد ما إذا كان ذلك البريد رسالة اقتحامية أم لا من حيث المحتوى أو عنوان الموضوع أو عنوان البريد الإلكتروني. فإذا لم يرغب متلقي البريد مثلاً في استلام إعلانات أو منشورات إلكترونية أو مواد دعائية، فإن بإمكانه إرسال شكوى من هذه الأنواع من البريد إلى كيان المعالجة المقاوم للرسائل الاقتحامية بواسطة آلية عميل البريد.
- بإمكان عميل البريد الإلكتروني تحميل قواعد ترشيح الرسائل الاقتحامية أوتوماتياً من كيان المعالجة المقاوم لهذه الرسائل. وتوضع قواعد الترشيح تبعاً لتقارير الشكاوى من عملاء البريد الإلكتروني. وهي تشمل حدود حجم الرسالة الإلكترونية الواحدة وعدد الرسائل التي تُرسَل في فترة معيَّنة من الزمن والكلمات الرئيسية في متن الرسائل، وغير ذلك. وهي تحدَّث دورياً طبقاً لتقارير الشكاوى، كما أنها تُفهرس بحسب اسم مستعمل صندوق البريد وعنوان خرج بروتوكول الإنترنت واسم الميدان.
- بإمكان عميل البريد الإلكتروني إحالة رسالة اقتحامية إلى كيان المعالجة المقاوم للرسائل الاقتحامية لمزيد من المعالجة أو لسحب بعض قواعد الترشيح التي تتسبَّب في ردود إيجابية كاذبة. وبإمكان كيان المعالجة تحديث قواعد الترشيح فوراً تبعاً للاحتياجات أو للشكوى من عميل البريد الإلكتروني.
- يمكن لعميل البريد الإلكتروني أن يقوم بترشيح الرسائل الاقتحامية مباشرةً. وينبغي لمتلقي البريد عادةً معرفة نتائج الترشيح تجنباً لمشكلة الردود الإيجابية الكاذبة.

2.7 وظائف مخدِّم البريد الإلكتروني

تشمل وظائف مخدِّم البريد الإلكتروني ما يلي:

- عندما يقوم مخدِّم البريد الإلكتروني بالوظائف العامة لإرسال البريد الإلكتروني فإنه يستكمل الإجراءات الاعتيادية لتبادل البريد مع مخدِّم بريد آخر أو إرسال واستلام البريد بين عملاء هذا البريد الإلكتروني، وفي الوقت ذاته ينبغي لمخدِّم البريد منع وظيفة الترحيل المفتوح لكي يحول دون قيام المقتحمين بالتحايل عليها لإرسال الرسائل الاقتحامية إلى مخدِّم بريد آخر.
- يجب على أي عميل أن يجتاز امتحان التحقق قبل أن يرسل أي بريد إلكتروني من مخدِّم هذا البريد. وقد تلجأ أنظمة البريد الإلكتروني المختلفة إلى استعمال آليات تحقق مختلفة. وتُستخدم عملية التحقق بين مخدِّم البريد وعميل البريد.
- يجوز لأي مورد خدمات بريد إلكتروني أن يحتفظ بقائمة سوداء بشأن المقتحمين، وتشمل القائمة السوداء بعض المعلومات عن المقتحمين (مثل اسم المضيف أو اسم الميدان أو عنوان البريد الإلكتروني)، ومن ثم يرفض مخدِّم البريد الإلكتروني تلقِّي الرسائل القادمة من هؤلاء المقتحمين.
- قد يعيد مخدِّم البريد الإلكتروني إرسال أمر تحقق إلى المصدر، المبيَّن في معلومات مرسِل البريد (مثل نظام أسماء الميادين أو اسم المضيف أو غيرها)، فإذا لم يؤكد أمر التحقق الاستيقان من المصدر، فإن مخدِّم البريد سوف يرفض ذلك البريد.
- قد يعمد المقتحمون إلى استعمال بعض أوامر البروتوكول البسيط لنقل البريد (SMTP) لتخمين اسم الحساب الحقيقي لمخدِّم البريد الإلكتروني. وينبغي لهذا الأخير أن يبطل الأوامر من قبيل EXPN وVRFY.

- تستمر بعض جهات الإعلان والدعاية في إرسال رسائل إلكترونية دون أي معلومات عن المرسِل. وينبغي لمخدِّم البريد الإلكتروني أن يضيف أوتوماتياً الوصلة HTTP في متن البريد. وبإمكان العملاء تقديم تقارير شكاوى بسهولة ويسر.
- تكتشف مخدمات البريد الإلكتروني الرسائل الاقتحامية بواسطة تكنولوجيا مكافحة هذه الرسائل وتقوم بالإبلاغ عنها إلى الكيان الفرعي للمعالجة المقاوم للرسائل الاقتحامية وتقوم بتحميل قواعد الترشيح منه.
- عندما يتم الكشف عن رسالة اقتحامية، ينبغي لمخدِّم البريد تخزين الرسالة الاقتحامية الأصلية التي تتضمن على الأقل رأسية البريد المصدر ويبعث بهذا البريد إلى جهاز الترشيح.
- ينبغي لمخدِّم البريد توفير معلومات سجل النظام والمعلومات الإحصائية الخاصة به والتي يتم تخزينها احتياطياً دورياً وإرسالها إلى الكيان الفرعي للمعالجة المقاوم للرسائل الاقتحامية.
- يعيد مخدِّم البريد رقم حالة مختلف تبعاً لقواعد مختلفة.
- يمكن لمخدِّم البريد أن يقيد من حجم الحركة المرسلة من عميل بريد إلكتروني محدد.

3.7 وظائف كيان المعالجة المقاوم للرسائل الاقتحامية

تشمل وظائف كيان المعالجة المقاوم للرسائل الاقتحامية ما يلي:

- تبادل قواعد الترشيح مع كيانات المعالجة الأخرى، ويمكن استعمال بروتوكولات مختلفة لإرسال المعلومات، مثل بروتوكول FTP وبرتوكول HTTP.
- تخزين المعلومات الأصلية للرسائل الاقتحامية المرسلة من العملاء ومن الكيان الفرعي للمعالجة.
- بث قواعد الترشيح إلى الكيانات الفرعية للمعالجة والمقاومة للرسائل الاقتحامية وتحذيرها من الرسائل الخطرة.
- ينبغي لكيان المعالجة إدارة قواعد الترشيح والحفاظ عليها، ويمكن الحصول على هذه القواعد من خلال موقع الويب من أجل:
  - استلام التقارير من العملاء ومن الكيانات الفرعية للمعالجة.
  - بث المعلومات الرسمية، بما في ذلك معلومات الإشراف والإدارة.

4.7 وظائف الكيان الفرعي للمعالجة المقاوم للرسائل الاقتحامية

تشمل وظائف الكيان الفرعي للمعالجة المقاوم للرسائل الاقتحامية ما يلي:

- استلام تقارير الشكاوى من العملاء وقواعد الترشيح من كيان المعالجة.
- تخزين المعلومات الأصلية الخاصة بالرسائل الاقتحامية الواردة من العملاء (على الأقل رأسية الرسالة الاقتحامية) ومن الكيانات الأخرى.
- بث قواعد الترشيح إلى مخدِّمات البريد أو عملاء البريد وتحذير مستعملي البريد من الرسائل الخطرة، إذا لزم الأمر.
- تعقُّب انتشار الرسائل الاقتحامية وجمع المعلومات المتصلة بذلك.
- الإبلاغ عن حالة انتشار رسائل اقتحامية والمعلومات المتصلة بذلك إلى الكيانات في المستوى الأعلى.
- استحداث قواعد ترشيح جديدة انطلاقاً من المخزون الاحتياطي للبريد المشتبه به والتحقق من قواعد الترشيح القائمة وتعديلها، ويمكن الحصول على هذه القواعد من خلال موقع الويب من أجل:
  - استحداث تقارير عن الرسائل الاقتحامية من العملاء ومن مخدِّم البريد.
  - استحداث قواعد ترشيح جديدة.

8 التعرف على الرسائل الاقتحامية

يصف هذا القسم الخصائص والمعايير الشائعة للرسائل الاقتحامية.

1.8 الخصائص الشائعة للرسائل الاقتحامية

تدرج فيما يلي بعض الخصائص الشائعة للرسائل الاقتحامية:

- إخفاء العنوان الصحيح للمرسِل أو تزييفه

  إدراج فراغ أو محتوى باطل إزاء "from" أو "sender" في حقل المصدر.

- إخفاء المصدر الحقيقي للبريد أو تزييفه

  إدراج فراغ أو محتوى باطل في حيّز "message-id" في حقل تعرف الهوية.

- المرسِل مقتحِم معروف

  إدراج عنوان مقتحِم وارد في القائمة السوداء إزاء "from" أو "sender" في حقل المصدر.

- معلومات مستلم كاذبة

  المحتوى المدرج في حقل المستلم ("to") أو حقل مستلم نسخة طبق الأصل ("cc") كاذب أو يتعلق بمقتحمين.

- احتواء كلمات شائعة يستعملها المقتحمون

  كلمات شائعة يستعملها المقتحمون واردة في حقل الموضوع ("subject") أو في محتوى البريد.

- معلومات ترحيل كاذبة

  المحتوى الوارد في "resent-from" أو "Resent-Sender" في حقل إعادة الإرسال كاذب.

- معلومات تعقُّب كاذبة

  محتوى مضلِّل وارد في حقل التعقُّب.

- الحجم غير ملائم

  حجم مجمل الرسالة، أو حقل الرأسية أو محتوى البريد مماثل لحجم حقول الرأسية ومحتوى الرسائل الاقتحامية.

- عدد مفرط من المستلمين

  هنالك عدد مفرط من المستلمين في حقل معيَّن.

- عدد مفرط من قفزات إعادة الإرسال

  هنالك عدد مفرط من علامات التعقب في حقل التعقُّب.

- عنوان بروتوكول الإنترنت للمرسل مدرج في بعض الحقول

  معلومات تتعلق بمقتحمين مدرجة في "from" أو "sender" في حقل المصدر.

- عنوان بروتوكول الإنترنت لمخدم البريد مدرج في بعض الحقول

  معلومات تتعلق بمقتحمين في "received" في حقل التعقُّب أو في "resent-from" أو "resent-sender" في حقل إعادة الإرسال.

- رسالة اقتحامية جديدة

  يمكن لكيان المعالجة المقاوم للرسائل الاقتحامية أن يلخِّص الخصائص من العينة الجديدة للرسالة الاقتحامية وأن يستحدث قواعد الترشيح المقابلة لذلك.

2.8 المعايير المشتركة لمكافحة الرسائل الاقتحامية

يمكن تضمين قواعد إفرادية في قاعدة مركَّبة على أساس أولوية مختلفة.

يمكن لمخدِّم البريد أن يطبِّق قاعدة إفرادية و/أو مركَّبة للتعامل مع الرسائل الاقتحامية.

1.2.8 القواعد الأساسية المشتركة

يمكن لمخدِّم البريد الإلكتروني أن يضع معاييراً وفقاً للعوامل التالية:

- حقل المصدر ("from" أو "sender") فراغ أو من محتوى غير صحيح.
- حقل تعرُّف الهوية ("message-id") فراغ أو به محتوى غير صحيح.
- حقل المصدر ("from" أو "sender") يحتوي كلمات رئيسية مدرجة في القائمة السوداء.
- الكلمات الرئيسية الواردة في القائمة السوداء مدرجة في حقل المستلم ("to") أو حقل مستلم النسخة طبق الأصل ("cc").
- يحتوي حقل الموضوع ("subject") أو محتوى البريد على كلمات رئيسية معيَّنة.
- لا يمكن العثور على المصدر الأصلي الحقيقي في "resent-from" و"Resent-Sender" في حقل إعادة الإرسال أو في محتوى حقل التعقُّب.
- حجم مجمل الرسالة أو حقل الرأسية أو محتوى الرسالة يساوي قيمةً معيَّنة (تقريباً).
- العدد الإجمالي للعناوين المحددة في "to" و"cc" و"bcc" في حقل المصدر يتجاوز الحد الذي وضعه مخدِّم البريد، أو عدد مرات تسليم بريد واحد يتجاوز الحد الذي وضعه مخدِّم البريد.
- عدد حالات التعقُّب في حقل التعقُّب يتجاوز الحد الذي وضعه مورد خدمة البريد أو مدير هذا الميدان.
- نتيجة البحث العكسي في نظام أسماء الميادين (DNS) عن معلومات "from" أو "sender" في حقل المصدر مدرجة في القائمة السوداء المحددة.
- نتيجة البحث العكسي في نظام أسماء الميادين (DNS) التي ينبغي أن تتبع "received" في حقل التعقُّب أو "resent-from" أو "resent-sender" في حقل إعادة الإرسال مدرجة في قائمة سوداء محددة.
- إذا لم يتسن التعرُّف على الرسالة الاقتحامية باستعمال قاعدة واحدة، عندئذٍ يجب استعمال قاعدة مركَّبة.

2.2.8 أولوية المعايير

لا بد من تأكيد أولويات المعايير. عندما يمتثل بريد إلكتروني واحد لعدة قواعد (ما يعرف باسم تعارض القواعد)، فإنه يعامل طبقاً للقاعدة بالأولوية الأعلى. وإذا كانت أولويات القواعد متساوية، تنتقى القاعدة المستعملة في آخر المطاف بموجب مبدأ تعارض الأولويات. وينبغي تجنب التعارض قدر الإمكان.

3.2.8 الكشف عن تعارض المعايير

تُستعمَل هذه الوظيفة للكشف عن حالات التعارض بين مختلف المعايير المخصصة. وفيما يلي وصف لأحوال التعارض المألوفة:

- "شروط القاعدة" للمعيارين تشمل نفس النوع من "قواعد بسيطة" (قواعد أساسية) في صنف البحث عن الكلمات الرئيسية (من قبيل "الموضوع يشمل XXX"، أو "ما يتم تفكيك شفرته من الأسطر العشرة الأولى يتضمن XXX" وهكذا)، وأن تكون الكلمات الرئيسية في "القواعد البسيطة" لكلا المعيارين هي نفسها وأن تضم الكلمة الرئيسية لأحدهما الكلمة الرئيسية للآخر.
- أن تشمل "شروط القاعدة" للمعيارين نفس النوع من "القواعد البسيطة" للصنف المقيَّد ببروتوكول الإنترنت (مثل "بروتوكول الإنترنت لدى العميل هو XXX" وهكذا)، وفراغات بروتوكول الإنترنت المحددة في "القواعد البسيطة" لكلا المعيارين متماثلة أو لديها مجموعة تقاطع.

- أن تشمل "شروط القاعدة" للمعيارين نفس النوع من "القواعد البسيطة" من الصنف المحدَّد بالحجم، والشروط المحدَّدة بالحجم تطابق الشكل "حجم XXX هو القيمة المحددة" (لا يمكن أن تكون "أكبر من" أو "أصغر من")، والقيم متماثلة. كأن تشتمل القاعدتان مثلاً على نفس القاعدة البسيطة: "حجم نص البريد الإلكتروني يساوي 5343 بايتة".

9 طرائق مكافحة الرسائل الاقتحامية

من الطرائق الرئيسية لمكافحة الرسائل الاقتحامية إبطال وظيفة 'الترحيل المفتوح' في مخدِّم البريد الإلكتروني والسيطرة على عملية التصريح بتسليم البريد، وتقنيات الترشيح. وينبغي لنظام مكافحة الرسائل الاقتحامية أن يدعم، حكماً أو خيارياً، الطرائق التالية.

1.9 إبطال وظيفة 'الترحيل المفتوح'

تعني وظيفة 'الترحيل المفتوح' أن مخدِّم البريد الإلكتروني يرحِّل جميع البريد الوارد، بصرف النظر عما إذا كان مرسلو البريد أو مستلموه هم العملاء المقررين. وعموماً، إذا قام مخدِّم البريد الإلكتروني بتفعيل وظيفة الترحيل غير المحدود، فإنه يعتبر في حالة ترحيل مفتوح.

2.9 التحكم في عملية التصريح بتسليم البريد الإلكتروني

منعاً لقيام العملاء غير المرخَّص لهم من استعمال مخدِّم البريد الإلكتروني،

- يجب أن يكون المرسلون عملاء شرعيين لدى المخدِّم.
- ينبغي للمخدم التحقق من عناوين IP للمرسل.
- تقييد عدد قفزات البريد الإلكتروني لمنع انتشار الرسائل الاقتحامية بصورة أسية.
- يمكن للمخدم تفحص مصدر الرسالة للتأكد من حقيقتها.

3.9 تقنية الترشيح

يمكن تقسيم تكنولوجيا الترشيح إلى صنفين: ترشيح عناوين بروتوكول الإنترنت والترشيح من خلال مسح النصوص.

1.3.9 ترشيح عناوين بروتوكول الإنترنت

بإمكان ترشيح عناوين بروتوكول الإنترنت تقييد التوصيل ببروتوكول SMTP في نظام البريد الإلكتروني. ومن السمات الرئيسية لهذه التقنية تحديد مدى بروتوكول الإنترنت وأساليب التقييد.

ويشمل مدى بروتوكول الإنترنت:

- مدى بروتوكول الإنترنت في الوقت الفعلي من كيان المعالجة المقاوم للرسائل الاقتحامية.
- مدى بروتوكول الإنترنت في الوقت الفعلي من قواعد الترشيح لدى منظمات أخرى.
- مدى بروتوكول الإنترنت في الوقت الفعلي المضاف في حد ذاته.

وتشمل أساليب التقييد:

- رفض التوصيل
- السماح بالتوصيل غير المشروط
- ينبغي تقييد عدد مرات التوصيل المتكرر من بروتوكول الإنترنت لدى أحد العملاء بمخدِّم البريد الإلكتروني بفترة زمنية معيَّنة.

فإذا كان بروتوكول الإنترنت لدى أحد العملاء ينتمي إلى نطاق بروتوكول الإنترنت المعني، عندئذٍ تُعتمَد أساليب التقييد.

2.3.9 الترشيح من خلال مسح النصوص

يمكن لمخدِّم البريد الإلكتروني وضع قواعد الترشيح وتحميلها من كيان المعالجة المقاوم للرسائل الاقتحامية. ويمكن للمديرين تعديل قواعد الترشيح في ظروف معيَّنة.

فعندما تتطابق رسالة ما مع قاعدة معنية، فإنها تُفرَز طبقاً لتصرف محدد. ومن هذه التصرفات الخاصة بقواعد مسح النصوص ما يلي:

- الرفض: إعادة الرسالة المرفوضة إلى المرسِل بعد استخلاص الخصائص.
- الاستبعاد: الاستجابة الاعتيادية لكل أمر لا ينطوي على تصرف.
- التسليم: التسليم الاعتيادي. يهمل الإسقاط بعد انتقاء التسليم.
- الوسم: إضافة العلامة المحدَّدة في الرأسية.
- التبليغ: التبليغ عن الخصائص المستخلصة من الرسالة إلى مركز التبليغ.
- الاحتجاز: الاحتفاظ بالرسالة كاملة قدر الإمكان والتبليغ بنسخة منها إلى كيان المعالجة المقاوم للرسائل الاقتحامية.

4.9 اختبار إمكانية تعقُّب البريد الإلكتروني

يتعذَّر أحياناً معرفة ما إذا كان المرسِل عميلاً فعلياً. ولأن من المستحيل للمخدِّم مستلم البريد الحصول على جميع المعلومات عن مخدِّم مرسِل البريد، فإن مخدِّم مستلم البريد لا يمكنه التحقق من جميع المعلومات بالنسبة للعملاء المشروعين.

ويمكن تقسيم البريد الإلكتروني إلى نوعين: البريد القابل للتعقُّب والبريد غير القابل للتعقُّب. ويتم إخضاع البريد المشتبه فيه القابل للتعقُّب لقواعد الترشيح إذا كانت الإنذارات لا تستنزف مجهوداً. ومن العسير التخلص من البريد المشتبه فيه غير القابل للتعقب لأنه يستعمل عادةً مصدر بريد إلكتروني مزيفاً. ومعظم البريد غير القابل للتعقُّب هو في الأساس بريد مشتبه فيه ومن ثم تعتبر عملية اختبار إمكانية التعقب هي أساس مكافحة الرسائل الاقتحامية. ويقترح اتباع الخطوات الثلاث التالية:

الخطوة الأولى: المطلوب

- معظم مخدِّمات استلام البريد (ما يسمى "MX" في اسم الميدان) تكون أيضاً مخدِّمات إرسال بريد.
- معظم المخدِّمات المنفصلة إلى مخدِّمات استلام ومخدِّمات إرسال لها بروتوكولات إنترنت متجاورة.
- قد يكون للحواسيب الأخرى التي يُسمح لها بتسليم البريد بروتوكولات إنترنت متجاورة مع مخدِّمات البريد "MX".
- من الممكن التعرُّف على بعض مخدِّمات البريد بأسلوب البحث العكسي في نظام أسماء الميادين (DNS)، وفي هذه الحالة تكون النتيجة هي نفس النتيجة التي يدعيها العميل.

الخطوة الثانية: آلية ملاحظة إمكانية التعقُّب

دعم عملية التحقق بشأن شبكة الاتصالات:

- التحقق من أن حقل البريد الخاص بالمرسل مسموح به.
- التحقق من أن المرسِل عميل مشروع لحقل البريد.

الخطوة الثالثة: آلية التعقُّب العكسي

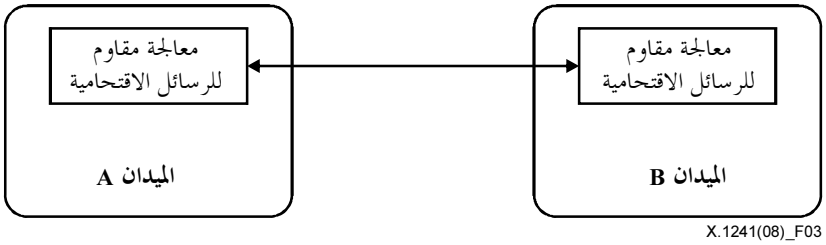
- تشكِّل الخدمة القابلة للتعقب والاختبار القابل للتعقب سلسلة التعقُّب العكسي.
- لا يمكن تزييف سلسلة التعقُّب العكسي.
- من السهل التمييز بين الجزء المزيف والجزء الأصلي.

بمقدور نظام التعقُّب القيام بعملية التحري أوتوماتياً بواسطة سلسلة التعقُّب العكسي.

10 التوصيل البيني بين ميادين المعالجة المقاومة للرسائل الاقتحامية

عندما توصل ميادين المعالجة المقاومة للرسائل الاقتحامية بعضها بالبعض، من الممكن الاختيار من بين ثلاثة أساليب: التوصيل البيني بين كيانات المعالجة الرئيسية، والتوصيل البيني بين كيانات المعالجة وكيانات المعالجة الفرعية، والتوصيل البيني بين كيانات المعالجة الفرعية ومخدمات البريد الإلكتروني. ولكل خيار بعض السيناريوهات أو المتطلبات.

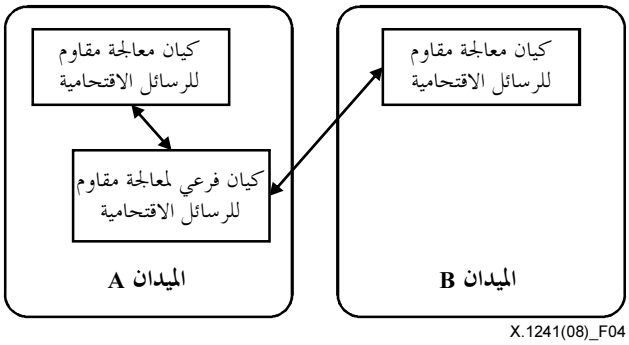
1.10 التوصيل البيني بين كيانات المعالجة الرئيسية



الشكل 3 – التوصيل البيني بين كيانات المعالجة الرئيسية

يعد أسلوب التوصيل البيني هنا بمثابة توصيل ثنائي الاتجاه بين كياني معالجة رئيسيين. وهنالك قواعد محددة يجري تبادلها بين الكيانين. فإذا تلقَّى أحد الكيانين معلومات من الكيان الآخر، فإنه يقوم بتنفيذ آليات معيَّنة وإجراءات معينة لانتقاء القواعد المفيدة من المعلومات المستلمة.

2.10 التوصيل البيني بين كيان المعالجة والكيان الفرعي للمعالجة

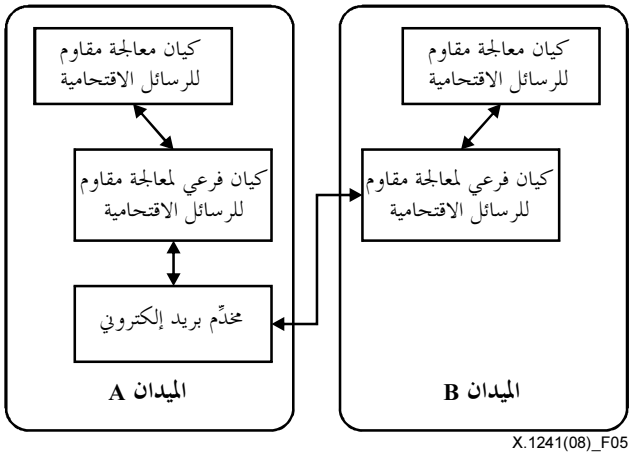


الشكل 4 – التوصيل البيني بين كيان المعالجة والكيان الفرعي للمعالجة

هذا الأسلوب من التوصيل البيني عبارة عن توصيل ثنائي الاتجاه بين كيان معالجة وكيان فرعي للمعالجة. وينبغي للكيان الفرعي تحميل جدولين من قواعد الترشيح من كياني المعالجة. ويستحدث الكيان الفرعي قواعداً وفقاً للبريد المشتبه به الوارد من المخدِّمات المتصلة به. وينبغي عليه تبليغ القواعد إلى الكيانين.

ويتسم هذا الأسلوب بقدر من الأمن. ولكنه يقوم على علاقة إدارية معقَّدة بين الكيان الفرعي والكيانين. وقد يواجه هذا الأسلوب مشكلات من حيث قابلية الاتساع. فهو ليس توصيلاً بينياً شاملاً بين الميادين.

3.10 التوصيل البيني بين كيان فرعي للمعالجة ومخدِّم بريد إلكتروني



الشكل 5 – التوصيل البيني بين كيان فرعي للمعالجة ومخدِّم بريد إلكتروني

هذا الأسلوب من التوصيل البيني عبارة عن توصيل ثنائي الاتجاه بين كيان فرعي للمعالجة ومخدِّم بريد إلكتروني. ويقوم مخدِّم البريد الإلكتروني بتحميل قواعد الترشيح الخاصة بالرسائل الاقتحامية من الكيان الفرعي ويبلِّغ عن البريد المشتبه فيه إلى الكيان الفرعي في الميدان الآخر. ويتلقَّى الكيان الفرعي تقاريراً عن البريد المشتبه فيه من مخدِّم البريد الإلكتروني وينشر القواعد الخاصة به على مخدِّم الميدان الآخر.

وهذا الأسلوب ميسور التحقيق بين الميادين. ولكن قد تهاجم المخدِّمات خارج الميدان ميدان المعالجة المقاوم للرسائل الاقتحامية، لذلك قد يعاني هذا الأسلوب من بعض مشكلات الأمن. كما يعاني أيضاً من مشكلات من حيث قابلية الاتساع. ولذلك، فإنه ليس توصيلاً بينياً شاملاً بين الميادين. والأسلوب المحدد في الفقرة 1.10 هو أسلوب التوصيل البيني المؤمن والموصى به.

ثبت المراجع

[b-IETF RFC 1869] IETF RFC 1869 (1995), *SMTP Service Extensions.* <http://www.ietf.org/rfc/rfc1869.txt>

[b-IETF RFC 1939] IETF RFC 1939 (1996), *Post Office Protocol – Version 3.* <http://www.ietf.org/rfc/rfc1939.txt>

[b-IETF RFC 2060] IETF RFC 2060 (1996), *Internet Message Access Protocol – Version 4rev1.* <http://www.ietf.org/rfc/rfc2060.txt>

[b-IETF RFC 2222] IETF RFC 2222 (1997), *Simple Authentication and Security Layer (SASL).* <http://www.ietf.org/rfc/rfc2222.txt>

[b-IETF RFC 2505] IETF RFC 2505 (1999), *Anti-Spam Recommendations for SMTP MTAs.* <http://www.ietf.org/rfc/rfc2505.txt>

[b-IETF RFC 2554] IETF RFC 2554 (1999), *SMTP Service Extension for Authentication.* <http://www.ietf.org/rfc/rfc2554.txt>

[b-IETF RFC 2821] IETF RFC 2821 (2001), *Simple Mail Transfer Protocol.* <http://www.ietf.org/rfc/rfc2821.txt>

[b-IETF RFC 2822] IETF RFC 2822 (2001), *Internet Message Format.* <http://www.ietf.org/rfc/rfc2822.txt>

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 والأمن**
السلسلة Y	البنية التحتية العالمية للمعلومات وملامح بروتوكول الإنترنت وشبكات الجيل التالي
السلسلة Z	اللغات والجوانب العامة للبرمجيات في أنظمة الاتصالات

طُبعت في سويسرا
جنيف، 2009