الاتحـ ـاد الـدولـ ـي للاتصـ ـ ـالات

ITU-T M.3016.3

قطـاع تقييس الاتصـالات
في الاتحاد الدولي للاتصالات

(2005/04)

السلسلة M: إدارة الاتصالات، بما في ذلك شبكة إدارة الاتصالات (TMN) وصيانة الشبكات

شبكة إدارة الاتصالات

أمن مستوي الإدارة: آليات الأمن

التوصية ITU-T M.3016.3

الاتحاد الدولي للاتصالات

ITU-T

توصيات السلسلة M لقطاع تقييس الاتصالات

إدارة الاتصالات، بما في ذلك شبكة إدارة الاتصالات (TMN) وصيانة الشبكات

مقدمة ومبادئ عامة بشأن الصيانة وتنظيمها	M.10 - M.299
أنظمة الإرسال الدولية	M.300 - M.559
الدارات الهاتفية الدولية	M.560 - M.759
أنظمة التشوير على قناة مشتركة	M.760 - M.799
أنظمة الإبراق الدولية وإرسال الصور برقياً	M.800 - M.899
وصلات الزمر والزمر الثانوية المؤجرة الدولية	M.900 - M.999
الدارات الدولية المؤجرة	M.1000 - M.1099
أنظمة وخدمات الاتصالات المتنقلة	M.1100 - M.1199
الشبكة الدولية للهواتف العمومية	M.1200 - M.1299
الأنظمة الدولية لإرسال المعطيات	M.1300 - M.1399
تبادل التسميات والمعلومات	M.1400 - M.1999
شبكة النقل الدولية	M.2000 - M.2999
شبكة إدارة الاتصالات	**M.3000 - M.3599**
الشبكات الرقمية متكاملة الخدمات	M.3600 - M.3999
أنظمة التشوير على قناة مشتركة	M.4000 - M.4999

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

أمن مستوي الإدارة: آليات الأمن

ملخص

تحدد هذه التوصية آليات تحقيق أمن مستوي الإدارة في شبكة إدارة الاتصالات. وتركز تحديداً على الجانب الأمني لمستوي إدارة عناصر الشبكة (NE) وأنظمة الإدارة (MS) التي تشكل جزءاً من البنية الأساسية للاتصالات.

المصدر

وافقت لجنة الدراسات 4 (2005-2008) لقطاع تقييس الاتصالات بتاريخ 13 أبريل 2005 على التوصية ITU-T M.3016.3 بموجب الإجراء المحدد في التوصية A.8.

تمهيد

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

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

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

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

ملاحظة

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

والتقيد بذه التوصية اختياري. غير أنها قد تضم بعض الأحكام الإلزامية (بدف تأمين قابلية التشغيل البيني والتطبيق مثلاً). ويعتبر التقّيد بذه التوصية حاصلاً عندما يتم التقّيد 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 التقّيد بذه 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).

جدول المحتويات

الصفحة

مقدمة

الاتصالات بنية أساسية بالغة الأهمية للاتصالات والاقتصاد العالميين. ومن الضروري توفير الأمن اللازم لوظائف الإدارة التي تتحكم في هذه البنية. وتوجد معايير كثيرة لتحقيق أمن إدارة شبكات الاتصالات. ومع ذلك، فإن التقيد بذه المعايير متدن، وعمليات تطبيقها لا تتفق مع مختلف مكونات المعدات والبرمجيات المستخدمة في الاتصالات. وتحدد هذه التوصية آليات أمنية لإفساح المال أمام الجهات البائعة، والوكالات، ومقدمي الخدمات لتنفيذ بنية أساسية آمنة لإدارة الاتصالات. وعلى الرغم من أن هذه المموعة من آليات الأمن تمثل الفهم الحالي لآخر ما تم التوصل إليه في هذا المال، فإن التكنولوجيات ستتقدم والظروف ستتغير. ومن أجل تكليل هذه التوصية بالنجاح، يجب أن تكون قابلة للتطور بحسب ما تقتضيه الظروف. والغرض من هذه التوصية هو الاستناد إليها كأساس. ويمكن أن يدرج مقدمو الخدمات آليات أمنية إضافية لتلبية احتياجاتم الخاصة علاوة على تلك التي ترد في هذه التوصية.

وهذه التوصية هي جزء من توصيات السلسلة M.3016.x الصادرة عن قطاع تقييس الاتصالات (ITU-T) والرامية إلى تقديم إرشادات ونصائح بشأن تأمين مستوي إدارة الشبكات المتطورة، وهي:

التوصية ITU-T M.3016.0 - *أمن مستوي الإدارة: نظرة عامة.*

التوصية ITU-T M.3016.1 - *أمن مستوي الإدارة: متطلبات الأمن.*

التوصية ITU-T M.3016.2 - *أمن مستوي الإدارة: خدمات الأمن.*

التوصية ITU-T M.3016.3 - *أمن مستوي الإدارة: آليات الأمن.*

التوصية ITU-T M.3016.4 - *أمن مستوي الإدارة: نموذج الملامح العامة.*

التوصية ITU-T M.3016.3

أمن مستوي الإدارة: آليات الأمن

1 مجال التطبيق

تحدد التوصيات M.3016.3-M.3016.1 الصادرة عن قطاع تقييس الاتصالات (ITU-T) مجموعة من المتطلبات والخدمات والآليات الرامية إلى تحقيق الأمن الملائم للوظائف الإدارية اللازمة لدعم البنية الأساسية للاتصالات. وبالنظر إلى ما تحتاجه الإدارات والمنظمات المختلفة من مستويات دعم متباينة في ميدان الأمن، لا تحدد هذه التوصيات (M.3016.3-M.3016.1) ما إذا كانت هذه المتطلبات/الخدمات/الآليات إلزامية أم اختيارية.

وتحدد هذه التوصية آليات الأمن اللازمة لمستوي الإدارة في شبكة إدارة الاتصالات. وتركز تحديداً على الجانب الأمني لمستوي إدارة عناصر الشبكة (NE) وأنظمة الإدارة (MS) التي تشكل جزءاً من البنية الأساسية للاتصالات.

وتتسم هذه التوصية بطابع تنوعي ولا تحدد آليات الأمن اللازمة لسطح بيني معين تابع لشبكة إدارة الاتصالات (TMN) أو تتطرق إلى هذه الآليات.

والصيغ الشكلية المحددة في التوصية M.3016.4 الصادرة عن قطاع تقييس الاتصالات (ITU-T) هي صيغ مقدمة لمساعدة المنظمات والإدارات وسائر المنظمات الوطنية/الدولية في تحديد الدعم الإلزامي أو الاختياري للمتطلبات إلى جانب تحديد مدى القيم، والقيم ذاتها، غير ذلك، من أجل مساعدة هذه المنظمات والإدارات على تنفيذ سياساتها الأمنية.

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، نحث جميع المستعملين لهذه التوصية على السعي إلى تطبيق أحدث طبعة للتوصيات 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.

- التوصية ITU-T G.8080/Y.1304 (2001)، *معمارية الشبكة البصرية المبدلة أوتوماتياً (ASON)*، زائداً التعديل 2 (2005).
- التوصية ITU-T M.3010 (2000)، *المبادئ المتعلقة بشبكة إدارة الاتصالات.*
- التوصية ITU-T M.3016.0 (2005)، *أمن مستوي الإدارة: نظرة عامة.*
- التوصية ITU-T M.3016.2 (2005)، *أمن مستوي الإدارة: خدمات الأمن.*
- التوصية ITU-T M.3016.3 (2005)، *أمن مستوي الإدارة: آليات الأمن.*
- التوصية ITU-T M.3016.4 (2005)، *أمن مستوي الإدارة: نموذج الملامح العامة.*
- التوصية ITU-T X.509 (2000)، *تكنولوجيا المعلومات - التوصل البيني للأنظمة المفتوحة: الدليل: أطر التصديق العمومية الرئيسية وتصديق النعوت*، زائداً التصويب 1 (2001) والتصويب 2 (2002) والتصويب 3 (2004).
- التوصية ITU-T X.800 (1991)، *معمارية الأمن المطبقة في التوصيل البيني للأنظمة المفتوحة والمستخدمة في تطبيقات اللجنة الاستشارية الدولية للبرق والهاتف (CCITT)*، زائداً التعديل 1 (1996).
- التوصية ITU-T X.805 (2003)، *معمارية أمن الأنظمة التي توفر اتصالات من طرف إلى طرف.*

3 التعاريف

لا تحدد هذه التوصية أية مصطلحات جديدة.

4 المختصرات

تستعمل هذه التوصية المختصرات التالية:

CORBA المعمارية الشائعة لبرمجيات نقل الطلبات إلى الهدف *(Common Object Request Broker Architecture)*

DoS رفض الخدمة *(Denial of Service)*

EMS نظام إدارة العناصر *(Element Management System)*

FTP بروتوكول نقل الملفات *(File Transfer Protocol)*

HTTP بروتوكول نقل النصوص الفائقة *(Hypertext Transfer Protocol)*

IETF فريق مهام هندسة الإنترنت *(Internet Engineering Task Force)*

IP بروتوكول الإنترنت *(Internet Protocol)*

IPSec أمن بروتوكول الإنترنت *(Internet Protocol Security)*

ISO/IEC المنظمة الدولية للتوحيد القياسي /اللجنة الكهرتقنية الدولية
(International Organization for Standardization/International Electrotechnical Commission)

ITU-T الاتحاد الدولي للاتصالات – قطاع تقييس الاتصالات
(International Telecommunication Union – Telecommunication Standardization Sector)

MS نظام الإدارة؛ سواء كان نظام إدارة العناصر (EMS)، أم نظام إدارة الشبكة (NMS)، أم نظام دعم التشغيل (OSS)[1] *(Management System; any EMS, NMS, or OSS)*

NE عنصر الشبكة *(Network Element)*

NE/MS عنصر الشبكة (NE) أو نظام الإدارة (MS) *(NE or MS)*

NMS نظام إدارة الشبكة *(Network Management System)*

NTP بروتوكول تحديث الوقت الإجرائي في الشبكة *(Network Time Protocol)*

NTPv3 الصيغة 3 من بروتوكول تحديث الوقت الإجرائي في الشبكة *(NTP version 3)*

OAM & P التشغيل والإدارة والصيانة والتوريد *(Operations, Administration, Maintenance and Provisioning)*

OS نظام تشغيل *(Operating System)*

OSS نظام دعم التشغيل *(Operations Support System)*

RFC طلب أبداء تعليقات *(Request for Comments)*

SAML لغة التشفير المتداولة في توكيد الأمن *(Security Assertion Markup Language)*

SNMP البروتوكول البسيط لإدارة الشبكة *(Simple Network Management Protocol)*

SNMPv3 الصيغة 3 من البروتوكول البسيط لإدارة الشبكة *(Simple Network Management Protocol version 3)*

SOAP البروتوكول البسيط للنفاذ إلى الهدف *(Simple Object Access Protocol)*

SSH برنامج شل للدخول الآمن *(Secure Shell)*

SSL طبقة مقابس الأمن *(Secure Socket Layer)*

TCP بروتوكول التحكم في الإرسال *(Transmission Control Protocol)*

---

[1] يمكن عموماً استخدام تعبير أنظمة دعم التشغيل (OSS) في نفس سياق استخدامه على أنه أنظمة إدارة (MS) أو أي طبقة من تراتب شبكة إدارة الاتصالات.

TLS أمن طبقة النقل *(Transport Layer Security)*

TMN شبكة إدارة الاتصالات *(Telecommunications Management Network)*

XML لغة تشفير قابلة للتوسيع *(Extensible Markup Language)*

5 الاصطلاحات

يستعمل في التوصيات M.3016.1 وM.3016.2 وM.3016.3 الصادرة عن قطاع تقييس الاتصالات (ITU-T) واصف يحدد مختلف المتطلبات والخدمات والآليات. ويتألف هذا الواصف من وسم واحد من الوسوم التالية المكونة من ثلاثة أحرف متبوعاً برقم، وهي:

- REQ ويستعمل لوصف المتطلب؛
- SER ويستخدم لوصف الخدمة؛
- MEC ويستعمل لوصف الآلية.

6 آليات الأمن

يضم هذا البند آليات أمنية معينة معنية بتحقيق الأمن في مجال التشغيل والإدارة والصيانة والتوريد (OAM&P) ونظام دعم التشغيل (OSS) بوصفها آليات تنطبق تحديداً على أمن مستوي إدارة البنية الأساسية، والخدمات، والتطبيقات.

والجدول 1 الوارد أدناه هو جدول منسوخ من التوصية M.3016.0 الصادرة عن قطاع تقييس الاتصالات (ITU-T) (الجدول 4 في التوصية المذكورة (M.3016.0)). وهو يعطي نظرة عامة عن العلاقة القائمة بين المتطلبات والخدمات الأمنية، وهو جدول يشكل أساساً لتنظيم سائر التوصيات المنتمية إلى هذه السلسلة. وتناقش مثلاً التوصية M.3016.1 الصادرة عن قطاع تقييس الاتصالات (ITU-T) المتطلبات الوظيفية للأمن، بينما تناقش التوصية M.3016.2 الصادرة عن نفس القطاع (ITU-T) خدمات الأمن، وتناقش هذه التوصية (M.3016.3 الصادرة عن ذات القطاع (ITU-T)) آليات أمنية محددة مقابلة لخدمات الأمن.

ولا يحدد هذا البند سوى خدمات الأمن المشمولة بحلول قياسية؛ ولا يحسب حساب الخدمات الأخرى المحتملة (مثل الكشف عن رفض الخدمة).

الجدول 1/التوصية M.3016.3 – تقابل متطلبات الأمن وخدماته

المتطلب الوظيفي للأمن	الخدمة الأمنية
التحقق من الهويات	استيقان المستعمل استيقان كيان الند استيقان مصدر المعطيات
النفاذ والترخيص المراقبان	مراقبة النفاذ
حماية السرية - المعطيات المخزونة	سرية مراقبة النفاذ
حماية السرية - المعطيات المنقولة	السرية
حماية تكاملية المعطيات - المعطيات المخزونة	مراقبة النفاذ
حماية تكاملية المعطيات - المعطيات المنقولة	التكاملية
المسؤولية	عدم الإنكار
تسجيل الأنشطة	تسجيل التدقيق
الإبلاغ عن إنذارات الأمن	إنذار أمني
تدقيق الأمن	تسجيل التدقيق
حماية شبكة تبادل المعطيات (DCN)	تفتيش الرزم

ويبين الجدول 2 تنظيم هذا البند:

الجدول 2/التوصية M.3016.3 – تنظيم البند 6

البند	المحتويات
1.6	يناقش آليات الأمن المطبقة في مجال الاستيقان التي تشمل استيقان المستعمل، واستيقان كيان الند.
2.6	يناقش استيقان مصدر المعطيات.
3.6	يناقش آليات الأمن المطبقة في مجال مراقبة النفاذ.
4.6	يناقش آليات الأمن المتعلقة بسرية المعطيات.
5.6	يناقش آليات الأمن المتعلقة بتكاملية المعطيات.
6.6	يناقش آليات الأمن المطبقة في مجال تسجيل التدقيق

1.6 استيقان المستعمل

استيقان المستعمل هو إجراء التحقق من هوية يزعمها شخص ما. وقد يستند هذا الاستيقان إلى آليات أمنية تشمل ما يلي:

- توليفة تجمع بين معرف هوية (ID) المستعمل وكلمة السر (مع كلمات السر المركبة بشكل ملائم) حيث يمكن أن تكون كلمة السر كلمة تستعمل لمرة واحدة (مثل معرف الهوية (ID) الآمن).
- استيقان متعدد العوامل.
- استيقان الدخول الأحادي.

وترد في هذا البند مناقشة لآليات الأمن المطبقة في مجال استيقان المستعمل.

1.1.6 الاستيقان من معرف هوية (ID) المستعمل وكلمات السر

يمكن استعمال معرف هوية (ID) المستعمل وكلمات السر من أجل استيقان المستعمل. وينطوي هذا الاستيقان على إثبات الهوية الحقيقية للمستعمل الشرعي للنظام وردع الهجمات التنكرية التي يشنها منتحلو الشخصيات غير الشرعيين على النظام. ويتسنى بموجب الاستيقان الصحيح تتبع الأنشطة وتطبيق مراقبة النفاذ لفرض قيود على المستعملين بشأن الاضطلاع بالأنشطة أو أداء الأدوار المُرخص بها مسبقاً على غرار المناقشة الواردة في البند 2.6.

وينطوي استيقان معرف هوية (ID) المستعمل وكلمات السر على تخصيص معرف هوية (ID) وحيد لكل فرد من المستعملين، ومن ثم تُخصص كلمة سر مركبة بشكل ملائم تستخدم بالتزامن مع معرف هوية (ID) المستعمل لإثبات الهوية.

وينبغي أن تضم كلمات السر ما يكفي من السمات وغيرها من الرموز المرتبة عشوائياً للحيلولة دون تخمينها من جانب الأشخاص أو بواسطة التقنيات المؤتمتة آلياً. وقد تشتمل الأمثلة المتعلقة بخصائص كلمات السر المركبة على متطلبات من قبيل ما يلي:

MEC 1: قد يُشترط أن يكون الحد الأدنى لعدد سمات كلمة السر بطول معين (مثل ثماني سمات).

MEC 2: يجوز رفض كلمات السر الحاوية على سمات معينة.

MEC 2a: قد تُمنع كلمات السر من أن تحوي معرف هوية (ID) مكرر أو معكوس لمعرف هوية (ID) المستعمل المصاحب.

MEC 2b: قد يُشترط ألا تتضمن كلمات السر مجموعة من تتابعات السمات المشكلة في أي موضع داخلها (مثل الكلمات المأخوذة من القواميس أو أسماء المنتجات).

MEC 3: قد يُشترط ألا تضم كلمات السر أكثر من عدد معين من نفس السمات المستعملة بالتتابع.

MEC 4: قد يُشترط أن تحوي كلمات السر عدداً معيناً على الأقل من سمات ألفا بحالة أدنى و/أو سمات ألفا بحالة أعلى.

MEC 5: قد يُشترط أن تتضمن كلمات السر عدداً معيناً على الأقل من السمات الرقمية.

MEC 6: قد يُشترط أن تحوي كلمات السر عدداً معيناً على الأقل من السمات الخاصة.

وإدارة كلمات السر مهمة أيضاً للغاية لضمان إقامة نظام آمن للاستيقان. وقد يُرغب مثلاً في الاستفادة من القدرات الواردة أدناه في مجال إدارة النظام المعني بكلمات السر، وهي:

MEC 7: قد يتطلب نظام إدارة كلمات السر إدخال كلمة السر القديمة لمنع مستعمل آخر من تغيير كلمة سر يستخدمها مستعمل غيره في الدخول من دون علم الأخير.

MEC 8: يمكن أن يتحقق النظام أوتوماتياً من كلمة السر ليضمن أن تكون كل كلمة سر جديدة تستعمل في الدخول تختلف عن سابقتها. (نظراً إلى أن كلمات السر عادة ما تُخزن بواسطة التجفير باتجاه واحد، فإن إدخال كلمة السر القديمة قد يكون ضرورياً أيضاً لإفساح المال أمام النظام لتحديد درجة الاختلاف بين كلمتي السر القديمة والجديدة[2]).

MEC 9: يمكن أن يقدم النظام الدعم لقائمة معينة بكلمات السر بحسب التسلسل الزمني للحيلولة دون استعمال هذه الكلمات مجدداً.

MEC 10: يمكن أن يلزم النظام المستعمل بتغيير كلمات السر بعد انقضاء فترات زمنية معينة.

MEC 11: يمكن للنظام، بعد إجراء المستعمل لعدد معين من المحاولات غير الصحيحة لاستعمال كلمة السر، بتقييد إجراء المزيد من هذه المحاولات لفترة زمنية معينة (مثل 60 دقيقة) أو بفرض حالة إغلاق على المستعمل. وقد يكون المستعمل الذين يعاني من هذه الحالة بحاجة إلى الاتصال بموظفي إدارة الأمن لإزالتها.

2.1.6 الاستيقان المتعدد العوامل

يشير الاستيقان المتعدد العوامل إلى عملية استيقان تتطلب نوعين أو أكثر من مختلف أنواع المعلومات أو العوامل لإثبات هوية المستعمل بغرض استيقانه. ويعزز طلب العديد من العوامل أمن نظام الاستيقان من خلال عدم اعتماد الاستيقان حصراً على عامل واحد يمكن أن يكون تزويره أسهل.

وتشتمل عوامل الاستيقان التي تستعمل عادة في أنظمة الاستيقان المتعدد العوامل من المستعمل على ما يلي:

شيء **يعرفه** المستعمل: مثل معرفته كلمة سر أو عبارة سرية معينة.

شيء معين **بحوزة** المستعمل: مثل إذنة، بطاقة ذكية، مولد كلمات سر تستعمل لمرة واحدة.

شيء **متأصل** في المستعمل: مثل بصمة الأصبع أو غيرها من قياسات السمات البيولوجية.

وتتمثل الآلية الشائعة للاستيقان المتعدد العوامل في الاستيقان المكون من عاملين، الذي يتطلب تقديم وثيقتي اعتماد من أجل الاستيقان. وثمة مثال نموذجي على هذا الاستيقان يتمثل في نظام البطاقات المصرفية حيث يجب أن تكون البطاقة بحوزة مستعمل هذا النظام وأن يثبت أيضاً معرفته برقم الهوية الشخصية (PIN) السري المقترن بالبطاقة.

MEC 12: الاستيقان المتعدد العوامل بعدد محدد من العوامل.

3.1.6 استيقان مستعمل الدخول الأحادي

يمكن أن يقدم استيقان المستعمل الدعم لطرائق رامية إلى تأمين الدخول الأحادي وتحقيق أمن البنية الأساسية للمفاتيح العمومية المشفوعة بشهادات المعيار X.509. وفيما يخص الدخول الأحادي الآمن، يواصل البروتوكول تحديه للكيان (الكيانات) من أجل الحصول على وثائق الاعتماد؛ ومع ذلك، فقد لا يضطر المستعمل إلى إدخال هذه الوثائق لأنها مخزونة بطريقة ما خزناً آمناً (مثل خزنها بأسلوب Kerberos). وتستعمل تقنيات الدخول الأحادي الآمن للتقليل من اضطرار النظام إلى استيقان المستعمل عدة مرات الأمر الذي يمكن أن يصبح فيه ذلك غير ملائم.

MEC 13: استيقان الدخول الأحادي.

---

[2] كاستثناء للتجفير باتجاه واحد، يمكن استعمال كلمات السر الفرة بالتناظر فيما يتعلق بكلمات السر التي هي بحاجة إلى إزالة التجفير منها من أجل استعمالها داخلياً أو بشكل انتقالي في اتصالات موثوقة من نظام إلى نظام أو في الدخول الأحادي.

2.6 استيقان الكيان الند ومصدر المعطيات

تستعمل آليات استيقان الكيان الند للتحقق من هوية مزعومة بين نظامين ندين. أما آليات الأمن المطبقة في مجال استيقان مصدر المعطيات فتستعمل لضمان تسلم الرسائل من النظام الذي يزعم أنه أرسلها. ويرتبط استيقان الكيان الند ارتباطاً وثيقاً باستيقان مصدر المعطيات، ويمكن أن يستندا إلى آليات أمنية تشمل ما يلي:

- آليات استيقان بالتجفير.
- آليات استيقان بمسير موثوق.

وترد في هذا البند مناقشة لهذه الآليات الأمنية المطبقة في مجال الاستيقان.

1.2.6 الاستيقان بالتجفير

تحقق آليات الاستيقان بالتجفير الاستيقان أثناء عمليات تبادل المعطيات بين الأنظمة (مثلاً، من نظام إلى نظام، من تطبيق إلى تطبيق)، وهي الأساس الذي يستند إليه في إجراء اتصالات خاصة مع الحفاظ على تكاملية المعطيات ككل. وأثناء عمليات تبادل المعطيات، يفسح الاستيقان الفر للكيان المرسل المال أمام مستلم الرسالة استيقان هوية المرسل (استيقان الكيان الند) والتثبت من مصدر الرسالة (استيقان مصدر المعطيات). وقد يكون استيقان الكيان الند ومصدر المعطيات داخل قناة اتصالات آمنة مستنداً إلى معلومات مجفرة مقترنة بكل رسالة لربط هوية الكيان المرسل بالرسالة. ويتحقق مستلم الرسالة من المعلومات الفرة المقدمة مع الرسالة للتثبت من الهوية الحقيقية للكيان المرسل.

وتشتمل تقنيات التجفير التي يمكن استعمالها في استيقان الكيان الند ومصدر المعطيات على تجفير المفاتيح العمومية، والتجفير المتناظر للمفاتيح، والشارات الرقمية، وتقنيات التظليل الرقمية).[3] ويمكن أن يكون الاستيقان الفر أحادي الاتجاه عندما يقتصر الاستيقان في هذه الحالة على طرف واحد من المحادثة، أو يمكن أن يكون ثنائي الاتجاه عندما يُستيقَنَ الطرفان على حد سواء. والاستيقان الأخير أكثر آمناً ويمكن الاستفادة منه في المساعدة على منع الهجمات الفعالة.

MEC 14: استيقان الكيان الند ومصدر المعطيات على أساس تجفير المفاتيح العمومية.

MEC 15: استيقان الكيان الند ومصدر المعطيات بالاستناد إلى التجفير المتناظر للمفاتيح.

MEC 16: استيقان الكيان الند ومصدر المعطيات القائم على شارات رقمية.

MEC 17: استيقان الكيان الند ومصدر المعطيات على أساس تقنيات التظليل الرقمية.

MEC 18: الاستيقان الفر ثنائي الاتجاه.

2.2.6 استيقان المستعمل بمسير موثوق

الاستيقان بمسير موثوق هو عبارة عن آلية أمنية يتم بموجبها تأمين جميع تفاعلات الاستيقان من نظام إلى نظام عبر مسير اتصالات آمن. ولا يمكن تنشيط هذه الآلية إلا من جانب النظام ولا يمكن تقليدها. ويمكن أن يكون المسير الموثوق مسيراً مادياً مخصصاً (كأن يكون مطرافاً موصولاً مباشرة بالنظام) أو مسيراً مجفراً يشمل حماية التكاملية والتكرار (مثل الشبكة التقديرية الخاصة لأمن بروتوكول الإنترنت (IPsec)، أو نفق طبقة مقابس الأمن/أمن طبقة النقل (SSL/TLS)، أو برنامج شل للدخول الآمن (SSH)).[4] انظر التذييل الأول للاطلاع على مناقشة بروتوكولات كل من أمن بروتوكول الإنترنت (IPsec) وطبقة مقابس الأمن/أمن طبقة النقل (SSL/TLS) وبرنامج شل للدخول الآمن (SSH).

MEC 19: استيقان الكيان الند ومصدر المعطيات على أساس مسير موثوق.

---

[3] المعيار T1.243-1995 الصادر عن المعهد الأمريكي للمعايير الوطنية، *التشغيل، والإدارة، والصيانة*.

[4] معدلة عن وثائق المركز الوطني لأمن الحاسوب، NCSC-TG-004-88، *مسرد مصطلحات أمن الحاسوب*، أكتوبر 1998 (متيسر على العنوان التالي http://csrc.nist.gov/SBC/PDF/NCSC-TG-004_COMPUSEC_Glossary.pdf).

3.6 مراقبة النفاذ

يمكن أن توفر شبكة إدارة الاتصالات (TMN) قدرات تكفل منع الأطراف الفاعلة من الحصول على سبيل للنفاذ إلى المعلومات أو الموارد غير المرخص لها بالنفاذ إليها. وتضمن آليات أمن مراقبة النفاذ أن يكون السماح بإدارة موارد أمن النظام مقصوراً على المستعملين المصرح لهم بذلك.

ويمكن أن تُوفر هذه الآليات من جانب نظام مركزي، وغالباً ما يتم الأمر بالاشتراك مع نظام الاستيقان. وقد تُستعمل مثلاً وحدة خدمة مركزية معينة للنفاذ عن بعد إلى نظام مستعمل المراقمة الداخلية (RADIUS) بالتزامن مع قاعدة معطيات خاصة بالبروتوكول الخفيف الوزن للنفاذ إلى الدليل (LDAP) لتوفير نظام مركزي معني بالاستيقان ومراقبة النفاذ.

ويمكن أن تتسم آليات الأمن المطبقة في مجال مراقبة النفاذ ببعض الخصائص التالية:

MEC 20: جميع الإجراءات الإدارية يمكن أن ترتبط بأفراد معينين.

MEC 21: يمكن أن تدعم آلية أمن مراقبة النفاذ الدعم مفهوم "التمتع بأقل الامتيازات" (أي، لا يكون لشخص معين دور ولا ترخيص بالاطلاع على المعطيات، أو تعديلها، أو استهلال إجراءات إدارية إلا فيما يتعلق بالوظائف التي يسمح هذا الدور بأدائها).

MEC 22: قد لا يُسمح على الأقل بإغلاق بعض حسابات الجهة القائمة على الإدارة بسبب الاضطلاع بأنشطة تتصل بكلمة السر من قبيل حالات فشل الدخول أو انقضاء المهل الزمنية.

MEC 23: يمكن تحديد عدد معين من أدوار الجهة القائمة على الإدارة، يحظى كل منها بدرجات من الامتياز فيما يتعلق بإجراءات إدارة الأمن البالغة الأهمية. فمثلاً، قد يحدد نظام ما خمسة أدوار للمستعمل التابع للجهة القائمة على الإدارة، بينما يمكن أن يحدد نظام آخر ثلاثة أدوار من هذا القبيل. ويمكن أن تُحدد الأدوار في أي من الحالتين لإفساح المال أمام التمتع بمختلف الامتيازات فيما يخص الإجراءات الأمنية الآتية:

MEC 23a: تحديد امتيازات المستعمل وتخصيصها.

MEC 23b: إضافة معرفات هوية (ID) المستعملين وحذفها.

MEC 23c: تشكيل كلمات السر المستخدمة في الدخول وإعادة تحديدها.

MEC 23d: تشكيل مفاتيح التجفير وتغييرها.

MEC 23e: ضبط عتبة تقادم النظام وفقاً لكلمات السر المستخدمة في الدخول إليه.

MEC 23f: ضبط حد الدخول إلى النظام على أساس عدد محاولات الدخول الفاشلة لكل معرف من معرفات هوية (ID) المستعمل.

MEC23g: إلغاء إغلاق النظام، أو تغيير قيمة مؤقت إغلاقه.

MEC 23h: ضبط قيمة مؤقت خمول النظام.

MEC 23i: تحديد تشكيلة التسجيل والإنذار بشأن أمن النظام.

MEC 23j: إدارة عمليات التسجيل المتعلقة بالأمن.

MEC 23k: تطوير برمجيات الأمن.

MEC 23l: إناء أية دورة من دورات المستعمل أو دورات النظام.

MEC 23m: تحديد وتخصيص امتيازات جديدة للمستعملين والموعات على مستوى التطبيق.

MEC 23n: حفظ سجل بجميع طلبات النفاذ إلى التطبيق.

MEC 23o: إضافة مستعملين وحذفهم على مستوى التطبيق.

MEC 23p: مراقبة جميع سجلات أمن التطبيق.

MEC 23q: تحديد تشكيلة التسجيل والإنذار بشأن أمن التطبيق.

MEC 23r: إدارة عمليات تسجيل أمن التطبيق.

MEC 23s: إناء أي دورة لمستعمل التطبيق.

4.6 سرية المعطيات

تُستعمل آليات أمن سرية المعطيات للحيلولة دون التلقي غير المصرح به. ويناقش هذا البند آليات أمنية مجفرة تؤمن سرية المعطيات.

وتستند هذه السرية إلى أسس تجفير معينة. ويستعمل التجفير خوارزميات خاصة قائمة على معايير معينة ومتيسرة عموماً الأمر الذي يتيح المجال بالتالي تدقيق تنفيذ هذه الخوارزميات وتيسيره على نطاق واسع. وتستند "قوة" التجفير إلى خوارزمية التجفير المستعملة، فضلاً عن حجم المفتاح المستخدم (أي، يشير تعبير القوة إلى الفترة الزمنية اللازمة للقيام من الناحية الهندسية بقلب (إيجاد أو تخمين) قيمة (قيم) المفتاح المستعمل بمعية خوارزمية معينة).

وتؤمن عادة البروتوكولات الأمنية (من قبيل أمن بروتوكول الإنترنت (IPsec) وطبقة مقابس الأمن (SSL)، وبرنامج شل للدخول الآمن/أمن طبقة النقل (TLS/SSH)) استيقان مصدر المعطيات وتكاملية المعطيات وسريتها. (انظر الملحق A للاطلاع على مناقشة بروتوكولات كل من أمن بروتوكول الإنترنت (IPsec) وطبقة مقابس الأمن/أمن طبقة النقل (SSL/TLS) وبرنامج شل للدخول الآمن (SSH)). وحالات توسيع نطاق الأمن ليضم بروتوكولات أخرى من قبيل الصيغة 3 من البروتوكول البسيط لإدارة الشبكة (SNMPv3)[5]، والمعمارية الشائعة لبرمجيات نقل الطلبات إلى الهدف (CORBA)، وبروتوكول بوابة الحدود، وبروتوكول المسير الأول المفتوح الأقصر، هي حالات يراد بها تأمين استيقان مصدر المعطيات وتكامليتها.

والطرائق المستخدمة في توليد وخزن وتوزيع وإتلاف وإلغاء مفاتيح التجفير التي تؤمن سرية المعطيات هي طرائق مهمة للغاية. وبالإضافة إلى ذلك، ترتبط عوامل من قبيل طول المفتاح، واختياره، وانتفاء الخوارزمية بصلة مباشرة مع مدى رصانة الأمن الذي يوفره نظام تجفير معين.

1.4.6 تأمين سرية المعطيات بالتجفير المتناظر

يشير تعبير التجفير المتناظر أو التجفير بمفاتيح سرية إلى نظام تجفير تكون فيه مفاتيح التجفير ومفاتيح إزالته متماثلة. وتتطلب أنظمة التجفير المتناظر إجراء ترتيبات أولية بخصوص تشارك الأفراد في مفتاح سري وحيد (مثل مفتاح التجفير). ويجب توزيع المفتاح على الأفراد باستخدام وسيلة آمنة، أو بوسيلة تُستنبط من الداخل (كأن تكون مستندة مثلاً إلى التشارك في مفتاح جذر سري) لأن معرفة مفتاح التجفير تدل ضمناً على معرفة مفتاح إزالته والعكس بالعكس.

وقد تستند الآليات الأمنية المطبقة في مجال تأمين سرية المعطيات إلى خوارزميات تجفير متناظر مثل معيار تجفير المعطيات (DES)، ومعيار التجفير المتقدم (AES)، والخوارزمية الثلاثية لتجفير المعطيات (3DES)، وغيرها من الخوارزميات.

ومعيار تجفير المعطيات (DES) هو عبارة عن خوارزمية تجفير متناظر مكونة من 56 بتة وهو قيد الاستعمال منذ سنوات عدة. ونظراً لقصر طول مفتاح هذا المعيار (DES)، فإنه معرض بشكل كبير لخطر استنزاف المفتاح بسبب تطبيقه كماً هائلاً من العمليات الحسابية المتوازية، وهو يعتبر الآن معياراً ضعيفاً. ويقلل المعهد الوطني الأمريكي للمعايير والتكنولوجيا (NIST) من أهمية هذا المعيار.

واختار المعهد المذكور (NIST) معيار التجفير المتقدم (AES) بوصفه الخوارزمية القياسية للتجفير المتناظر ليحل محل معيار تجفير المعطيات (DES) لاستعماله في التطبيقات التي تجريها حكومة الولايات المتحدة. ولهذا المعيار (AES) مفاتيح بأطوال 128 و192 و256 بتة.

والخوارزمية الثلاثية لتجفير المعطيات (3DES) هي أساساً خوارزمية معيار تجفير المعطيات (DES) المستعملة ثلاث مرات إما بمعية مفتاحين بطول 56 بتة أو ثلاثة مفاتيح بنفس الطول (56 بتة). وهذه الخوارزمية (3DES) محددة في المنشور 3-46 المتعلق بالمعايير الاتحادية لمعالجة المعلومات (FIPS)، *معيار تجفير المعطيات*، أكتوبر 1999، التذييل 2، الصفحة 22 (متيسر على العنوان التالي http://csirc.nist.gov/publications/fips/fips46-3/fips46-3.pdf).

---

[5] قد تؤمن أيضاً هذه الصيغة (SNMPv3) السرية.

ويمكن تطبيق هذه الخوارزمية (3DES) إما باستعمال مفتاحين مستقلين بطول 56 بتة أو ثلاثة مفاتيح مستقلة بطول 56 بتة، بحيث يمكن أن يتوقع لقوتا أن تبلغ في الحالتين 112 و168 بتة على التوالي. بيد أن هذه الخوارزمية عرضة لشن هجمة عليها "في منتصف الطريق"، الأمر الذي يمكن أن يُضعف قوتا في حال كانت مكونة من مفتاحين إلى 57 بتة فقط بدلاً من قوتا المتوقعة البالغة 112 بتة. وبمقدور نفس الهجمة أن تضعف قوة هذه الخوارزمية (3DES) عندما تكون مؤلفة من ثلاثة مفاتيح إلى 112 بتة فقط عوضاً عن قوتا المتوقعة بمقدار 168 بتة. ولذلك، ينبغي استعمال خوارزمية ثلاثية لتجفير المعطيات (3DES) مؤلفة من ثلاثة مفاتيح مستقلة من أجل تحقيق مستوى أعلى من الأمن، ويفترض أن تكون قوتا في أسوأ الحالات بمقدار 112 بتة .

ويمكن تطبيق خوارزمية معيار تجفير المعطيات (DES) بشكل سريع نسبياً بسبب قصر طول مفتاحها البالغ 56 بتة، بينما ينبغي أساساً أن تطبق الخوارزمية الثلاثية لتجفير المعطيات (3DES) معيار تجفير المعطيات (DES) ثلاث مرات وتكون بالتالي أبطأ. أما معيار التجفير المتقدم (AES)، الذي يكون الحد الأدنى لطول مفتاحه 128 بتة، فهو معيار أقوى من الخوارزمية (3DES) من حيث التجفير، وبالإمكان أيضاً تطبيقه بسرعة عالية داخل العتاديات والبرمجيات على حد سواء. ويمكن مثلاً معالجة تطبيق معيار التجفير المتقدم (AES) داخل البرمجيات بسرعة مماثلة تقريباً لسرعة معالجة تطبيق معيار تجفير المعطيات (DES) على نفس المنصة، ولكن بقوة تجفير تفوق بكثير قوة المعيار DES.

MEC 24: تأمين سرية المعطيات بالتجفير المتناظر بالاستناد إلى خوارزمية التجفير بمعيار تجفير المعطيات (DES).

MEC 25: تأمين سرية المعطيات بالتجفير المتناظر على أساس خوارزمية التجفير بمعيار التجفير المتقدم (AES).

MEC 26: تأمين سرية المعطيات بالتجفير المتناظر المستندة إلى خوارزمية تجفير ثلاثية لتجفير المعطيات (3DES).

2.4.6 تأمين سرية المعطيات بالتجفير غير المتناظر

نظام التجفير غير المتناظر هو نظام يرتبط فيه مفتاح التجفير بمفتاح إزالته ولكنهما يختلفان بعضهما عن بعض. ويكون أحد المفتاحين عمومياً، بينما يبقى الآخر سرياً. ويختلف المفتاح العمومي عن المفتاح الخاص، وليست هناك طريقة عملية معروفة لاستنباط المفتاح الخاص من العمومي. وتُوزع المفاتيح العمومية على نطاق واسع؛ غير أن المفاتيح الخاصة تبقى طي الكتمان دوماً.

وقد تستند الآليات الأمنية المطبقة في مجال تأمين سرية المعطيات إلى خوارزميات تجفير غير متناظر من قبيل خوارزمية التجفير Rivest Shamir Adleman (RSA)، وطريقة التجفير بمنحني إهليلجي (ECC)، وغيرهما من الخوارزميات.

وخوارزمية RSA هي خوارزمية تجفير غير متناظر مستخدمة بشكل شائع يمكن استعمالها في التجفير والشارات الرقمية. وهي تستند إلى الصعوبة الرياضية لتحليل كم هائل من الأعداد الأولية. والطولان الشائعان للمفاتيح المستخدمة في هذه الخوارزمية هما 1024 و2048 بتة. وتجدر الإشارة إلى أن قوة تجفير الخوارزمية RSA التي يبلغ طول مفتاحها 2048 بتة هي قوة مكافئة تقريباً لقوة التجفير المتناظر بمفتاح طوله 128 بتة.

أما طريقة التجفير بمنحني إهليلجي (ECC) فهي طريقة جديدة لتطبيق التجفير بمفتاح عمومي (أي، بالمقارنة مع الخوارزمية RSA). ويُحدد المنحني الإهليلجي في هذه الطريقة (ECC) عبر مجال معين؛ ومن ثم تُحل المسألة اللوغارتمية المنفصلة لهذا المنحني عبر هذا المجال. وتتمثل الميزة الرئيسية لهذه الطريقة (ECC) بمقارنتها مع سائر الخوارزميات التي تستعمل مفاتيح عمومية في حجم المفتاح. ويحقق مفتاح بطول 160 بتة يُستعمل في طريقة التجفير بمنحني إهليلجي (ECC) مستوى أمن مساو تقريباً لذلك الذي يحققه مفتاح بطول 1024 بتة يُستخدم في خوارزمية RSA، بينما يحقق مفتاح بطول 210 بتة يُستعمل في الطريقة ECC مستوى أمن مكافئ تقريباً للذي يحققه مفتاح بطول 2048 بتة في خوارزمية RSA. ويؤدي استعمال مفتاح أصغر في الطريقة ECC إلى تقليل التكاليف الحسابية الثابتة وزيادة كفاءة نظام التجفير.[6]

MEC 27: تأمين سرية المعطيات بالتجفير غير المتناظر المستند إلى خوارزمية التجفير Rivest Shamir Adleman (RSA) التي تستعمل مفتاح بطول معين.

---

[6] انظر *معيار الشارة الرقمية*، نوفمبر 2002، (متيسر على العنوان التالي http://csrc.nist.gov/cryptval/dss.htm) من أجل الاطلاع على تفاصيل إضافية عن خوارزمية التجفير Rivest Shamir Adleman (RSA)، وخوارزمية Diffie Hellman، وخوارزمية التجفير بمنحني إهليلجي (ECC).

MEC 28: تأمين سرية المعطيات بالتجفير غير المتناظر القائم على خوارزمية التجفير بمنحني إهليلجي (ECC) التي تستعمل مفتاح بطول معين.

3.4.6 سرية المعطيات - ملخص

ترد في الجدول 3 أمثلة على خوارزميات يمكن تطبيقها لتأمين سرية المعطيات. ويجب أيضاً مراعاة مسائل أخرى من قبيل الإنساق، والملء، ومعالجة حالات الخطأ، واختيار الأعداد الأولية المناسبة وحجم الأس العام الملائم، وفي حالة تطبيق طريقة التجفير بمنحني إهليلجي (ECC)، المال والمنحني الأساسيين؛ غير أن هذه المسائل لا تندرج ضمن نطاق هذه التوصية.

الجدول 3/التوصية M.3016.3 - خوارزميات تجفير نموذجية لتأمين سرية المعطيات

الفئة	الخوارزمية	التعليقات
خوارزميات تجفير متناظر	AES	معيار تجفير متقدم
	3-DES	خوارزمية ثلاثية لتجفير المعطيات
	DES	معيار تجفير معطيات
خوارزميات تجفير غير متناظر	RSA	Rivest، Shamir، Adleman
	ECC	تجفير بمنحني إهليلجي

5.6 تكاملية المعطيات

تُستعمل آليات أمن تكاملية المعطيات لضمان عدم تعديل المعطيات الموصلة.

وتستند هذه التكاملية إلى أسس تجفير معينة. ويستعمل التجفير خوارزميات خاصة قائمة على معايير معينة ومتيسرة عموماً الأمر الذي يفسح المال بالتالي أمام دقة تطبيق هذه الخوارزميات وسهولته على نطاق واسع. وتقدم عادة البروتوكولات الأمنية (مثل أمن بروتوكول الإنترنت (IPsec) وطبقة مقابس الأمن/أمن طبقة النقل (SSL/TLS) وبرنامج شل للدخول الآمن (SSH)) خدمات في مجال تأمين تكاملية المعطيات على أساس خوارزميات تجفير رئيسية بالإضافة إلى ما تقدمه من خدمات أمنية أخرى من قبيل تأمين سرية المعطيات واستيقان مصدرها. (انظر التذييل الأول للاطلاع على مناقشة بروتوكولات كل من أمن بروتوكول الإنترنت (IPsec) وطبقة مقابس الأمن/أمن طبقة النقل (SSL/TLS) وبرنامج شل للدخول الآمن (SSH)).

والطرائق المستخدمة في توليد وخزن وتوزيع وإتلاف وإلغاء مفاتيح التجفير التي تؤمن تكاملية المعطيات هي طرائق مهمة للغاية. وإضافة إلى ذلك، ترتبط عوامل من قبيل طول المفتاح، واختياره، وانتفاء الخوارزمية بصلة مباشرة مع مدى رصانة الأمن الذي يحققه نظام تجفير معين.

1.5.6 تأمين تكاملية المعطيات بالتجفير المتناظر

يشير تعبير تكاملية المعطيات بالتجفير المتناظر أو التجفير بمفاتيح سرية إلى نظام تجفير تكون فيه المفاتيح المستخدمة لتأمين تكاملية المعطيات متماثلة في الجهة المرسلة للمعلومات والجهة المستقبلة لها على حد سواء. وتتطلب أنظمة التجفير المتناظر إجراء ترتيبات أولية لتحقيق تشارك الأفراد في مفتاح سري وحيد (مثل مفتاح التحقق). ويجب توزيع المفتاح على الأفراد باستخدام أداة تأمين، أو بوسيلة تُستنبط من الداخل (كأن تكون مثلاً على أساس التشارك في مفتاح جذر سري).

وقد تستند آليات أمن تكاملية المعطيات بالتجفير المتناظر للرسائل العشوائية الأطوال إلى خوارزميات تستعمل مفاتيح بخصوص ملخصات الرسائل بالاقتران مع وظائف تظليل معينة. وتشمل الأمثلة المتعلقة بذه الخوارزميات خوارزمية شفرة استيقان الرسائل المظللة مع ملخص الرسالة 5 (HMAC-MD5-96)[7] وشفرة استيقان الرسائل المظللة مع خوارزمية التظليل الآمنة 1 (HMAC-SHA-1-96)[8].

---

[7] الطلب 2403 المقدم من فريق مهام هندسة الإنترنت (IETF) بشأن إبداء تعليقات، *استعمال الوظيفة HMAC-MD5-96 داخل ESP وAH*، C. Madson، R. Glenn، نوفمبر 1998.

[8] الطلب 2404 المقدم من فريق مهام هندسة الإنترنت (IETF) بشأن إبداء تعليقات، *استعمال الوظيفة HMAC-SHA-1-96 داخل ESP وAH*، C. Madson، R. Glenn، نوفمبر 1998.

MEC 29: تكاملية المعطيات بالتجفير المتناظر المستندة إلى خوارزمية التجفير بشفرة استيقان الرسائل المظللة مع ملخص الرسالة 5 (HMAC-MD5-96).

MEC 30: تكاملية المعطيات بالتجفير المتناظر القائمة على خوارزمية التجفير بشفرة استيقان الرسائل المظللة مع خوارزمية التظليل الآمنة 1 (HMAC-SHA-1-96).

2.5.6 تأمين تكاملية المعطيات بالتجفير غير المتناظر

نظام التجفير غير المتناظر المستعمل في تأمين تكاملية المعطيات هو نظام يرتبط فيه مفتاح التسجيل بمفتاح التحقق ولكنهما يختلفان بعضهما عن بعض. ويكون مفتاح التحقق عمومياً، بينما يبقى مفتاح التسجيل في طي الكتمان. ويختلف مفتاح التسجيل عن مفتاح التحقق، وليس هناك طريقة عملية معروفة لاستنباط الأول من الأخير. وتُوزع مفاتيح التحقق على نطاق واسع؛ غير أن مفاتيح التسجيل تبقى سرية دوماً.

وقد تستند الآليات الأمنية المطبقة في مجال تأمين تكاملية المعطيات إلى خوارزميات تجفير غير متناظر من قبيل خوارزمية الشارات الرقمية (DSA) وخوارزمية التجفير Rivest Shamir Adleman (RSA).

وبتطبيق الآليات الأمنية الرامية إلى تأمين تكاملية المعطيات بالتجفير غير المتناظر، تُسجل الجهة المرسلة ملخص الرسالة بواسطة مفتاح (خاص) للتسجيل بينما تستعمل الجهة المتلقية للرسالة المفتاح (العمومي) للتحقق بغية التثبت من تسجيل ملخص الرسالة من جانب المصدر الذي يدعي إرسالها.

MEC 31: تكاملية المعطيات بالتجفير غير المتناظر المستندة إلى خوارزمية الشارات الرقمية (DSA) التي تستعمل مفتاح بطول معين.

MEC 32: تكاملية المعطيات بالتجفير غير المتناظر القائمة على خوارزمية التجفير Rivest Shamir Adleman (RSA) التي تستعمل مفتاح بطول معين.

3.5.6 تكاملية المعطيات - ملخص

ترد في الجدول 4 أمثلة على خوارزميات يمكن تطبيقها لتأمين تكاملية المعطيات. ويجب أيضاً مراعاة مسائل أخرى مثل الإنساق، والملء، ومعالجة حالات الخطأ، واختيار الأعداد الأولية المناسبة؛ بيد أن هذه المسائل لا تندرج ضمن نطاق هذه التوصية.

الجدول 4/التوصية M.3016.3 - خوارزميات تجفير نموذجية لتأمين سرية المعطيات

الفئة	الخوارزمية	التعليقات
خوارزميات تحقق من الرسائل بتجفير غير متناظر	DSA	خوارزمية الإشارة الرقمية
خوارزميات تحقق من الرسائل بتجفير متناظر	HMAC-MD5-96	شفرة استيقان الرسائل المظللة مع ملخص الرسالة 5.
	HMAC-SHA-1-96	شفرة استيقان الرسائل المظللة مع خوارزمية التظليل الآمنة 1.

6.6 تسجيل التدقيق

ينبغي أن توفر عناصر الشبكة وأنظمة الإدارة قدرات كافية لإفساح المال أمام الاضطلاع بأنشطة التحقيق، والتدقيق، والكشف عن الانتهاكات في الوقت الفعلي وتحليلها وتوفير الحماية من ذلك، لكي يتسنى اتخاذ إجراءات تصحيحية مناسبة. ويدرس هذا البند آليات الأمن المستعملة بشأن سجلات تدقيق الأمن هذه. ولا تندرج التفاصيل الدقيقة لمضمون هذه السجلات ونسقها ضمن نطاق هذه التوصية.

ويجوز أن تحتفظ عناصر الشبكة وأنظمة الإدارة بسجلات تدقيق الأمن. ويمكن حفظ هذه السجلات محلياً، وبالإمكان إحالتها إلى جهاز مركزي لإيداع السجلات و/أو تحليلها.

وسيسلوغ (Syslog) هي واحدة من الآليات الشائعة التي تُستعمل لإرسال سجلات تدقيق الأمن من مخزن محلي ما إلى مستودع مركزي للسجلات.

وعموماً، قد يكون بإمكان جهاز ما من هذا القبيل أن يسجل أي إجراء يغير نعوت الأمن وخدماته، أو عمليات مراقبة النفاذ، أو سائر معلمات تشكيل الأجهزة؛ وأن يسجل كل محاولة دخول ونتيجتها؛ وكل حالة خروج أو إناء للدورة، سواء تمت عن بعد أو بواسطة وحدة تحكم. وتسجيل رسائل التشغيل والإدارة والصيانة والتوريد (OAM&P) غير المتصلة بالأمن، التي يُشار إليها أحياناً بوصفها رسائل تعبر عن "آخر ما استجد من تغييرات"، هو تسجيل ضروري بالنسبة لجميع الإجراءات القابلة للتدقيق.

ويمكن أن تُرسل قيود سجل التدقيق إلى وحدة خدمة حاسوب غير قابلة للتغيير لتدقيقها بعد وسمها بحسب التتابع واستيقانا (توقيعها) بواسطة التجفير من جانب عنصر الشبكة أو نظام الإدارة. ويمكن إرسال سجلات تدقيق الأمن إلى مستودع مركزي عبر مسير موثوق. ولضمان تحليل الإجراءات تحليلاً دقيقاً، ينبغي توخي الدقة والأمن في تحقيق تزامن موعد ووقت مختلف مصادر السجلات (مثل تحقيق ذلك بتطبيق الصيغة 3 من بروتوكول تحديث الوقت الفعلي في الشبكة (NTPv3)).

MEC 33: سجلات تدقيق الأمن القائمة على آلية سيسلوغ (Syslog).

MEC 34: قيود سجلات تدقيق الأمن التي تتضمن المعلومات الآتية:

MEC 34a: وصف للإجراء أو الإجراء الحقيقي المسجل .

MEC 34b: هوية المستعمل ومستوى الأمن الذي يتمتع به أو العملية التي شُرع على أساسها في اتخاذ الإجراء.

MEC 34c: موعد ووقت حصول الإجراء.

MEC 34d: معلومات عن مصدر الشبكة ومقصدها، في حال انطباق ذلك (عند الدخول مثلاً).

MEC 34e: إشارة تنم عن نجاح النشاط أو فشله.

MEC 34f: أي إجراء يتطلب التدقيق.

MEC 35: سجلات تدقيق الأمن المحالة إلى وحدة خدمة حاسوب غير قابلة للتغيير لتدقيقها.

MEC 36: سجلات تدقيق الأمن المقيدة بواسطة التجفير.

MEC 37: سجلات تدقيق الأمن المحالة إلى مستودع مركزي عبر مسير موثوق.

7.6 تبادل المفاتيح

ينبغي تبادل مفاتيح التجفير بين النقاط الطرفية بطريقة آمنة في التطبيقات المتعلقة بتأمين سرية المعطيات وتكامليتها بالتجفير المتناظر. وعموماً، فإن من الضروري أن يتم تبادل المفاتيح المستعملة في خوارزميات التجفير المتناظر هذه بعملية ترتبط ارتباطاً وثيقاً بالاستيقان، لكي لا يتسنى لجهة مهاجمة ما أن تتغلغل بين عمليتي الاستيقان وتوزيع المفاتيح.

والطرائق المستخدمة في توليد وخزن وتوزيع وإتلاف وإلغاء مفاتيح التجفير هذه هي طرائق مهمة للغاية. وإضافة إلى ذلك، ترتبط عوامل من قبيل طول المفتاح، واختياره، وانتفاء الخوارزمية بصلة مباشرة مع مستوى الأمن الذي يوفره نظام تجفير معين.

ويمكن استعمال طرائق شتى لتوفير مفاتيح التجفير و/أو تبادلها. وتتمثل إحدى الطرائق البسيطة لتحقيق ذلك من الناحية النظرية في التشارك مسبقاً في تبادل المفاتيح حيث تُرسل المفاتيح بموجب هذه الطريقة خارج النطاق وتُوفر عند كل نقطة طرفية حسب الاقتضاء. وبإمكان الجهات القائمة على إدارة الشبكة، أن تقوم مثلاً بعد تكليفها بذلك، بانتقاء المفاتيح وتشكيلها في نقاط طرفية. وقد يكون تبادل المفاتيح التي يتم التشارك فيها مسبقاً مقبولاً لدى عدد ضئيل من النقاط الطرفية، غير أن هذا التبادل ليس مقياساً ينطبق تماماً على الأعداد الكبيرة منها لأن توليد وتشكيل أعداد هائلة من المفاتيح يصبح أمراً مربكاً للغاية.

ويمكن استعمال خوارزميات التجفير غير المتناظر مثل خوارزمية Rivest، Shamir، Adleman دعماً لتقديم خدمات تبادل المفاتيح. وبتطبيق هذه الخوارزمية (RSA)، تنتقي إحدى النقاط الطرفية مفاتيح مُجفرة بالتناظر وتوزعها على النقاط الطرفية الأخرى تحت حماية خوارزمية التجفير RSA هذه. وينبغي عند استعمال هذه الطريقة أن يكون طول مفاتيح خوارزمية

التجفير المتناظر ملائماً من أجل حماية مفاتيح التجفير المتناظر المُرسلة. ولتوفير الحماية لمفتاح تجفير متناظر بطول 128 بتة مثلاً، لا بد أن تستعمل الخوارزمية RSA مفتاحاً بطول 2048 بتة أو أكثر ليكون مساوياً تقريباً من حيث قوة التجفير لمفتاح تجفير متناظر بطول 128 بتة.

وخوارزمية ديفي هيلمان (Diffie-Hellman) المعنية بتوافق المفاتيح هي طريقة شائعة لتوزيع المفاتيح. وباستعمال هذه الخوارزمية، تستنبط النقاط الطرفية على نحو مستقل مفاتيح تجفير متناظر سرية عبر إحدى الشبكات العمومية. ولا تُرسل سوى نتائج متوسطة بين النقاط الطرفية أثناء عملية تطبيق خوارزمية ديفي هيلمان، ولا يُكشف أبداً عن المفتاح السري. وبانتقاء الأعداد الأولية الملائمة عند تطبيق هذه الخوارزمية، فإن من المتعذر من الناحية الحسابية على الجهات المهاجمة أن تستنبط المفتاح السري من النتائج المتوسطة.

وفيما يتعلق بخوارزميتي RSA وديفي هيلمان، ينبغي أيضاً أن تُراعى مسائل من قبيل انتقاء الأعداد الأولية الملائمة، واختيار الأس العام، ومعالجة حالات الخطأ.

MEC 38: تبادل مفاتيح التجفير على أساس التشارك مسبقاً في المفاتيح.

MEC 39: تبادل مفاتيح التجفير بالاستناد إلى خوارزمية التجفير غير المتناظر RSA التي تستعمل مفتاح بطول معين.

MEC 40: تبادل مفاتيح التجفير على أساس خوارزمية ديفي هيلمان (Diffie-Hellman) المعنية بتوافق المفاتيح التي تستعمل مجموعة معينة من الأعداد الأولية لديفي هيلمان.

8.6 الإبلاغ بإنذارات الأمن

ينبغي إرسال إنذارات الأمن إلى الجهات القائمة على الإدارة بشأن الكشف عن جميع انتهاكات الأمن أو العجز عن مواصلة تدوين سجلات التدقيق.

MEC 41: آليات الإبلاغ عن إنذارات الأمن مثل X.736.

9.6 ترشيح الرزم

ينبغي استعمال ترشيح الرزم في الأجهزة ذات التوصيلية القائمة على الرزم من أجل حماية شبكة تبادل المعطيات (DCN) من الهجمات والحيلولة دون فقدان المعلومات المتعلقة بذه الشبكة.

MEC 42: ترشيح الرزم على أساس معيار واحد أو أكثر من معايير التفتيش التالية:

MEC 42a: عنوان بروتوكول الإنترنت (IP) المصدر.

MEC 42b: عنوان بروتوكول الإنترنت (IP) المقصد.

MEC 42c: البروتوكول المستعمل.

MEC 42d: منفذ المصدر.

MEC 42e: منفذ المقصد.

وعلى أساس تنفيذ إجراء واحد أو أكثر من الإجراءات الآتية:

MEC 42f: مرر.

MEC 42g: أسقط.

MEC 42h: عدل.

MEC 42i: وجه إلى الأمام.

مع احتمال توفير قدرة على بحث القرارات المتخذة سابقاً (أي، بحث شامل).

التذييل I

آليات أمن بروتوكول الإنترنت (IPsec) وطبقة مقابس الأمن/أمن طبقة النقل (SSL/TLS) وبرنامج شل للدخول الآمن (SSH)

1.I أمن بروتوكول الإنترنت (IPsec)

يتطرق أمن بروتوكول الإنترنت (IPsec) إلى الأمن على مستوى طبقة بروتوكول الإنترنت (IP)، الذي يتحقق باستعمال توليفة تجمع بين آليات التجفير وآليات أمن البروتوكول. ويعمل بروتوكول IPSec بين طبقة الشبكة (الطبقة 3) وطبقة النقل (الطبقة 4) ويمكن استعماله لحماية جميع أنواع حركة المعطيات (بروتوكول مراقبة النقل (TCP) أو بروتوكول داتاغرام المستعمل (UDP)) وهو بروتوكول مستقل عن التطبيقات. والغرض من هذا البروتوكول (IPsec) هو توفير أمن قائم على التجفير يتسم بجودة عالية وقابلية للتشغيل البيني للصيغتين 4 و6 من بروتوكول الإنترنت ((IPv6)&(IPv4)). وتشتمل مجموعة الخدمات الأمنية التي يقدمها أمن بروتوكول الإنترنت (IPsec) على ما يلي:

أ) تأمين تكاملية المعطيات؛

ب) استيقان مصدر المعطيات على أساس عنوان بروتوكول الإنترنت (IP)؛

ج) الاستيقان من الآلة إلى الآلة؛

د) توفير حماية ضد التكرار؛

ه) تأمين سرية المعطيات؛

و) تبادل مفاتيح التجفير.

وتُحقق هذه الأهداف بالاستفادة من خدمتين أمنيتين متعلقتين بالحركة، وهما رأسية الاستيقان (AH) وتغليف الحمولة النافعة الأمنية (ESP)، وعن طريق تطبيق إجراءات وبروتوكولات إدارة مفاتيح التجفير. وتحقق خدمة رأسية الاستيقان (AH) الاستيقان من مصدر المعطيات واستيقان الآلة إلى الآلة، وتؤمن تكاملية معطيات رزم بروتوكول الإنترنت (IP). أما خدمة تغليف الحمولة النافعة الأمنية (ESP) فتؤمن سرية المعطيات بالإضافة إلى استيقان مصدر المعطيات واستيقان الآلة إلى الآلة وتأمين تكاملية معطيات رزم بروتوكول الإنترنت (IP). كما أن الغرض من آليات أمن بروتوكول الإنترنت (IPsec) هو جعلها خوارزميات تجفير مستقلة تفسح المال أمام انتقاء مجموعات مختلفة من الخوارزميات من دون التأثير على الأجزاء الأخرى من التنفيذ.

ويضطلع بروتوكول تبادل مفاتيح الإنترنت (IKE) بإدارة المفاتيح. ويوفر آليات يدوية وأوتوماتية على حد سواء للتفاوض بشأن المفاتيح بين النقاط الطرفية. ويمكن أن يستند التفاوض الأوتوماتي بشأن المفاتيح إلى التشارك المسبق في المفاتيح (مثل كلمات السر) أو شهادات المعيار X.509.

ويرجى الاطلاع على المراجع [RFC 2401]، [RFC 2402]، [RFC 2403]، [RFC 2404]، [RFC 2405]، [RFC 2406]، [RFC 2407]، [RFC 2408]، [RFC 2409]، [RFC 2410]، [RFC 2411]، [RFC 2412]، [RFC 3602]، [RFC 2451]، [FIPS-197].

2.I طبقة مقابس الأمن/أمن طبقة النقل (SSL/TLS)

يوفر بروتوكول أمن طبقة مقابس الأمن (SSL) تجفير المعطيات، واستيقان وحدة الخدمة، وتكاملية الرسائل، واستيقان الزبائن اختيارياً في التوصيل ببروتوكول مراقبة النقل (TCP)/بروتوكول الإنترنت (IP) على مستوى طبقة النقل (الطبقة 4). وتخضع حالياً طبقة مقابس الأمن (SSL) للتنقيح بموجب المعيار 3.0. وأمن طبقة النقل (TLS) هو عبارة عن صيغة الطبقة SSL القياسية الصادرة عن فريق مهام هندسة الإنترنت (IETF) وهو يشمل حالات تعزيز الأمن عبر هذه الطبقة (SSL) بما في ذلك ما يلي:

- توفير الدعم الضروري بخوارزمية ديفي هيلمان وخوارزمية الشارات الرقمية (DSA)، مع توفير الدعم الاختياري بخوارزمية RSA.
- استعمال خوارزمية أقوى لشفرة استيقان الرسائل المظللة (HMAC) بدلاً من استعمال خوارزمية غير قياسية لاستيقان الرسائل (MAC) تكون محددة بموجب طبقة مقابس الأمن (SSL).
- استعمال خوارزمية معدلة لتوليد المفاتيح تستخدم (ملخص الرسالة 5) (MD5) وخوارزمية التظليل الآمنة 1 (SHA-1) مع شفرة استيقان الرسائل المظللة (HMAC).

ويعمل بروتوكول طبقة مقابس الأمن/أمن طبقة النقل (SSL/TLS) فوق طبقة الشبكة (الطبقة 4)، ولا يعمل سوى مع بروتوكول مراقبة النقل (TCP) ولا يمكن أن يعمل مع بروتوكول داتاغرام المستعمل (UDP). وتشمل بروتوكولات طبقة التطبيق التي تعمل عادة في أعلى طبقة مقابس الأمن/أمن طبقة النقل (SSL/TLS) بروتوكول نقل النصوص الفائقة (HTTP)، والبروتوكول الخفيف الوزن للنفاذ إلى الدليل (LDAP)، وبروتوكول الإنترنت للنفاذ إلى الرسائل، ولكنها لا تقتصر على ذلك. ويمكن أن يعمل البروتوكول المستعمل في التطبيقات الأعلى مستوى فوق طبقة مقابس الأمن/أمن طبقة النقل (SSL/TLS) بصرف النظر عن هذه الطبقة (SSL/TLS)؛ ومع ذلك، ينبغي ربط مستوى التطبيق بالطبقة SSL/TLS عن طريق اللجوء إلى إجراء حالات إعادة نداء الدخل/الخرج (I/O).

ويؤدي بروتوكول طبقة مقابس الأمن/أمن طبقة النقل (SSL/TLS) ثلاث وظائف أمنية لحركة بروتوكول مراقبة النقل (TCP)، وهي: تأمين سرية المعطيات وتأمين تكامليتها والاستيقان منها.

وتوفر معمارية بروتوكول أمن طبقة مقابس الأمن/أمن طبقة النقل (SSL/TLS) طبقتين تعملان فوق بروتوكول مراقبة النقل (TCP)، وهما:

- بروتوكولات الطبقة العلوية لطبقة مقابس الأمن/أمن طبقة النقل (SSL/TLS)؛
- بروتوكول تسجيل طبقة مقابس الأمن/أمن طبقة النقل (SSL/TLS).

وتشمل بروتوكولات الطبقة SSL/TLS بروتوكول التفاوض بذه الطبقة SSL/TLS، وبروتوكول تغيير شفرات الطبقة SSL/TLS، وبروتوكول الإنذار بالطبقة SSL/TLS المعني بإصدار التبليغات. وتُنشأ من حيث المبدأ دورات طبقة مقابس الأمن/أمن طبقة النقل (SSL/TLS) من جانب بروتوكول التفاوض بالطبقة SSL/TLS الذي يحقق ما يلي:

أ) التفاوض بشأن آليات الاستيقان وآليات الأمن.

ب) الاستيقان من الزبون ومن وحدة الخدمة. (باستعمال المفتاحين العمومي/الخاص لوحدة الخدمة والزبون.)

ج) توليد مفاتيح أمنية.

وحالما يتم إنشاء دورة طبقة مقابس الأمن/أمن طبقة النقل (SSL/TLS)، يُستعمل بروتوكول تسجيل الطبقة SSL/TLS لتقديم خدمات كبيرة في مجال نقل المعطيات. ويؤمن بروتوكول تسجيل الطبقة SSL/TLS ما يلي:

أ) الاستيقان من مصدر المعطيات بالاستناد إلى مفاتيح وحدة الخدمة.

ب) تكاملية المعطيات.

ج) سريتها.

ومن الجدير بالذكر أن طبقة مقابس الأمن (SSL) متيسرة الآن بالصيغة 3 (SSLv3)، بينما يتيسر أمن طبقة النقل (TLS) بالصيغة 1. ولا يوصى باستعمال الصيغ الموضوعة سابقاً لطبقة مقابس الأمن (SSL) وأمن طبقة النقل (TLS).

وتفسح طبقة مقابس الأمن/أمن طبقة النقل (SSL/TLS) المال أمام تحقيق استيقان أحادي الاتجاه حيث يؤمن استيقان وحدة الخدمة إلى الزبون حصراً، أو أمام استيقان ثنائي الاتجاه حيث يستيقن الزبون ووحدة الخدمة كل من الآخر على حد سواء. والاستيقان أحادي الاتجاه هو الطريقة المستعملة عادة في الإنترنت العمومية. أما فيما يتعلق بتطبيقات إدارة الشبكة، فيوصى بتطبيق استيقان ثنائي الاتجاه لإفساح المال أمام كلا الطرفين ليكونا على بينة من أنما يتصلان بالنقطة الطرفية التي يرغبان فيها.

يرجى الاطلاع على المراجع [RFC 2246]، [RFC 3546]، [SSL V3].

3.I برنامج شل للدخول الآمن (SSH)

برنامج شل للدخول الآمن (SSH) هو بروتوكول أمن طبقة التطبيق (الطبقة 7) ويستعمل بشكل شائع ليحل مباشرة محل البروتوكولين غير الآمنين لشبكة الاتصالات (Telnet) ونقل الملفات (FTP). ويقوم هذان البروتوكولان غير الآمنين (Telnet) و(FTP) بنقل كلمات السر وجميع المعطيات الأخرى بنص واضح غير مشفر. ويمكن أيضاً استعمال برنامج شل للدخول الآمن (SSH) لحماية بروتوكولات أخرى من خلال اللجوء إلى إحالة المنافذ، لكي يتسنى استعماله كبروتوكول يحقق أمن الشبكة بصورة عامة.

وتوجد صيغتان من البروتوكول SSH، وهما: الصيغة 1 (SSHv1) والصيغة 2 منه (SSHv2). وقد وضعت الصيغة 1 من هذا البروتوكول في عام 1998 وتعتبر الآن غير آمنة/بطل استعمالها.

أما سمات الصيغة 2 من برنامج شل الآمن فهي كما يلي:

- تحل هذه الصيغة تماماً محل بروتوكولات كل من Telnet، وRloging، وRsh، وRcp، وFTP بغية تأمين نقل الملفات ونسخها.
- استيقان المستعملين أوتوماتياً. (عدم إرسال كلمات سر بنص واضح غير مشفر.)
- استيقان ثنائي الاتجاه (يُستيقن فيه وحدة الخدمة ويستيقن الزبون على حد سواء).
- إمرار التطبيقات العشوائية القائمة على بروتوكول مراقبة النقل (TCP)/بروتوكول الإنترنت (IP) عبر أنفاق عن طريق الإحالة التي تكفلها المنافذ.
- تجفير المعطيات من أجل الحفاظ على سريتها.
- توفير العديد من خيارات الاستيقان التي تشمل كلمات السر، والمفاتيح العمومية، والاستيقان المأمون لمعرف الهوية (ID).
- تيسر العديد من متواليات الشفرات.

ومعمارية الصيغة 2 من برنامج شل الآمن (SSHv2) مؤلفة من ثلاثة مكونات رئيسية، هي:

- بروتوكول طبقة النقل [SSH-TRANS] الذي يؤمن استيقان وحدة الخدمة، ويحفظ سرية المعطيات، وتكامليتها. ويمكن أن يؤمن أيضاً انضغاط المعطيات حسب الاختيار.
- بروتوكول استيقان المستعمل [SSH-USERAUTH] الذي يعمل على استيقان مستعمل جانب الزبون إلى وحدة الخدمة.
- بروتوكول التوصيل [SSH-CONNECT] الذي يعمل على تعدد إرسال الأنفاق المفرة داخل عدة قنوات منطقية.

ويوفر بروتوكول التوصيل قنوات يمكن استعمالها لتحقيق طائفة واسعة من الأغراض. ويوفر كذلك طرائق قياسية لإنشاء دورات تفاعلية مأمونة تتعلق ببرنامج شل ولإحالة المنافذ والتوصيلات العشوائية القائمة على بروتوكول مراقبة النقل (TCP)/بروتوكول الإنترنت (IP) ("تمريرها عبر أنفاق").

وقد سُجل المنفذ رقم 22 لدى هيئة تخصيص أرقام الإنترنت (IANA) بوصفه المنفذ القياسي الذي يستعمل في تطبيقات الصيغة 2 من برنامج شل للدخول الآمن (SSHv2).

ويرجى الاطلاع على المراجع [SSH-ARCH]، [SSH-TRANS]، [SSH-USERAUTH]، [SSH-CONNECT].

التذييل II

يصف هذا التذييل آلية لترشيح الرزم لتعزيز أمن شبكة تبادل المعطيات (DCN). وتُستعمل هذه الشبكة (DCN) لتوصيل تطبيقات الإدارة (الموجودة عادة في مركز تشغيل الشبكة) بعناصر الشبكة من أجل الاضطلاع بأنشطة تقديم الخدمات على الصعيد المركزي، ومراقبة توجيه الإنذارات، والاختبار، والفوترة، وغيرها من الأنشطة المتعلقة بإدارة الشبكة. وترد في الأقسام 10.2-8.2 من المرجع RFC 3871 مجموعة من المتطلبات اللازمة لترشيح الرزم في مجال البنية الأساسية العظمى لشبكة بروتوكول الإنترنت (IP) لمقدمي خدمة الإنترنت. وتستند هذه المساهمة إلى المرجع RFC 3871 لتحديد نصائح الترشيح المتعلقة بشبكة تبادل المعطيات (DCN).

وترشيح الرزم هو عملية البت بشأن وصف كل رزمة تمر عبر عنصر ما من عناصر الشبكة بالاستناد إلى معايير تواؤم معينة[9]. وقد يكون هناك عدة حالات وصف، مثل تمرير، إهمال، إحالة (توجيه الرزمة إلى مكان آخر)، غير ذلك. ويوفر ترشيح الرزم آلية الحماية الأساسية التي تحدد ماهية الحركة التي تمر إلى داخل عنصر الشبكة أو نظام الإدارة أو تمر عبر أحدهما.

وينصب الاهتمام الرئيسي على ترشيح الحركة الوافدة من شبكات أخرى (مثل الشبكات الحاملة لحركة المشتركين، وشبكات إدارة الأنداد) إلى شبكة تبادل المعطيات (DCN). وإضافة إلى ذلك، قد يكون فصل بعض عناصر الشبكة DCN عن عناصر أخرى أمراً ضرورياً. وعليه، يمكن استعمال الترشيح بين شبكات فرعية مختلفة (أو فيما بين مجالات) الشبكة DCN.

1.II الأهداف

تتمثل الأهداف العامة لآلية ترشيح الرزم فيما يلي:

1) حماية البنية الأساسية لشبكة تبادل المعطيات (DCN) من حركة المشتركين. وينبغي أن تشمل الحماية تقاسم الموارد المشتركة بإنصاف للحيلولة دون تعرضها للانحطاط أو رفض الخدمة.

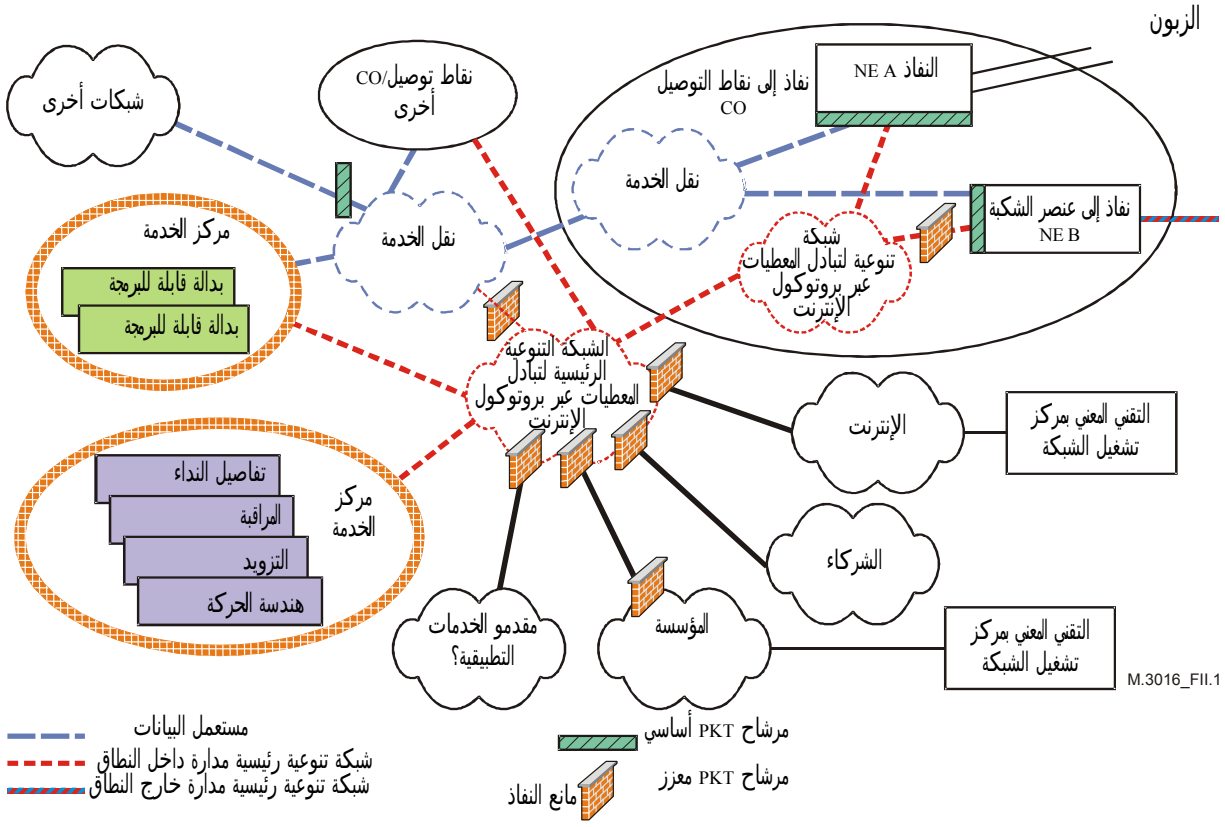
2) حماية البنية الأساسية لشبكة تبادل المعطيات (DCN) من شبكات الأنداد.

3) منع الحركة المسيرة عبر شبكة تبادل المعطيات (DCN) والغير متمشية مع السياسة الأمنية المطبقة فيها من الانتشار إلى ما هو أبعد من ذلك في البنية الأساسية للشبكة DCN.

2.II اعتبارات تصميم الشبكة التي تؤثر على ترشيح الرزم

لا يتضمن هذا التذييل المتطلبات اللازمة لتصميم شبكة تبادل المعطيات (DCN)؛ غير أن تصميم هذه الشبكة (DCN) وطريقة نشرها يؤثران على نشر ترشيح الرزم والمتطلبات اللازمة لذلك داخل الشبكة. ويبين الشكل 1.II تصميماً نموذجياً للشبكة DCN.

[9] يشابه وصف ترشيح الرزم هذا إلى حد بعيد تسيير الرزم؛ غير أن هذا التذييل يركز على ترشيح الرزم ولا يتناول تسييرها.



الشكل II.1/التوصية M.3016.3 - مثال توضيحي لشبكة تنوعية لتبادل المعطيات (DCN)

ويُسلم عموماً بوجود ثلاثة أنواع من تصاميم الشبكة DCN، وهي:

- إدارة داخل النطاق: تستعمل الشبكة DCN عرض نطاق محجوز من شبكة الخدمة المستخدمة في حمل معطيات المشترك. ويمكن مثلاً تخصيص إحدى شبكات المناطق المحلية التقديرية (VLAN) عبر وصلة ما من وصلات إثرنت لحمل حركة الإدارة أو بالإمكان استعمال توصيل بأمن بروتوكول الإنترنت (IPsec) أو توصيل ببرنامج شل للدخول الآمن (SSH) عبر توصيل بالإنترنت (مثلاً في حالة توصيل التقني المعني بمركز تشغيل الشبكة (NOC) عبر الإنترنت مثلما هو مبين في الشكل II.1).
- إدارة خارج النطاق: تختلف شبكة تبادل المعطيات (DCN) في هذه الحالة اختلافاً تاماً عن شبكة الخدمة الحاملة لحركة الزبون. وقد تكون هذه الشبكة مضمنة في الجزء العلوي من نفس الشبكة المادية التي تحمل أيضاً حركة معطيات المستعمل.
- نج هجين: هو نج يجمع بين النهجين داخل النطاق وخارجه.

ولا تندرج مقارنة هذه الأنواع من معماريات الإدارة ولا مناقشتها العامة ضمن نطاق هذه التوصية (انظر القسم 2.2 من المرجع RFC 3871)؛ بيد أن استعمال نوع منها أو آخر يؤثر على متطلبات الترشيح.

ويتباين الأساس المنطقي الذي يُستند إليه في إنشاء شبكات تبادل المعطيات (DCN) بتباين نوع عناصر الشبكة المدعومة، وإجراءات التشغيل وأفضلياته، والخصائص الهندسية للشبكة، والاقتصاديات، غير ذلك. أما سعة الشبكة، ومرونتها، وأمنها فهي مسائل يتم بحثها في كل نج.

وستُنفذ عروض الخدمة المدارة بواسطة الجيل المقبل باستعمال أجهزة نقل قائم على الرزم (مثل ترحيل الأرتال، أسلوب النقل غير المتزامن (ATM)، بروتوكول الإنترنت (IP)، تبديل الوسوم ببروتوكولات متعددة (MPLS)، الإثرنت). ويحتم قدوم هذه الخدمات إدارة أجهزة النفاذ (CPE).

وقد تقتضي الضرورة استعمال نموذج هجين يطبق إدارة خارج النطاق على نقاط التوصيل (POP) وإدارة داخل النطاق من نقطة التوصيل (POP) إلى أجهزة النفاذ CPE، لأن تمديد الإدارة خارج النطاق عبر جميع أجهزة النفاذ CPE يمكن أن يكون أمراً غير مجد من الناحية الاقتصادية. ويوضح النفاذ إلى عنصر الشبكة B (NE B) الحالة الأخيرة المبينة في الشكل 1.II. ويمكن في هذه الحالة استعمال الترشيح المعزز (مثل جدران الحماية) لحماية شبكة تبادل المعطيات (DCN) من أجهزة النفاذ CPE. ويوجد مثالان آخران على استعمال التوصيل داخل النطاق أحدهما إدارة نقطة توصيل (POP) معينة بعيدة ومعزولة يكون فيها إنشاء شبكة مستقلة أمراً متعذراً والآخر استعمال شبكة الخدمة بوصفها شبكة دعم لشبكة تبادل المعطيات (DCN).

كما يفترض استعمال ترشيح الرزم فصل مجال العنوان الذي تستخدمه شبكة تبادل المعطيات (DCN) عن المجال المخصص للمشتركين وليس من الضروري أن تتدفق الحركة بين هذين المجالين. ويبسط فصل مجالات العناوين أمر استحداث مرشحات الرزم لمنع حركة المشتركين من النفاذ إلى موارد الإدارة. ويتمثل النهج الأبسط المتبع في ذلك في وقف جميع الحركة التي مقصدها الشبكة DCN ومصدرها من خارج هذه الشبكة (DCN) من أجل حماية البنية الأساسية للإدارة من حركة المشتركين. ومع ذلك، قد تكون هناك حاجة لتبادل حركة معينة بين شبكات خارجية وشبكة تبادل المعطيات (DCN) في بعض الحالات، مثل تبادل معلومات الإدارة بين اثنين من مقدمي الخدمات (مثلاً، قناة تبادل المعطيات (DCC) الواقعة في نقطة الالتقاء الوسطية بين مقدمَيْن من مقدمي الخدمات (SP)).

ولذلك، فإن التيسر ضروري من أجل إفساح المجال أمام تدفق بعض الحركة المقيدة بين المجالات، وثمة حاجة إلى المزيد من التحكمات (مثل ترشيح الرزم المعزز) لتوفير مستوى أمن ملائم لشبكة تبادل المعطيات (DCN).

ويوضح الشكل 1.II تصميماً معيناً للشبكة DCN على أساس الافتراضات المذكورة أعلاه. وتقوم خدمة النقل (باللون الأزرق) بحمل حركة المشترك. أما شبكة تبادل المعطيات (DCN) (باللون الأحمر) فتحمل حركة الإدارة. ويحوي مركز الخدمة وحدات الخدمة، وغير ذلك، التي تقدم خدمات إلى المشتركين ويتسنى لهؤلاء سبيل للنفاذ إلى (البدالات القابلة للبرمجة على سبيل المثال). ويضم مركز المعطيات وحدات خدمة وغيرها من أنظمة التشغيل المستعملة لإدارة الشبكة ومراقبتها ويتعذر على المشتركين النفاذ إليه مباشرة. ويمكن الاستفادة من بروتوكول الإنترنت (IP) أو بروتوكول لطبقة رزمة X.25 أو اللاتزامن أو خدمة الشبكة بدون توصيل (CLNS) المقدمة وفقاً لمعايير المنظمة الدولية للتوحيد القياسي (ISO) في التوصيل من الشبكة DCN إلى عناصر الشبكة.

ويعد توفير ترشيح رزم الإدخال عبر حدود شبكة تبادل المعطيات (DCN)/شبكة الخدمة شرطاً أساسياً لتحقيق أمن الشبكة DCN في النفاذ إلى عنصر الشبكة (NE). غير أن هذا الترشيح الأساسي للرزم قد يكون غير كاف لأنه يمكن أن تُشن أيضاً هجمات من عنصر شبكة (NE) معرض للخطر أو مركز داخل الشبكة DCN. وبناء على ذلك، قد يكون من الضروري تنفيذ آليات ملائمة لترشيح الرزم تنفيذاً استراتيجياً في العديد من النقاط الموجودة داخل شبكة تبادل المعطيات (DCN) لضمان التقيد بالسياسة الأمنية المطبقة. وإضافة إلى ذلك، قد تكون هناك حاجة إلى ترشيح الرزم المعزز في الحالات التي توصل فيها الشبكة DCN بشبكات خارجية (مثل الإنترنت، شبكة مؤسسة مقدم الخدمة، الشركاء، غير ذلك).

ومع أن ترشيح الرزم هو مكون من مكونات استراتيجية أمن الشبكة، فإنه ينبغي استعماله ضمن سياق المبادئ والاستراتيجيات العامة بشأن أمن الشبكة التي تشمل مثلاً تقسيم الشبكة إلى خانات والدفاع عنها بشكل متعمق. وهكذا، ومع أن أي استراتيجية أمنية جيدة تشمل متطلبات الأمن المتعلقة بالمراكز تحديداً (مثل البدالات القابلة للبرمجة) وتقسيم الشبكة إلى خانات، فإن هذه المتطلبات لا تندرج ضمن نطاق هذه التوصية.

ولحماية البنية الأساسية للإدارة، وشبكة تبادل المعطيات (DCN) عموماً، فإن من المفيد لمشغل الشبكة أن يستبعد رزماً معينة يستقبلها من خارج نطاق الشبكة DCN (أي من الأنداد والمشتركين). ولا ينبغي مثلاً السماح للرزم التي تحمل عناوين بروتوكول الإنترنت (IP) صادرة عن مصدر غير صحيح والرزم التي مقصدها هذه العناوين (IP) والمستعملة حصراً عبر الشبكة DCN بالنفاذ إلى داخل نطاق هذه الشبكة (DCN). وتسمى هذه الوظيفة ترشيح الإدخال. وهذه المتطلبات مستنبطة من المرجعين [RFC 3871] و[RFC 2827].

وتوجد فئتان من ترشيح الرزم، هما:

- ترشيح رزم أساسي يستند إلى المعلومات المتعلقة برأسية الرزم والتي تضم القدرة على الكشف عن الرزم الحاملة لعنوان مصدر مزيف وعلى إيقافها.
- ترشيح رزم معزز يشمل ما يلي:
  - فحص الرزم مع الحفاظ على حالتها الذي يُستفاد منه أيضاً من المعلومات المتعلقة بالسياق أو المعلومات ذات الصلة بالحالة في اتخاذ القرارات المتصلة بالترشيح.
  - ترشيح دينامي لبروتوكولات معينة تُفتح فيه المراشح دينامياً على أساس المعلومات المحمولة داخل الحمولة النافعة للبروتوكول.
  - تفتيش دقيق للرزم تُفحص فيه البروتوكولات على مستوى التطبيق من أجل الكشف عن أي شذوذ يعتريها أو أية محتويات غير عادية أو مريبة بداخلها.

3.II ترشيح الرزم الأساسي

ينبغي أن يُتاح أمام الأجهزة الموصولة بشبكة تبادل المعطيات (DCN) خيار استبعاد الرزم المُستقبلة من سطوح بينية مواجهة لمصادر خارجية (مثل المشتركين والأنداد) والتي تحوي عناوين بروتوكول الإنترنت (IP) لمصدر غير صحيح. ويمكن أن تتضمن هذه العناوين ما يلي:

- عناوين بوغون (Bogon) (انظر القسم 8.1 من المرجع RFC 3871).
- رزم حاملة لعناوين إنترنت مزيفة (رزم مريخية) (انظر القسم 8.1 من المرجع RFC 3871).
- عناوين بروتوكول الإنترنت (IP) غير المخصصة للمشتركين (أو غير الصالحة لأن يُرسلها الند).

ولا بد أن تكون آلية ترشيح الرزم قادرة على ترشيح الحركة الموجهة إلى قدرات العناوين المخصصة لشبكة تبادل المعطيات (DCN) والصادرة من الخارج (من المشتركين مثلاً) على أساس النعوت المحددة في الآلية 42 (MEC 42).

ومن الضروري أن تقدم آلية ترشيح الرزم إحصاءات دقيقة عن الحركة عبر كل سطح بيني. وقد يتباين مستوى تحبحب الإحصاءات بتباين آلية ترشيح الرزم.

وينبغي أن تكون الأجهزة قادرة على ترشيح الحركة الواردة من خارج شبكة تبادل المعطيات (DCN) (من المشتركين على سبيل المثال)، أي الحركة الموجهة مباشرة إلى أحد عناصر الشبكة عبر أي سطح من سطوحها البينية، بما فيها السطوح البينية بعروة رجعة، وذلك على أساس النعوت المحددة في الآلية 42 (MEC 42).

ويمكن أن تقدم آلية ترشيح الرزم الدعم لمفهوم تعددية المجالات الأمنية المتعلق بنموذج شبكة إدارة الاتصالات (TMN) الذي تُلزم فيه جميع العناصر الموجودة داخل مجال أمني ما بإتباع سياسة أمنية مشتركة.

ويمكن أن تتمتع الأجهزة بقدرة إصدار إنذارات مناسبة على أساس الحركة والحالات الاستثنائية وظروف تشغيلها.

4.II ترشيح الرزم المعزز

لا بد من مراعاة هذه النصائح في الحالات التي توجد فيها درجة عالية من التراكب بين حركة المستعمل وحركة الإدارة، أي، عدم فصل الحركتين عند حافة الشبكة تماماً، وفي حال كانت شبكة تبادل المعطيات (DCN) موصولة مباشرة بشبكات أخرى. وبالإضافة إلى ذلك، ينبغي الاستفادة من قدرات الترشيح هذه عند حدود الشبكات الفرعية المحمية (بين شبكة تبادل المعطيات (DCN) ومركز المعطيات مثلاً).

ومن الضروري أن تتفحص الآلية بروتوكولات التطبيق المستعملة عبر الشبكة DCN من أجل الكشف عن أي شذوذ أو سلوك غير عادي يعتريها وأن توقف هذه الحركة حسبما يقتضي الأمر.

وينبغي أن تتفحص الآلية محتوى الحركة المسيرة عبر شبكة تبادل المعطيات (DCN) من أجل الكشف عما إذا كان بداخلها محتويات ضارة من قبيل الفيروسات، برامج وورم التخريبية، برنامج حصان طروادة للتلصص، غير ذلك، حيثما انطبق الأمر.

ولا بد أن توفر الحماية للأنواع القابلة للانطباق من هجمات رفض الخدمة (DoS).

ومن الضروري أن تكون الآلية قادرة على ترشيح الرزم مع الحفاظ على حالتها، أي الاستفادة من معلومات الدورة في ترشيح الرزم. وينبغي دوماً إفساح المجال أمام مرور الحركة العائدة إلى دورة معينة.

وينبغي أن تقدم الآلية الدعم لقدرة التثقيب الدينامي اللازمة لجميع البروتوكولات المستعملة في الشبكة الحاملة لمعلومات المنفذ داخل حمولتها النافعة، مثل بروتوكول نقل الملفات (FTP)، بروتوكول استهلال الدورة (SIP)، غير ذلك. ولا بد أن تتفحص آلية ترشيح الرزم معلومات المنفذ الموجودة داخل الحمولة النافعة وأن تفتح الاتصال عبر المنفذ المحدد (تثقيب دينامي) لعمر الدورة. ويتعين إيجاد آلية مناسبة لتحديد المهل الزمنية لإغلاق المنفذ في حال إنهاء الدورة فجأة.

ومن الضروري أن تقدم الآلية الدعم لإنفاذ البروتوكولات بما في ذلك إسقاط الرزم المشوهة أو إنشاء الدورات بطريقة غير صحيحة، غير ذلك.

ويمكن الاطلاع على قدرات أخرى موصى بها في مجال الترشيح في الأقسام 7.2-10.2 من المرجع RFC 3871.

بيبليوغرافيا

[RFC 2827] IETF RFC 2827 (2000), *Network Ingress Filtering: Defeating Denial of Service Attacks which employ IP Source Address Spoofing*.

[RFC 2401] IETF RFC 2401 (1998), *Security Architecture for the Internet Protocol*, http://www.ietf.org/rfc/rfc2401.txt?number=2401

[RFC 3704] IETF RFC 3704 (2004), *Ingress Filtering for Multihomed Networks*.

[RFC 3871] IETF RFC 3871 (2004), *Operational Security Requirements for Large Internet Service Provider (ISP) IP Network Infrastructure*.

[NDS/IP] 3GPP TS 33.210 (2001), *3rd Generation Partnership Project; Technical Specification Group Services and System Aspects; 3G Security; Network Domain Security; IP network layer security*.

[RFC 2402] IETF RFC 2402 (1998), *IP Authentication Header*, http://www.ietf.org/rfc/rfc2402.txt?number=2402

[RFC 2403] IETF RFC 2403 (1998), *The Use of HMAC-MD5-96 within ESP and AH*, http://www.ietf.org/rfc/rfc2403.txt?number=2403

[RFC 2404] IETF RFC 2404 (1998), *The Use of HMAC-SHA-1-96 within ESP and AH*, http://www.ietf.org/rfc/rfc2404.txt?number=2404

[RFC 2405] IETF RFC 2405 (1998), *The ESP DES-CBC Cipher Algorithm with Explicit IV*, http://www.ietf.org/rfc/rfc2405.txt?number=2405

[RFC 2406] IETF RFC 2406 (1998), *IP Encapsulating Security Payload (ESP)*, http://www.ietf.org/rfc/rfc2406.txt?number=2406

[RFC 2407] IETF RFC 2407 (1998), *The Internet IPsecurity Domain of Interpretation for ISAKMP*, http://www.ietf.org/rfc/rfc2407.txt?number=2407

[RFC 2408] IETF RFC 2408 (1998), *Internet Security Association and Key Management Protocol (ISAKMP)*, http://www.ietf.org/rfc/rfc2408.txt?number=2408

[RFC 2409] IETF RFC 2409 (1998), *The Internet Key Exchange (IKE)*, http://www.ietf.org/rfc/rfc2409.txt?number=2409

[RFC 2410] IETF RFC 2410 (1998), *The NULL Encryption Algorithm and Its Use with IPsec*, http://www.ietf.org/rfc/rfc2410.txt?number=2410

[RFC 2411] IETF RFC 2411 (1998), *IPsecurity Document Roadmap*, http://www.ietf.org/rfc/rfc2411.txt?number=2411

[RFC 2412] IETF RFC 2412 (1998), *The OAKLEY Key Determination Protocol*, http://www.ietf.org/rfc/rfc2412.txt?number=2412

[RFC 3602] IETF RFC 3602 (2003), *The AES-CBC Cipher Algorithm and Its Use with IPsec*, http://www.ietf.org/internet-drafts/draft-ietf-ipsec-ciph-aes-cbc-04.txt

[RFC 2451] IETF RFC 2451 (1998), *The ESP CBC-Mode Cipher Algorithms*, http://www.ietf.org/rfc/rfc2451.txt

[RFC 2246] IETF RFC 2246 (1999), *The TLS Protocol, Version 1.0*, ftp://ftp.rfc-editor.org/in-notes/rfc2246.txt

[RFC 3546] IETF RFC 3546 (2003), *Transport Layer Security (TLS) Extensions*, ftp://ftp.rfc-editor.org/in-notes/rfc3546.txt

[SSL V3] *Secure Socket Layer Version 3.0 Specification*, Netscape Communications. http://wp.netscape.com/eng/ssl3/

[SSH-ARCH] YLONEN (T.): *SSH Protocol Architecture*, I-D draft-ietf-architecture-15.txt, October 2003. http://www.ietf.org/internet-drafts/draft-ietf-secsh-architecture-15.txt

[SSH-TRANS] YLONEN (T.): *SSH Transport Layer Protocol*, I-D draft-ietf-transport-17.txt, October 2003. http://www.ietf.org/internet-drafts/draft-ietf-secsh-transport-17.txt

[SSH-USERAUTH] YLONEN (T.): *SSH Authentication Protocol*, I-D draft-ietf-userauth-18.txt, September 2002. http://www.ietf.org/internet-drafts/draft-ietf-secsh-userauth-18.txt

[SSH-CONNECT] YLONEN (T.): *SSH Connection Protocol*, I-D draft-ietf-connect-18.txt, October 2003. http://www.ietf.org/internet-drafts/draft-ietf-secsh-connect-18.txt

[FIPS-46-3] Data Encryption Standard. (Describes both DES and 3DES). http://csrc.nist.gov/publications/fips/fips46-3/fips46-3.pdf

[FIPS-197] Advanced Encryption Standard (AES), FIPS Publication 197, National Institute of Standards and Technology, November 2001. http://csrc.nist.gov/publications/fips/fips197/fips-197.pdf

[RFC 2437] IETF RFC 2437 (1998), *PKCS #1: RSA Cryptography Specifications Version 2.0*, http://www.ietf.org/rfc/rfc2437.txt?number=2437

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 وتعدد الوسائط
السلسلة I	الشبكة الرقمية متكاملة الخدمات
السلسلة J	الشبكات الكبلية وإرسال إشارات البرامج الإذاعية الصوتية والتلفزيونية 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 المعطيات على الشبكة الهاتفية
السلسلة X	شبكات المعطيات والاتصالات بين الأنظمة المفتوحة والأمن
السلسلة Y	البنية التحتية العالمية للمعلومات وملامح بروتوكول الإنترنت وشبكات الجيل التالي
السلسلة Z	لغات البرمجة والخصائص العامة للبرمجيات في أنظمة الاتصالات

طبعت في سويسرا
جنيف، 2005