الاتحـــــــــاد الدولـــــــــي للاتصـــــــــالات

CCITT **X.800**

اللجنة الاستشارية الدولية
للبرق والهاتف

شبكات اتصالات البيانات: التوصيل البيني للأنظمة المفتوحة (OSI)؛ والأمن والهيكل والتطبيقات

معمارية الأمن في التوصيل البيني للأنظمة المفتوحة من أجل تطبيقات اللجنة الاستشارية الدولية للبرق والهاتف

التوصيـــة X.800

جنيف، 1991

تمهيـــد

اللجنة الاستشارية الدولية للبرق والهاتف (CCITT) هي هيئة دائمة في الاتحاد الدولي للاتصالات (ITU). وهي تتولى مسؤولية دراسة المسائل التقنية والمسائل المتعلقة بالتشغيل والتعريفة، وإصدار التوصيات بشأنها بغرض تقييس الاتصالات على الصعيد العالمي.

وتحدد الجمعية العامة للجنة الاستشارية الدولية للبرق والهاتف، التي تجتمع مرة كل أربع سنوات، المواضيع التي يجب أن تدرسها لجان الدراسات التابعة لها وتوافق على التوصيات التي تعدها هذه اللجان. ويوافق أعضاء اللجنة الاستشارية الدولية للبرق والهاتف على هذه التوصيات في الفترة الفاصلة ما بين انعقاد جمعية عامة وأخرى وفقاً للإجراء المنصوص عليه في القرار رقم 2 للجنة الاستشارية الدولية للبرق والهاتف (ملبورن، 1988).

وقد أعدت لجنة الدراسات السابعة التوصية X.800 وتمت الموافقة عليها بموجب الإجراء المنصوص عليه في القرار رقم 2 في 22 مارس 1991.

ملاحظة من اللجنة الاستشارية الدولية للبرق والهاتف

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

التوصيـــة X.800

معمارية الأمن في التوصيل البيني للأنظمة المفتوحة من أجل تطبيقات اللجنة الاستشارية الدولية للبرق والهاتف[1]

0 مقدمة

تصف التوصية X.200 النموذج المرجعي للتوصيل البيني للأنظمة المفتوحة (OSI). وهي تنشئ إطاراً لتنسيق وضع التوصيات الحالية والمستقبلية بشان التوصيل البيني للأنظمة.

ويهدف التوصيل البيني للأنظمة المفتوحة للسماح بالتوصيل البيني لأنظمة الحاسوب غير المتجانسة بحيث يمكن تحقيق التواصل المفيد بين عمليات التطبيق. وفي أوقات مختلفة، يجب وضع ضوابط أمنية من أجل حماية المعلومات المتبادلة بين عمليات التطبيق. وينبغي لهذه الضوابط أن تجعل تكلفة الحصول على البيانات أو تعديلها بطريقة غير سليمة أكبر من القيمة المحتملة للقيام بذلك، أو أن تطيل الوقت اللازم للحصول على البيانات بشكل غير سليم إلى حد تُهدر فيه قيمة البيانات.

وتعرّف هذه التوصية العناصر المعمارية العامة المتعلقة بالأمن التي يمكن تطبيقها على نحو ملائم في الظروف التي تتطلب حماية الاتصالات بين الأنظمة المفتوحة. وتضع، في إطار نموذج مرجعي، خطوطاً توجيهية وتقييدات لتحسين التوصيات الحالية أو لوضع توصيات جديدة في سياق توصيل بيني للأنظمة المفتوحة من أجل السماح بتأمين الاتصالات، ومن ثم توفير منهج متسق للأمن في التوصيل البيني للأنظمة المفتوحة.

ويستفاد من وجود خلفية في مجال الأمن لفهم هذه التوصية. وينصح القارئ غير المتمرس في مجال الأمن بقراءة الملحق أولاً.

وتتوسع هذه التوصية في النموذج المرجعي (التوصية X.200) لتشمل جوانب الأمن التي تشكل عناصر معمارية عامة في بروتوكولات الاتصالات، والتي لم يرد بحثها في النموذج المرجعي.

1 نطاق ومجال التطبيق

إن هذه التوصية:

أ) توفر وصفاً عاماً لخدمات الأمن والآليات ذات الصلة التي قد يوفرها النموذج المرجعي؛

ب) تعرّف الحالات في النموذج المرجعي حيث يمكن توفير الخدمات والآليات.

وتوسع هذه التوصية مجال تطبيق التوصية X.200، ليشمل الاتصالات الآمنة بين الأنظمة المفتوحة.

وقد حُددت خدمات الأمن والآليات الأساسية وتموضعها المناسب في جميع طبقات النموذج المرجعي. وبالإضافة إلى ذلك، حُددت العلاقات المعمارية للخدمات والآليات الأمنية مع النموذج المرجعي. وقد تكون هناك حاجة إلى إجراءات أمنية إضافية في الأنظمة الطرفية والمنشآت والمنظمات. وتسري هذه التدابير في سياقات تطبيق مختلفة. ويقع تعريف خدمات الأمن اللازمة لدعم مثل هذه التدابير الأمنية الإضافية خارج نطاق التوصية.

لا تعنى الوظائف الأمنية للتوصيل البيني للأنظمة المفتوحة (OSI) إلا بالجوانب المرئية من مسير الاتصالات التي تسمح للأنظمة الطرفية بتحقيق نقل آمن للمعلومات فيما بينها. ولا يعنى أمن التوصيل البيني للأنظمة المفتوحة بالتدابير الأمنية اللازمة في الأنظمة الطرفية والمنشآت والمنظمات، إلا إذا كانت لها آثار مرئية على اختيار ووضعية خدمات الأمن في التوصيل البيني للأنظمة المفتوحة. ويمكن تقييس هذه الجوانب الأخيرة من الأمن ولكنها لا تقع في نطاق توصيات التوصيل البيني للأنظمة المفتوحة.

وإذ تضيف هذه التوصية إلى المفاهيم والمبادئ المحددة في التوصية X.200، فهي لا تعدلها. وهي لا توصِّف التنفيذ ولا تشكل أساساً لتقييم مطابقة حالات التنفيذ الفعلية.

2 المراجع

التوصية X.200 – النموذج المرجعي للتوصيل البيني للأنظمة المفتوحة في تطبيقات اللجنة الاستشارية الدولية للبرق والهاتف.

[1] هناك تواؤم تقني بين التوصية X.800 والمعيار ISO 7498-2 (أنظمة معالجة المعلومات – التوصيل البيني للأنظمة المفتوحة – النموذج المرجعي الأساسي – الجزء 2: معمارية الأمن).

ISO 7498 – Information processing systems – Open systems interconnection – Basic Reference Model (1984).

ISO 7498-4 – Information processing systems – Open systems interconnection – Basic Reference Model – Part 4: Management framework (1989).

ISO 7498/AD1 – Information processing systems – Open systems interconnection – Basic Reference Model – Addendum 1: Connectionless-mode transmission (1987).

ISO 8648 – Information processing systems – Open systems interconnection – Internal organization of the network layer (1988).

3 التعاريف والمختصرات

1.3 تستند هذه التوصية إلى المفاهيم التي وُضعت في التوصية X.200 وهي تستخدم المصطلحات التالية المعرفَّة فيها:

أ) (N)–توصيل؛

ب) (N)–إرسال–بيانات؛

ج) (N)–كيان؛

د) (N)–مرفق؛

ه) (N)–طبقة؛

و) نظام مفتوح؛

ز) الكيانات النظيرة؛

ح) (N)–بروتوكول؛

ط) (N)–وحدة–بيانات–بروتوكول

ي) (N)–مرحِّل؛

ل) التسيير؛

م) التتابع؛

ن) (N)–خدمة؛

س) (N)–وحدة–بيانات– خدمة؛

ع) (N)–بيانات–مستخدم؛

ف) شبكة فرعية؛

ص) مورد التوصيل البيني للأنظمة المفتوحة (OSI)؛

ق) قواعد نظم النقل.

2.3 تستخدم هذه التوصية المصطلحات التالية المستمدة من التوصيات/المعايير الدولية ذات الصلة:

إرسال بالأسلوب الخالي من التوصيل (ISO 7498/AD1)

نظام طرفي (التوصية X.200/المعيار ISO 7498)

وظيفة الترحيل والتسيير (ISO 8648)

قاعدة معلومات الإدارة (MIB) (ISO 7498-4)

وبالإضافة إلى ذلك، تُستخدم المختصرات التالية:

OSI للتوصيل البيني للأنظمة المفتوحة؛

SDU لوحدة بيانات الخدمة؛

SMIB لقاعدة معلومات إدارة الأمن؛

MIB لقاعدة معلومات الإدارة.

3.3 لأغراض هذه التوصية، تسري التعاريف التالية:

1.3.3 *التحكم في النفاذ*

منع استخدام غير مرخص به لمورد ما، بما في ذلك منع استخدام مورد بطريقة غير مرخص بها.

2.3.3 *قائمة التحكم في النفاذ*

قائمة بالكيانات المرخص لها بالنفاذ إلى مورد ما، مشفوعة بحقوق هذه الكيانات في النفاذ.

3.3.3 *المساءلة*

الخاصية التي تضمن أن أعمال كيان ما يمكن إسنادها إلى ذلك الكيان حصراً.

4.3.3 *التهديد النشِط*

تهديد بتغيير متعمد غير مخول لحالة نظام.

ملاحظة – قد تشمل أمثلة التهديدات النشطة المتعلقة بالأمن: إدخال تعديل على الرسائل وتكرار الرسائل وإدراج رسائل هامشية وانتحال صفة كيان مخول والحرمان من الخدمة.

5.3.3 *التدقيق*

انظر التدقيق الأمني.

6.3.3 *سجل التدقيق*

انظر سجل التدقيق الأمني.

7.3.3 *الاستيقان*

انظر الاستيقان من مصدر البيانات والاستيقان من الكيان النظير.

ملاحظة – في هذه التوصية، لا يُستخدم مصطلح "الاستيقان" فيما يتعلق بسلامة البيانات، بل يُستخدم بدلاً منه مصطلح "سلامة البيانات".

8.3.3 *معلومات الاستيقان*

المعلومات المستخدمة للتثبت من صحة الهوية المدعاة.

9.3.3 *تبادل الاستيقان*

آلية القصد منها التأكد من هوية كيان بواسطة تبادل المعلومات.

10.3.3 *التخويل*

منح الحقوق، الذي يتضمن إتاحة النفاذ استناداً إلى حقوق النفاذ.

11.3.3 *التيسر*

خاصية إمكانية النفاذ وإمكانية الاستعمال بناءً على طلب من كيان مخول.

12.3.3 *المقدرة*

تأشيرة تستخدم كمعرّف لمورد بحيث تضفي حيازة التأشيرة حقوق نفاذ إلى المورد.

13.3.3 *القناة*

مسير نقل المعلومات.

14.3.3 *نص التجفير*

بيانات منتجة من خلال استخدام التجفير. ولا يتاح المحتوى الدلالي للبيانات الناتجة.

ملاحظة – قد يخضع النص المجفَّر نفسه للتجفير، بحيث يكون الناتج نصاً مضاعف التجفير.

15.3.3 *نص واضح*

بيانات مفهومة يكون محتوى دلالاتها متاحاً.

16.3.3 *الكتمان*

خاصية عدم إتاحة المعلومات أو الكشف عنها لأشخاص غير مخولين أو لكيانات، أو عمليات غير مُخَوَّلَة.

17.3.3 *بيانات الاعتماد*

بيانات تُنقل لإثبات هوية الكيان المدّعاة.

18.3.3 *تحليل التجفير*

تحليل نظام مجفر و/أو مدخلاته ومخرجاته لاستخراج متغيرات سرية و/أو بيانات حساسة بما في ذلك نص واضح.

19.3.3 *قيمة التحقق التجفيرية*

المعلومات المشتقة من إجراء تحويل تجفيري (انظر علم التجفير) على وحدة البيانات.

ملاحظة – يمكن القيام باشتقاق قيمة التحقق في واحدة أو أكثر من الخطوات ويأتي هذا الاشتقاق نتيجة لدالة رياضية للمفتاح ووحدة البيانات. وهو يُستخدم عادة للتحقق من سلامة وحدة البيانات.

20.3.3 *علم التجفير*

التخصص الذي يجسد مبادئ ووسائل وطرائق تحويل البيانات من أجل إخفاء محتواها من المعلومات ومنع تعديلها خلسة و/أو منع استخدامها غير المرخص به.

ملاحظة – يحدد علم التجفير الطرائق المستخدمة في التجفير وفك التجفير. ويعتبر الهجوم على أي مبدأ أو وسيلة أو طريقة للتجفير بمثابة تحليل للتجفير.

21.3.3 *سلامة البيانات*

خاصية بقاء البيانات على حالتها دون أن يطرأ عليها تغيير أو تلف بطريقة غير مرخص بها.

22.3.3 *الاستيقان من أصل البيانات*

التأكد من أن مصدر البيانات المتلقاة هو المصدر المزعوم.

23.3.3 *فك التشفير*

عكس عملية تشفير قابلة لذلك.

24.3.3 *فك التجفير*

انظر فك التشفير.

25.3.3 *الحرمان من الخدمة*

منع نفاذ مرخص له إلى الموارد أو تأخير عمليات حرجة التوقيت.

26.3.3 *التوقيع الرقمي*

بيانات ملحقة أو تحويل مجفر (انظر علم التجفير) لوحدة بيانات تسمح لمتلقي وحدة بيانات أن يثبت مصدر وسلامة وحدة البيانات، وتحميها من التزوير، من جانب المتلقي مثلاً.

27.3.3 *التشفير*

التحويل المجفر للبيانات (انظر علم التجفير) لإنتاج نص مشفر.

ملاحظة – قد يكون التشفير غير قابل للعكس، وفي هذه الحالة لا يمكن إجراء عملية فك التشفير المقابلة.

28.3.3 *التجفير*

انظر التشفير.

29.3.3 *تشفير من طرف إلى طرف*

تشفير البيانات ضمن نظام أو في طرف مصدره يقابله فك تشفير لا يحدث إلا ضمن نظام أو في طرف مقصده. (انظر أيضاً التشفير من وصلة إلى وصلة).

30.3.3 *سياسة أمنية قائمة على الهوية*

سياسة أمنية قائمة على هويات و/أو نعوت المستعملين أو مجموعة المستعملين أو الكيانات العاملة نيابة عن المستعملين والموارد/الأغراض الجاري النفاذ إليها.

31.3.3 *السلامة*

انظر سلامة البيانات.

32.3.3 *مفتاح*

متوالية رموز تتحكم في عمليات التشفير وفك التشفير.

33.3.3 *إدارة مفاتيح*

توليد المفاتيح وتخزينها وتوزيعها وإلغاؤها وأرشفتها وتطبيقها طبقاً لسياسة الأمن.

34.3.3 *تشفير من وصلة إلى وصلة*

تطبيق فردي لتشفير البيانات على كل وصلة في نظام الاتصالات. (انظر أيضاً تشفير من طرف إلى طرف).

ملاحظة – تطبيق التشفير وصلة بوصلة هو أن تكون البيانات في شكل نص واضح في كيانات ترحيل.

35.3.3 *كشف التلاعب*

آلية تستخدم لكشف ما إذا كانت البيانات قد عُدلت (سواء عَرَضياً أو عمداً).

36.3.3 *انتحال صفة*

ادعاء كيان بأنه كيان آخر.

37.3.3 *التوثيق*

تسجيل البيانات لدى طرف ثالث موثوق به يسمح لاحقاً بتأكيد دقة خصائص البيانات من حيث المحتوى والأصل والوقت والتسليم مثلاً.

38.3.3 *تهديد مستتر*

تهديد بإفشاء غير مرخص به لمعلومات دون تغيير في حالة النظام.

39.3.3 *كلمة المرور*

معلومات الاستيقان السرية وتتألف عادة من سلسلة سمات.

40.3.3 *الاستيقان من الكيان النظير*

تأكيد أن الكيان النظير المصاحب هو من يدعي كونه.

41.3.3 *الأمن المادي*

تدابير مستخدمة لتوفير حماية مادية لموارد من تهديدات متعمدة أو عارضة.

42.3.3 *السياسة المرعية*

انظر سياسة الأمن.

43.3.3 *الخصوصية*

حق الأفراد في التحكم أو التأثير فيما يتناول المعلومات التي تتعلق بهم من حيث جمعها وتخزينها ومن يقوم بذلك ولمن يجوز إفشاء هذه المعلومات.

ملاحظة – بما أن هذا المصطلح يتعلق بحق الأفراد فإنه لا يمكن أن يكون دقيقاً جداً وينبغي تجنب استخدامه إلا كدافع لاشتراط الأمن.

44.3.3 *التنصل*

إنكار أحد الكيانات المشاركة في الاتصال أنه قد شارك في الاتصال بالكامل أو في جزء منه.

45.3.3 *التحكم في التسيير*

تطبيق قواعد خلال عملية التسيير من أجل اختيار أو تجنب شبكات أو وصلات أو ترحيلات محددة.

46.3.3 *سياسة أمن قائمة على القواعد*

سياسة أمن قائمة على قواعد شاملة تفرض على جميع المستعملين. وتعتمد هذه القواعد على مقارنة حساسية الموارد التي يجري النفاذ إليها وامتلاك خواص متطابقة لمستعملين أو مجموعة مستعملين أو كيانات تعمل نيابة عن مستعملين.

47.3.3 *تدقيق أمني*

استعراض مستقل وفحص لسجلات النظام وأنشطته بغية اختبار مدى كفاية ضوابط النظام، ولضمان الامتثال للسياسات والإجراءات التشغيلية المعمول بها، ولكشف الخروقات الأمنية، وللتوصية بأي تغييرات ضرورية في الضوابط والسياسات والإجراءات.

48.3.3 *سجل التدقيق الأمني*

بيانات مجمعة قد تُستخدم لتيسير التدقيق الأمني.

49.3.3 *وسم أمني*

وسم مرتبط بمصدر (قد يكون وحدة بيانات) يسمي أو يعين نعوت الأمن لذلك المصدر.

ملاحظة – قد يكون الوسم و/أو الإسناد واضحاً أو ضمنياً.

50.3.3 *سياسة الأمن*

مجموعة معايير لتوفير خدمات الأمن (انظر أيضاً سياسة الأمن القائمة على الهوية والقائمة على القواعد).

ملاحظة – تتناول سياسة الأمن الكاملة بالضرورة شواغل كثيرة تقع خارج نطاق التوصيل البيني للأنظمة المفتوحة.

51.3.3 *خدمة الأمن*

خدمة توفرها طبقة في أنظمة الاتصالات المفتوحة تضمن الأمن الكافي للأنظمة أو لنقل البيانات.

52.3.3 *الحماية الانتقائية للمجالات*

حماية مجالات محددة في رسالة تُرسَل.

53.3.3 *الحساسية*

خاصية المورد التي تتضمن قيمته أو أهميته وقد تشمل الثغرات الأمنية فيه.

54.3.3 *التوقيع*

انظر التوقيع الرقمي.

55.3.3 *التهديد*

خرق أمني محتمل.

56.3.3 *تحليل الحركة*

استدلال معلومات من ملاحظة تدفقات الحركة (وجودها وغيابها وكميتها واتجاهها وتواترها).

57.3.3 *كتم تدفق الحركة*

خدمة كتم لحماية تحليل الحركة.

58.3.3 *حشو الحركة*

توليد حالات هامشية للاتصالات ووحدات بيانات هامشية و/أو بيانات هامشية في وحدات البيانات.

59.3.3 *خاصية وظيفية موثوقة*

خاصية وظيفية تبدو صحيحة فيما يتعلق ببعض المعايير، كما تحددها سياسة الأمن مثلاً.

4 الترميز

إن ترميز الطبقة المستخدم هو نفسه المعرَّف في التوصية X.200.

ومصطلح "الخدمة" يُستخدم للإشارة إلى خدمة الأمن، حيثما لا يُنعت خلاف ذلك.

5 الوصف العام للخدمات والآليات الأمنية

1.5 *نظرة عامة*

يرد في هذه الفقرة بحث خدمات الأمن المشمولة في معمارية وآليات أمن التوصيل البيني للأنظمة المفتوحة (OSI) التي تنفِّذ تلك الخدمات. وخدمات الأمن المبينة أدناه هي خدمات الأمن الأساسية. وفي الممارسة العملية، سيجري تنفيذها في طبقات مناسبة وتوليفات مناسبة، مع خدمات وآليات مغايرة عادةً للتوصيل البيني للأنظمة المفتوحة، لتلبية السياسة الأمنية و/أو متطلبات المستخدم. ويمكن استخدام آليات أمنية خاصة لتنفيذ توليفات من خدمات الأمن الأساسية. والتنفيذ العملي للأنظمة يمكن أن يطبق توليفات معينة من خدمات الأمن الأساسية للتشغيل المباشر.

2.5 *خدمات الأمن*

تعتبر الخدمات التالية خدمات أمن يمكن توفيرها اختيارياً ضمن إطار النموذج المرجعي للتوصيل البيني للأنظمة المفتوحة (OSI). وتتطلب خدمات الاستيقان معلومات الاستيقان التي تضم المعلومات والبيانات المخزنة محلياً التي تُنقل (بيانات الاعتماد) لتسهيل الاستيقان.

1.2.5 *الاستيقان*

تتيح هذه الخدمات الاستيقان من الكيان النظير المتصل ومصدر البيانات على النحو الموضح أدناه.

1.1.2.5 *الاستيقان من الكيان النظير*

عندما تقدم الطبقة (N) هذه الخدمة، فهي تقدم إفادة مؤيدة إلى الكيان – (N + 1) بأن الكيان هو الكيان النظير المدّعى للكيان – (N + 1).

وتقدَّم هذه الخدمة للاستخدام في إنشاء مرحلة نقل بيانات توصيل، أو خلالها في بعض الأحيان، لتأكيد هوية واحدة أو أكثر للكيانات الموصولة. وتوفر هذه الخدمة الثقة، في وقت الاستخدام فقط، في أن الكيان لا يحاول انتحال صفة أو تكرار توصيل سابق على نحو غير

مخوَّل. ويمكن تنفيذ خطط الاستيقان من الكيان النظير في اتجاه واحد أو متبادل، مع أو من دون التحقق الآني، ويمكن أن يوفر ذلك درجات متفاوتة من الحماية.

2.1.2.5 *الاستيقان من مصدر البيانات*

عندما تقدم الطبقة (N) هذه الخدمة، فهي تقدم إفادة مؤيدة إلى الكيان – (N + 1) بأن مصدر البيانات هو الكيان النظير المدّعى للكيان – (N + 1).

وتوفر خدمة الاستيقان من مصدر البيانات إفادة مؤكدة لمصدر وحدة البيانات. ولا توفر هذه الخدمة حماية ضد نسخ أو تعديل وحدات البيانات.

2.2.5 *التحكم في النفاذ*

توفر هذه الخدمة الحماية ضد الاستخدام غير المخوَّل لموارد يمكن الوصول إليها عبر التوصيل البيني للأنظمة المفتوحة (OSI). وقد تخص هذه الموارد التوصيل البيني للأنظمة المفتوحة أو غيره، ويجري النفاذ إليها عبر بروتوكولات التوصيل البيني للأنظمة المفتوحة. ويمكن تطبيق خدمة الحماية هذه على أنواع متنوعة من النفاذ إلى مورد (مثل استخدام مورد الاتصالات؛ وقراءة مورد المعلومات أو كتابته أو حذفه، وتنفيذ مورد المعالجة) أو على جميع حالات النفاذ إلى مورد.

ويكون التحكم في النفاذ وفقاً لسياسات الأمن المختلفة (انظر الفقرة 1.1.2.6).

3.2.5 *كتم البيانات*

تتيح هذه الخدمات حماية البيانات من الكشف غير المخوَّل على النحو الموضح أدناه.

1.3.2.5 *كتم التوصيل*

توفر هذه الخدمة كتمان جميع بيانات المستخدم – (N) على التوصيل – (N).

ملاحظة – حسب الاستخدام والطبقة، قد لا تكون حماية جميع البيانات مناسبة، ومثال ذلك البيانات المعجلة أو البيانات في طلب توصيل.

2.3.2.5 *الكتمان عند الاستغناء عن التوصيل*

توفر هذه الخدمة كتمان جميع بيانات المستخدم – (N) في وحدة واحدة لبيانات الخدمة – (N) خالية من التوصيل.

3.3.2.5 *كتم المجالات الانتقائي*

توفر هذه الخدمة كتمان مجالات منتقاة ضمن بيانات المستخدم – (N) على التوصيل – (N) أو في وحدة واحدة لبيانات الخدمة – (N) خالية من التوصيل.

4.3.2.5 *كتم تدفق الحركة*

توفر هذه الخدمة حماية المعلومات التي قد تستقى من مراقبة تدفقات الحركة.

4.2.5 *سلامة البيانات*

تتصدى هذه الخدمات للتهديدات النشطة وقد تتخذ أحد الأشكال الموضحة أدناه.

ملاحظة – في توصيل ما، يمكن لاستخدام خدمة الاستيقان من الكيان النظير في بداية التوصيل وخدمة سلامة البيانات طيلة قيام التوصيل، أن يوفر تأكيداً لمصدر كل وحدات البيانات المنقولة على توصيل ولسلامة وحدات البيانات تلك، وقد يتيح بالإضافة إلى ذلك كشف نسخ وحدات البيانات، عن طريق استخدام أرقام التتابع على سبيل المثال.

1.4.2.5 *سلامة التوصيل مع تدارك البيانات*

توفر هذه الخدمة سلامة جميع بيانات المستخدم – (N) على التوصيل – (N)، وتكشف أي تعديل أو دس أو حذف أو تكرار لأي من البيانات ضمن كامل تتابع وحدة بيانات الخدمة (SDU) (مع محاولة تدارك البيانات).

2.4.2.5 *سلامة التوصيل دون تدارك البيانات*

كما في الفقرة 1.4.2.5، ولكن دون السعي لتدارك البيانات.

3.4.2.5 *سلامة التوصيل الانتقائية حسب المجالات*

توفر هذه الخدمة سلامة مجالات منتقاة ضمن بيانات المستخدم – (N) في وحدة بيانات الخدمة – (N) المنقولة عبر توصيل، وتأخذ شكل تحديد ما إذا كانت المجالات المنتقاة قد عُدلت أو دُست أو حُذفت أو استُعرضت.

4.4.2.5 *السلامة بدون توصيل*

عندما تقدم الطبقة – (N) هذه الخدمة، فهي توفر ضمان السلامة إلى الكيان (N + 1) صاحب الطلب.

وتوفر هذه الخدمة السلامة في وحدة واحدة لبيانات الخدمة – (N) خالية من التوصيل وقد تأخذ شكل تحديد ما إذا كانت وحدة بيانات الخدمة (SDU) الواردة قد تعرضَّت للتعديل. وبالإضافة إلى ذلك، يمكن تقديم شكل محدود من كشف تكرار البيانات.

5.4.2.5 *السلامة الانتقائية حسب المجالات دون التوصيل*

توفر هذه الخدمة سلامة مجالات منتقاة في وحدة واحدة لبيانات الخدمة خالية من التوصيل. وتأخذ هذه الخدمة شكل تحديد ما إذا كانت المجالات المنتقاة قد تعرضَّت للتعديل.

5.2.5 *عدم التنصل*

هذه الخدمة قد تتخذ واحداً من شكلين أو كليهما.

1.5.2.5 *عدم التنصل بإثبات المصدر*

يزوَّد متلقي البيانات بإثبات لأصل البيانات. وسيقي ذلك من أي محاولة من جانب المرسل لأن ينكر زوراً إرسال البيانات أو محتوياتها.

2.5.2.5 *عدم التنصل بإثبات الإيصال*

يزوَّد مرسل البيانات بإثبات لإيصال البيانات. وسيقي ذلك من أي محاولة لاحقة من جانب المتلقي لأن ينكر زوراً تلقي البيانات أو محتوياتها.

3.5 *آليات أمنية محددة*

يمكن إدراج الآليات التالية في الطبقة – (N) المناسبة من أجل تقديم بعض الخدمات الموضحة في الفقرة 2.5.

1.3.5 *التشفير*

1.1.3.5 يمكن للتشفير أن يبقي إما البيانات أو معلومات تدفق الحركة طي الكتمان، ويمكن أن يؤدي دوراً في عدد من آليات الأمن الأخرى أو أن يتممها على النحو الموضح في الفقرات التالية.

2.1.3.5 يمكن أن تكون خوارزميات التشفير عكوسة أو غير عكوسة. وهناك نوعان من التصنيفات العامة لخوارزمية التشفير العكوسة:

أ) تشفير متناظر (أي مفتاح سري)، الذي تعني فيه معرفة مفتاح التشفير ضمناً معرفة مفتاح فك التشفير وبالعكس؛

ب) تشفير غير متناظر (مثل المفتاح العمومي)، الذي لا تعني فيه معرفة مفتاح التشفير ضمناً معرفة مفتاح فك التشفير وبالعكس. ويشار إلى اثنين من مفاتيح مثل هذا النظام أحياناً باسم "المفتاح العمومي" و"المفتاح الخاص".

ويمكن لخوارزميات التشفير غير العكوسة أن تستخدم أو لا تستخدم مفتاحاً. وعندما تستخدم مفتاحاً، قد يكون هذا المفتاح علنياً أو سرياً.

3.1.3.5 ويعني وجود آلية تشفير ضمناً استخدام آلية لإدارة مفاتيح، إلا في حالة بعض خوارزميات التشفير غير العكوسة. وترد في الفقرة 4.8 بعض المبادئ التوجيهية بشأن منهجيات إدارة المفاتيح.

2.3.5 *آليات التوقيع الرقمي*

تحدد هذه الآليات إجراءين:

أ) توقيع وحدة بيانات؛

ب) التحقق من وحدة البيانات الموقعة.

وتستخدم العملية الأولى معلومات خاصة (أي فريدة وسرية) بالنسبة إلى الموقّع. وتستخدم العملية الثانية الإجراءات والمعلومات المتاحة علناً والتي لا يمكن استنتاج معلومات الموقّع الخاصة منها.

1.2.3.5 تنطوي عملية التوقيع إما على تشفير وحدة البيانات أو إنتاج قيمة تحقق تجفيرية من وحدة البيانات، وذلك باستخدام معلومات الموقِّع الخاصة باعتبارها مفتاحاً خاصاً.

2.2.3.5 وتنطوي عملية التحقق على استخدام الإجراءات والمعلومات العلنية لتحديد ما إذا كانت تنتج التوقيع مع معلومات الموقِّع الخاصة.

3.2.3.5 وتتمثل السمة الأساسية لآلية التوقيع في تعذر إنتاج التوقيع باستخدام معلومات الموقِّع الخاصة. وبالتالي عندما يُتحقق من التوقيع، يمكن بعد ذلك أن يثبَت لطرف ثالث (مثل قاض أو محكم) في أي وقت أن لا أحد سوى المالك الأوحد للمعلومات الخاصة يمكنه أن ينتج التوقيع.

3.3.5 *آليات التحكم في النفاذ*

1.3.3.5 يمكن لهذه الآليات استخدام هوية كيان أو معلومات عن الكيان مستيقَن منها (مثل العضوية في مجموعة معروفة من الكيانات) أو قدرات للكيان، من أجل تحديد وإنفاذ حقوق النفاذ للكيان. فإذا حاول الكيان استخدام مورد غير مخوَّل به، أو مورد مخوَّل به بنمط غير مناسب من النفاذ، سترفض وظيفة التحكم في النفاذ المحاولة وقد تبلغ عن الحادثة بالإضافة إلى ذلك لأغراض توليد إنذار و/أو تسجيلها كجزء سجل التدقيق الأمني. ولا يمكن تقديم أي إشعار إلى المرسل بالحرمان من النفاذ من أجل إرسال بيانات دون توصيل إلا كنتيجة للضوابط المفروضة على النفاذ في المصدر.

2.3.3.5 ويمكن لآليات التحكم في النفاذ أن تستند، على سبيل المثال، إلى استخدام واحد أو أكثر مما يلي:

أ) قواعد معلومات التحكم في النفاذ، حيث تُحفظ حقوق نفاذ الكيانات النظيرة. يمكن الحفاظ على هذه المعلومات من خلال مراكز تخويل أو من جانب الكيان الذي يُنفذ إليه، ويمكن أن تكون في شكل قائمة تحكم في النفاذ أو مصفوفة ذات بنية تراتبية أو موزعة. وهذا يفترض أن الاستيقان من الكيان النظير قد ضُمن.

ب) معلومات الاستيقان مثل كلمات المرور، التي يُستدل من حيازتها وعرضها لاحقاً على كون الكيان القائم بالنفاذ مخولاً؛

ج) قدرات يُستدل من حيازتها وعرضها لاحقاً على الحق في النفاذ إلى الكيان أو الموارد التي تحددها القدرة.

ملاحظة – يجب ألا تكون القدرة قسرية وينبغي نقلها بطريقة موثوقة.

د) وسوم الأمن التي يمكن استخدامها، عندما ترتبط بكيان ما، لمنح النفاذ أو حجبه، وفقاً لسياسة الأمن عادةً.

ه) وقت محاولة النفاذ.

و) مسير محاولة النفاذ.

ز) مدة النفاذ.

3.3.3.5 يمكن تطبيق آليات التحكم في النفاذ على طرفي ارتباط اتصالات و/أو في أي نقطة وسيطة.

وتُستخدم ضوابط النفاذ المعنية في المصدر أو في أي نقطة وسيطة لتحديد ما إذا كان المرسل مخوَّلاً بالتواصل مع المتلقي و/أو باستخدام موارد الاتصالات المطلوبة.

ويجب أن تُعرف مسبقاً في المصدر متطلبات آليات التحكم في النفاذ على مستوى الأقران في طرف مقصد إرسال البيانات بدون توصيل، ويجب أن تسجَّل هذه المتطلبات في قاعدة معلومات إدارة الأمن (انظر الفقرتين 2.6 و1.8).

4.3.5 *آليات سلامة البيانات*

1.4.3.5 يتمثل جانبا سلامة البيانات في سلامة وحدة بيانات واحدة أو مجال بيانات واحد، وفي سلامة تدفق وحدات أو مجالات البيانات. وبشكل عام، تُستخدم آليات مختلفة لتوفير هذين النوعين من خدمات السلامة، على أن توفير الثاني دون الأول غير عملي.

2.4.3.5 وينطوي تحديد سلامة وحدة بيانات واحدة على عمليتين، واحدة لدى الكيان المرسل والأخرى لدى كيان المتلقي. فيُلحِق الكيان المرسل كمية بوحدة بيانات تتوقف على البيانات نفسها. فقد تكون هذه الكمية معلومات تكميلية مثل شفرة التحقق من الكتلة أو قيمة التحقق التجفيرية ويمكن أن تكون هي ذاتها مشفرة. ويولد الكيان المتلقي كمية مقابلة ويقارنها مع الكمية الواردة لتحديد ما إذا كانت البيانات قد عُدلت أثناء العبور. وهذه الآلية وحدها لا تحمي ضد تكرار وحدة بيانات واحدة. وفي طبقات مناسبة من المعمارية، قد يؤدي كشف التلاعب إلى إجراءات تدارك البيانات (عن طريق إعادة الإرسال أو تصحيح الخطأ، على سبيل المثال) في تلك الطبقات أو فيما أعلى منها.

3.4.3.5 ولنقل البيانات بأسلوب التوصيل، تتطلب حماية سلامة تتابع وحدات البيانات (أي حمايتها ضد اختلال ترتيب البيانات أو ضياعها أو تكرارها أو الدس فيها أو تعديلها) بالإضافة إلى ذلك شكلاً من أشكال الترتيب الصريح مثل ترقيم التتابع أو الختم الزمني أو التسلسل التجفيري.

4.4.3.5 ولنقل البيانات بأسلوب يستغني عن التوصيل، يمكن استخدام الختم الزمني لتوفير شكل محدود من الحماية ضد تكرار وحدات البيانات الفردية.

5.3.5 *آلية تبادل الاستيقان*

1.5.3.5 فيما يلي بعض التقنيات التي يمكن تطبيقها على تبادلات الاستيقان:

أ) استخدام معلومات الاستيقان، مثل كلمات المرور التي قدمها الكيان المرسل، وفحصها من جانب الكيان المتلقي؛

ب) تقنيات التجفير؛

ج) استخدام خصائص و/أو ممتلكات الكيان.

2.5.3.5 يمكن إدراج الآليات في الطبقة (N) من أجل توفير الاستيقان من الكيان النظير. وإذا لم تنجح الآلية في الاستيقان من الكيان، يؤدي ذلك إلى حجب أو إنهاء التوصيل ويمكن أيضاً أن يتسبب بإدراج قيد في سجل التدقيق الأمني و/أو تقرير إلى مركز إدارة الأمن.

3.5.3.5 وعندما تستخدم تقنيات التجفير، فإنها قد تُجمع مع بروتوكولات "التنظيم" للحماية ضد التكرار (أي لضمان الإرسال الحي).

4.5.3.5 وستتوقف خيارات تقنيات تبادل الاستيقان على الظروف التي ستدعو الحاجة لاستخدامها فيها:

أ) الختم الزمني والميقاتيات المتزامنة؛

ب) تنظيم ثنائي أو ثلاثي الاتجاهات (للاستيقان أحادي الجانب والمتبادل على التوالي)؛

ج) خدمات عدم التنصل المنجَزة عن طريق التوقيع الرقمي و/أو آليات التوثيق.

6.3.5 *آلية حشو الحركة*

يمكن استخدام آليات حشو الحركة لتوفير مستويات مختلفة من الحماية ضد تحليل الحركة. ولا يمكن أن تكون هذه الآلية فعالة إلا إذا كان حشو الحركة محمياً بخدمة الكتمان.

7.3.5 *آلية التحكم في التسيير*

1.7.3.5 يمكن اختيار المسيّرات إما دينامياً أو بترتيب مسبق بحيث لا تُستخدم إلا الشبكات الفرعية أو المرحّلات أو الوصلات الآمنة فعلياً.

2.7.3.5 وقد ترغب الأنظمة الطرفية عند الكشف عن هجمات تلاعب مستمرة، بالإيعاز إلى مقدم خدمة الشبكة بإقامة توصيل عبر مسير مختلف.

3.7.3.5 وقد تحظر سياسة الأمن عبور وسوم أمنية معينة تحمل بيانات عبر شبكات فرعية أو مرحّلات أو وصلات معينة. ويمكن أيضاً للمبادر بالتوصيل (أو مرسل وحدة بيانات بدون توصيل) أن يحدد محاذير التسيير التي تتطلب تجنب شبكات فرعية أو مرحّلات أو وصلات معينة.

8.3.5 *آلية التوثيق*

1.8.3.5 يمكن ضمان خصائص البيانات المتداولة في اتصالات بين اثنين أو أكثر من الكيانات، مثل سلامتها ومصدرها ووقتها ومقصدها، من خلال توفير آلية التوثيق. ويتوفر الضمان من طرف ثالث موثّق ويحظى بثقة الكيانات المتواصلة فيما بينها، ويملك المعلومات اللازمة لتقديم الضمانات المطلوبة بطريقة مشهود بصحتها. ويمكن لكل واقعة اتصال أن تستخدم التوقيع الرقمي والتشفير وآليات السلامة بما يتناسب مع الخدمة التي يقدمها الموثّق. وعند تنفيذ آلية التوثيق هذه، تُتداول البيانات بين الكيانات المتواصلة عبر وقائع الاتصالات المحمية والموثّق.

4.5 *آليات الأمن المنتشرة*

تصف هذه الفقرة الفرعية عدداً من الآليات التي لا تختص بها أي خدمة معينة. وهكذا لا يرد وصفها صراحةً في الفقرة 7 على أنها تقع في أي طبقة معينة. ويمكن اعتبار بعض هذه الآليات الأمنية المنتشرة كجوانب من إدارة الأمن (انظر أيضاً الفقرة 8). وترتبط أهمية هذه الآليات، بصفة عامة، مباشرة بمستوى الأمان المطلوب.

1.4.5 *الخواص الوظيفية الموثوقة*

1.1.4.5 يمكن استخدام الخواص الوظيفية الموثوقة لتوسيع نطاق آليات أمنية أخرى أو للتثبت من فعاليتها. وأي خاصية وظيفية توفر آليات الأمن مباشرة، أو توفر النفاذ إليها، ينبغي أن تكون جديرة بالثقة.

2.1.4.5 وتقع الإجراءات المستخدمة لضمان الثقة في مثل هذه الأعتدة والبرمجيات خارج نطاق هذه التوصية، وهي على أي حال تختلف باختلاف مستوى التهديد المتصور وقيمة المعلومات التي تجب حمايتها.

3.1.4.5 وهذه الإجراءات مكلفة وصعبة التنفيذ بصفة عامة. ويمكن التقليل من المشاكل باختيار معمارية تسمح بتنفيذ المهام الأمنية في وحدات يمكن أن تكون منفصلة عن الوظائف غير ذات الصلة الأمنية، وتقدَّم انطلاقاً منها.

4.1.4.5 ويجب توفير أي حماية للارتباطات فوق الطبقة التي تطبَّق فيها الحماية بوسائل أخرى، من قبيل الخواص الوظيفية الموثوقة المناسبة.

2.4.5 *وسوم الأمن*

1.2.4.5 قد تمتلك الموارد، بما في ذلك بنود البيانات، وسوماً أمنية ترتبط بها، لبيان مستوى حساسيتها مثلاً. فمن الضروري في كثير من الأحيان التعبير عن الوسم الأمني المناسب مع البيانات في طور العبور. وقد يتكون الوسم الأمني من بيانات إضافية ترتبط بالبيانات المنقولة أو قد يكون ضمنياً، ومثال ذلك أن يرد ضمناً باستخدام مفتاح محدد لتشفير البيانات أو يرد ضمناً في سياق البيانات مثل مصدرها أو مسيرها. ويجب أن تكون وسوم الأمن الصريحة واضحة المعالم كي يتسنى التحقق منها بشكل مناسب. وبالإضافة إلى ذلك، يجب أن تُسند بشكل آمن إلى البيانات التي ترتبط بها.

3.4.5 *كشف الحدث*

1.3.4.5 يتضمن كشف الحدث ذو الصلة بالأمن كشف ما يبدو انتهاكات للأمن، ويمكن أن يشمل أيضاً الكشف عن أحداث "طبيعية"، مثل النفاذ الناجح (أو تسجيل الدخول). ويمكن لكيانات ضمن التوصيل البيني للأنظمة المفتوحة (OSI) بما فيها آليات الأمن أن تكشف الأحداث ذات الصلة بالأمن. وتتولى إدارة التعامل مع الحدث توصيف ما يشكل حدثاً (انظر الفقرة 1.3.8). وعلى سبيل المثال، يمكن لكشف مختلف الأحداث ذات الصلة بالأمن أن يتسبب بواحد أو أكثر من الإجراءات التالية:

أ) الإبلاغ محلياً عن الحدث؛

ب) الإبلاغ عن الحدث عن بُعد؛

ج) تسجيل الحدث (انظر الفقرة 3.4.5)؛

د) إجراءات التدارك (انظر الفقرة 4.4.5).

ومن أمثلة هذه الأحداث ذات الصلة بالأمن:

أ) انتهاك أمني محدد؛

ب) حدث مختار محدد؛

ج) فيض تعداد عدد الوقائع.

2.3.4.5 والتقييس في هذا المجال سيأخذ في الاعتبار إرسال المعلومات ذات الصلة بإعداد تقارير الأحداث وتسجيل الأحداث، والتعريف النحوي والدلالي الذي سيُستخدم لإرسال التقارير المبلغة عن الأحداث وتسجيل الأحداث.

4.4.5 *سجل التدقيق الأمني*

1.4.4.5 توفر سجلات التدقيق الأمني آلية أمنية قيّمة لما تنطوي عليه من إمكانية الكشف والتحقيق في انتهاكات الأمن من خلال السماح بالتدقيق الأمني اللاحق. والتدقيق الأمني هو استعراض وفحص مستقل لسجلات وأنشطة النظام من أجل اختبار كفاية ضوابط النظام، لضمان الامتثال لسياسات وإجراءات التشغيل المقررة، وللمساعدة في تقييم الأضرار، وللتوصية بأي تغييرات لازمة في الضوابط والسياسة والإجراءات المشار إليها. ويتطلب التدقيق الأمني تسجيل المعلومات ذات الصلة بالأمن في سجل التدقيق الأمني، وتحليل وإبلاغ المعلومات من هذا السجل. ويعتبر التدوين أو التسجيل آلية أمنية ويرد وصفها في هذه الفقرة. ويُعتبر التحليل وإنتاج التقارير وظيفة إدارة أمن (انظر الفقرة 2.3.8).

2.4.4.5 ويمكن تكييف جمع معلومات سجل التدقيق الأمني وفق متطلبات مختلفة بتحديد نوع (أو أنواع) الأحداث ذات الصلة بالأمن التي يتعين تسجيلها (خروقات أمنية ماثلة للعيان أو إكمال عمليات ناجحة).

ولعل العلم بوجود سجل تدقيق أمني يكون رادعاً لبعض المصادر المحتملة للهجمات المخلة بالأمن.

3.4.4.5 وستراعي اعتبارات سجل التدقيق الأمني ماهية المعلومات التي يتعين تسجيلها اختيارياً وماهية الظروف التي يتعين فيها تسجيل تلك المعلومات، والتعريف النحوي والدلالي الذي يتعين استخدامه لتبادل معلومات سجل التدقيق الأمني.

5.4.5 *استعادة الأمن*

1.5.4.5 تتعامل استعادة الأمن مع الطلبات المقدمة من آليات مثل وظائف التعامل مع الحدث وإدارته، وتتخذ إجراءات الاستعادة نتيجة لتطبيق مجموعة من القواعد. ويمكن أن تكون إجراءات الاستعادة هذه على ثلاثة أنواع:

أ) فورية؛

ب) مؤقتة؛

ج) طويلة الأمد.

فعلى سبيل المثال:

الإجراءات الفورية قد تؤدي إلى إجهاض فوري للعمليات، من قبيل فصل التوصيل.

والإجراءات المؤقتة قد تؤدي إلى نزع صلاحية كيان مؤقتاً.

وقد تُدرج الإجراءات طويلة الأمد كياناً في "القائمة السوداء" أو تغير مفتاحاً.

2.5.4.5 وتتضمن مواضيع التقييس بروتوكولات لإجراءات الاستعادة ولإدارة استعادة الأمن (انظر الفقرة 3.3.8).

5.5 *بيان العلاقة بين خدمات وآليات الأمن*

يوضح الجدول 1/X.800 أي آليات تُعتبر في بعض الأحيان، بمفردها أو بالاشتراك مع آليات أخرى، مناسبة لتقديم كل خدمة. ويقدم هذا الجدول لمحة عامة عن هذه العلاقات وهو ليس جدولاً نهائياً. ويرد وصف الخدمات والآليات المشار إليها في هذا الجدول في الفقرتين 2.5 و3.5. ويدرج وصف أكمل لهذه العلاقات في الفقرة 6.

الجدول 1/X.800

بيان العلاقة بين خدمات وآليات الأمن

آلية / خدمة	تشفير	التوقيع الرقمي	التحكم في النفاذ	سلامة البيانات	تبادل الاستيقان	حشو الحركة	التحكم في التسيير	التوثيق
الاستيقان من الكيان النظير	ن	ن	.	.	ن	.	.	.
الاستيقان من مصدر البيانات	ن	ن	.	.	.	.	.	.
خدمة التحكم في النفاذ	.	.	ن	.	.	.	.	.
كتم التوصيل	ن	.	.	.	.	.	ن	.
الكتمان عند الاستغناء عن التوصيل	ن	.	.	.	.	.	ن	.
كتم المجالات الانتقائي	ن	.	.	.	.	.	.	.
كتم تدفق الحركة	ن	.	.	.	.	ن	ن	.
سلامة التوصيل مع تدارك البيانات	ن	.	.	ن	.	.	.	.
سلامة التوصيل دون تدارك البيانات	ن	.	.	ن	.	.	.	.
سلامة التوصيل الانتقائية حسب المجالات	ن	.	.	ن	.	.	.	.
السلامة الانتقائية حسب المجالات دون التوصيل	ن	ن	.	ن	.	.	.	.
السلامة بدون توصيل	ن	ن	.	ن	.	.	.	.
عدم التنصل بإثبات المصدر	.	ن	.	ن	.	.	.	ن
عدم التنصل بإثبات الإيصال	.	ن	.	ن	.	.	.	ن

. لا تُعتبر هذه الآلية مناسبة.

ن نعم: تُعتبر هذه الآلية مناسبة إما من تلقاء نفسها أو بالاشتراك مع غيرها من الآليات.

ملاحظة – في بعض الحالات، توفر هذه الآلية أكثر مما هو ضروري للخدمة ذات الصلة ومع ذلك يمكن استخدامها.

6 العلاقة بين الخدمات والآليات والطبقات

1.6 *مبادئ إعداد طبقات الأمن*

1.1.6 استُخدمت المبادئ التالية من أجل تحديد توزيع خدمات الأمن على الطبقات والتموضع اللاحق لآليات الأمن في الطبقات:

أ) يجب إقلال عدد السبل البديلة لتحقيق الخدمة إلى الحد الأدنى؛

ب) من المقبول بناء أنظمة آمنة من خلال تقديم خدمات الأمن في أكثر من طبقة واحدة؛

ج) ينبغي ألا تكرر الخاصية الوظيفية الإضافية المطلوبة من أجل الأمن، بلا داع، وظائف التوصيل البيني للأنظمة المفتوحة (OSI) القائمة؛

د) ينبغي تجنب انتهاك استقلال الطبقة؛

هـ) ينبغي التقليل إلى الحد الأدنى من كمية الخواص الوظيفية الموثوقة؛

و) أينما اعتمد كيان على آلية أمنية يوفرها كيان في طبقة أدنى، ينبغي أن تبنى أي طبقات وسيطة على نحو يجعل من انتهاك الأمن غير عملي؛

ز) ينبغي تحديد الوظائف الأمنية الإضافية لطبقة بحيث لا يُستبعد تنفيذ وحدة (وحدات) محتواة ذاتياً، كلما أمكن؛

ح) يفترض أن تسري هذه التوصية على أنظمة مفتوحة تتكون من أنظمة طرفية تضم جميع الطبقات السبع وعلى أنظمة الترحيل.

2.1.6 وقد تتطلب تعاريف الخدمة في كل طبقة التعديل لتلبية طلبات خدمات الأمن، سواء كانت الخدمات المطلوبة مقدمة في تلك الطبقة أو في ما دونها.

2.6 *نموذج استدعاء الخدمات – (N) المحمية وإدارتها واستخدامها*

تنبغي قراءة هذه الفقرة الفرعية بالاقتران مع الفقرة 8 التي تتضمن بحثاً عاماً لقضايا إدارة الأمن. والقصد هو أن كيان الإدارة يمكن أن يفعّل خدمات وآليات الأمن عبر السطح البيني للإدارة و/أو باستدعاء الخدمة.

1.2.6 *تحديد ميزات الحماية لواقعة اتصالات*

1.1.2.6 *اعتبارات عامة*

تصف هذه الفقرة الفرعية استدعاء الحماية لحالات اتصالات مهيأة للتوصيل وبدون توصيل. ففي حالة الاتصالات المهيأة للتوصيل، عادة ما تُطلب/تُمنح خدمات الحماية في وقت إنشاء التوصيل. أما في حالة استدعاء خدمة بدون توصيل، فتُطلب/تُمنح الحماية لكل واقعة طلب خدمة بدون توصيل.

ومن أجل تبسيط الوصف التالي، سيُستخدم مصطلح "طلب خدمة" ليعني إما طلب خدمة إنشاء توصيل أو طلب خدمة بدون توصيل. ويمكن أن يتحقق استدعاء الحماية لبيانات منتقاة عن طريق طلب الحماية الانتقائية لمجال. فعلى سبيل المثال، يمكن القيام بذلك عن طريق إنشاء عدة توصيلات، لكل منها نوع أو مستوى مختلف من الحماية.

وتستوعب معمارية الأمن هذه مجموعة متنوعة من السياسات الأمنية بما في ذلك تلك التي تستند إلى قواعد وتلك التي تقوم على أساس الهوية وتلك التي هي مزيج من الاثنين معاً. وتستوعب معمارية الأمن أيضاً الحماية التي تفرض إدارياً وتلك المختارة دينامياً ومزيج من الاثنين معاً.

2.1.2.6 *طلبات الخدمة*

في كل طلب خدمة – (N)، يمكن أن يطلب الكيان (N + 1) الحماية الأمنية المنشودة المستهدفة. وسيحدد طلب الخدمة – (N) خدمات الأمن إلى جانب المعلمات وأي معلومات إضافية ذات صلة (مثل حساسية المعلومات و/أو وسوم الأمن) لتحقيق الحماية الأمنية المستهدفة.

وقبل كل واقعة اتصالات، يمكن للطبقة – (N) أن تنفذ إلى قاعدة معلومات إدارة الأمن (SMIB) (انظر الفقرة 1.8). وستحتوي قاعدة معلومات إدارة الأمن على معلومات عن متطلبات الحماية المفروضة إدارياً المرتبطة بالكيان (N + 1). وتلزم خاصية وظيفية موثوقة لإنفاذ هذه المتطلبات الأمنية المفروضة إدارياً.

وقد يتطلب توفير ميزات الأمن أثناء واقعة اتصالات مهيأة للتوصيل التفاوض بشأن خدمات الأمن المطلوبة. ويمكن تنفيذ الإجراءات المطلوبة للتفاوض بشأن الآليات والمعلمات إما كإجراء منفصل أو كجزء أساسي من الإجراء العادي لإقامة توصيل.

وعند تنفيذ التفاوض كإجراء منفصل، تُدرج نتائج الاتفاق (أي بشأن نوع آليات الأمن ومعلمات الأمن الضرورية لتقديم خدمات الأمن هذه) في قاعدة معلومات إدارة الأمن (انظر الفقرة 1.8).

وعند تنفيذ التفاوض كجزء أساسي من الإجراء العادي لإقامة توصيل، تخزَّن نتائج المفاوضات بين الكيانات – (N) مؤقتاً في قاعدة معلومات إدارة الأمن (SMIB). وقبل التفاوض، يتاح لكل كيان – (N) النفاذ إلى قاعدة معلومات إدارة الأمن للحصول على المعلومات المطلوبة للتفاوض.

وسترفض الطبقة – (N) طلب الخدمة إذا انتهك المتطلبات المفروضة إدارياً المسجلة في قاعدة معلومات إدارة الأمن (SMIB) للكيان – (N + 1).

وستضيف الطبقة – (N) أيضاً إلى طلب خدمات الحماية أي خدمات أمنية معرَّفة على أنها إلزامية في قاعدة معلومات إدارة الأمن للحصول على الحماية الأمنية المستهدفة.

وإن لم يحدد الكيان – (N + 1) حماية أمنية مستهدفة، تتبع الطبقة – (N) سياسة أمنية وفقاً لقاعدة معلومات إدارة الأمن التي قد تملي المضي قدماً في التواصل باستخدام الحماية الأمنية المبدئية ضمن المدى المحدد للكيان – (N + 1) في قاعدة معلومات إدارة الأمن.

2.2.6 *تقديم خدمات الحماية*

بعد تحديد توليفة المتطلبات الأمنية المفروضة إدارياً والمنتقاة دينامياً على النحو الموضح في الفقرة 1.2.6، تحاول الطبقة – (N) تحقيق الحماية المستهدفة كحد أدنى. ويتحقق ذلك من خلال أحد الأسلوبين التاليين أو كليهما:

أ) استدعاء آليات الأمن مباشرة ضمن الطبقة – (N)؛ و/أو

ب) طلب خدمات الحماية من الطبقة – (N – 1). وفي هذه الحالة، لا بد من توسيع نطاق الحماية لتشمل خدمة – (N) عن طريق الجمع بين الخاصية الوظيفية الموثوقة و/أو آليات أمنية محددة في الطبقة – (N).

ملاحظة – هذا لا يعني بالضرورة وجوب الوثوق بكل خاصية وظيفية في الطبقة – (N).

ومن ثم، تحدد الطبقة – (N) ما إذا كانت قادرة على تحقيق الحماية المستهدفة المطلوبة. فإذا كانت عاجزة عن تحقيق ذلك، لا تقع واقعة اتصالات.

1.2.2.6 *إقامة التوصيل – (N) المحمي*

يتناول البحث التالي تقديم الخدمات ضمن الطبقة – (N)؛ (بدلاً من الاعتماد على خدمات (N – 1)).

ففي بروتوكولات معينة، يعد تحقيق حماية مستهدفة مرضية وتتابع العمليات أمراً بالغ الأهمية.

أ) التحكم في النفاذ الصادر

يمكن للطبقة – (N) أن تفرض ضوابطاً على النفاذ الصادر، أي يمكن أن تحدد محلياً (من قاعدة معلومات إدارة الأمن) ما إذا كانت محاولة إقامة التوصيل – (N) متاحة أو ممنوعة.

ب) الاستيقان من الكيان النظير

إن تضمنت الحماية المستهدفة الاستيقان من الكيان النظير، أو إذا عُلم (من قاعدة معلومات إدارة الأمن) أن الكيان – (N) في المقصد سيتطلب الاستيقان من الكيان النظير، فلا بد من أن يحصل تبادل الاستيقان. وقد يستخدم ذلك تنظيماً ثنائي أو ثلاثي الاتجاهات ليوفر استيقاناً من جانب واحد أو متبادلاً، حسب الطلب.

وفي بعض الأحيان، يمكن دمج تبادل الاستيقان في إجراءات إقامة التوصيل – (N) المعتادة. وفي ظروف أخرى، يمكن تحقيق تبادل الاستيقان على نحو منفصل عن إقامة التوصيل – (N).

ج) خدمة التحكم في النفاذ

يمكن للكيان – (N) أو الكيانات الوسيطة في المقصد أن تفرض قيوداً من حيث التحكم في النفاذ. فإذا لزمت معلومات محددة من خلال آلية التحكم في النفاذ عن بُعد، يقدم الكيان – (N) المبادرة هذه المعلومات ضمن بروتوكول الطبقة -(N) أو عبر القنوات الإدارية.

د) الكتمان

إذا اختيرت خدمة الكتمان الكلية أو الانتقائية، وجبت إقامة التوصيل – (N) المحمي. ويجب أن يتضمن ذلك إنشاء ما يناسب من مفتاح عامل (أو مفاتيح عاملة) وتفاوض معلمات التجفير في التوصيل. وقد يتم ذلك بترتيب مسبق، أو في تبادل الاستيقان، أو عن طريق بروتوكول منفصل.

هـ) سلامة البيانات

إذا اختيرت سلامة جميع بيانات المستخدم – (N)، مع أو من دون تدارك البيانات، أو سلامة التوصيل الانتقائية حسب المجالات، وجبت إقامة التوصيل – (N) المحمي الذي قد يكون هو نفسه المقام لتقديم خدمة الكتمان ويمكن أن يوفر الاستيقان. وتسري نفس الاعتبارات المرعية لخدمة كتم التوصيل – (N) المحمي.

و) خدمات عدم التنصل

إذا اختير عدم التنصل بإثبات المصدر، وجب وضع معلمات التجفير السليمة، أو وجبت إقامة توصيل محمي بكيان توثيق.

وإذا اختير عدم التنصل بإثبات الإيصال، وجب وضع معلمات التجفير السليمة (التي تختلف عن تلك المطلوبة لعدم التنصل بإثبات المصدر)، أو وجبت إقامة توصيل محمي بكيان توثيق.

ملاحظة – قد تفشل إقامة التوصيل – (N) المحمي جراء عدم وجود اتفاق على معلمات التجفير (بما في ذلك ربما عدم امتلاك المفاتيح المناسبة) أو من جراء رفض من آلية التحكم في النفاذ.

3.2.6 *تشغيل التوصيل – (N) المحمي*

1.3.2.6 أثناء مرحلة نقل البيانات من التوصيل – (N) المحمي، يجب تقديم خدمات الحماية التي جرى التفاوض بشأنها.

وسيكون التالي مرئياً عند حدود الخدمة – (N):

أ) الاستيقان من الكيان النظير (على فترات)؛

ب) حماية المجالات الانتقائية؛

ج) الإبلاغ عن هجوم نشط (على سبيل المثال، عند وقوع التلاعب في البيانات وكون الخدمة المقدمة هي "سلامة التوصيل سلامة التوصيل دون تدارك البيانات" – انظر الفقرة 2.4.2.5).

بالإضافة إلى ذلك، قد تكون هناك حاجة إلى ما يلي:

أ) تسجيل سجل التدقيق الأمني؛

ب) كشف الحدث والتعامل معه.

2.3.2.6 والخدمات القابلة للتطبيق الانتقائي هي التالية:

أ) الكتمان؛

ب) سلامة البيانات (مع الاستيقان ربما)؛

ج) عدم التنصل (من جانب المتلقي أو المرسل).

الملاحظة 1 – تُقترح تقنيتان لوسم البيانات المحددة لتطبيق خدمة. أولاهما تنطوي على استخدام تنميط قوي. ويُتوقع أن تتعرف طبقة العرض التقديمي على أنماط معينة مثل تلك التي تتطلب تطبيق خدمات حماية معينة. فيما تنطوي الثانية على شكل من أشكال إبراز بنود البيانات الفردية التي ينبغي تطبيق خدمات حماية محددة لها.

الملاحظة 2 – يُفترض أن أحد أسباب تقديم التطبيق الانتقائي لخدمات عدم التنصل قد تنشأ عن السيناريو التالي: شكل من أشكال الحوار التفاوضي يحدث عبر وجود ارتباط قبل اتفاق كل من الكيانين – (N) على النسخة النهائية المقبولة للطرفين لبند البيانات. وعندئذ، قد يطلب المتلقي المقصود إلى المرسل تطبيق خدمات عدم التنصل (سواء كانت بإثبات المصدر أو إثبات الإيصال) على الصيغة النهائية المتفق عليها لبند البيانات. ويطلب المرسل هذه الخدمات ويحصل عليها، ويرسل بند البيانات، ويرده لاحقاً إشعار باستلام بند البيانات هذا وإقرار بذلك من جانب المتلقي. فتضمن خدمات عدم التنصل لكل من منشئ بند البيانات ومتلقيه أنه قد أُرسل بنجاح.

الملاحظة 3 – يستدعي المنشئ خدمتي عدم التنصل كلتيهما (أي بإثبات المصدر وبإثبات الإيصال).

4.2.6 *تقديم إرسال البيانات المحمي بدون توصيل*

لا تتوفر جميع خدمات الأمن التي تتيحها البروتوكولات المهيأة للتوصيل ضمن البروتوكولات بدون توصيل. وعلى وجه التحديد، إذا لزمت الحماية ضد هجمات الحذف والدس والتكرار، فيجب أن تقدَّم في الطبقات العليا المهيأة للتوصيل. ويمكن توفير حماية محدودة ضد هجمات التكرار من خلال آلية الختم الزمني. وبالإضافة إلى ذلك، تتعدد خدمات الأمن العاجزة عن تقديم نفس درجة إنفاذ الأمن التي يمكن تحقيقها من خلال بروتوكولات مهيأة للتوصيل.

وفيما يلي خدمات الحماية المناسبة لإرسال البيانات دون توصيل:

أ) الاستيقان من الكيان النظير (انظر الفقرة 1.1.2.5)؛

ب) الاستيقان من مصدر البيانات (انظر الفقرة 2.1.2.5)؛

ج) خدمة التحكم في النفاذ (انظر الفقرة 2.2.5)؛

د) كتم التوصيل (انظر الفقرة 2.3.2.5)؛

ه) كتم المجالات الانتقائي (انظر الفقرة 3.3.2.5)؛

و) السلامة بدون توصيل (انظر الفقرة 4.4.2.5)؛

ز) السلامة الانتقائية حسب المجالات دون التوصيل (انظر الفقرة 5.4.2.5)؛

ح) عدم التنصل بإثبات المصدر (انظر الفقرة 1.5.2.5).

ويجري تقديم الخدمات من خلال التشفير و/أو آليات التوقيع و/أو آليات التحكم في النفاذ و/أو آليات التسيير و/أو آليات سلامة البيانات و/أو آليات التوثيق (انظر الفقرة 3.5).

وعلى الجهة المبادرة بإرسال البيانات بدون توصيل أن تضمن احتواء وحدة بيانات الخدمة (SDU) الواحدة التي تخصها على جميع المعلومات المطلوبة لجعلها مقبولة في المقصد.

7 تموضع خدمات وآليات الأمن

تحدد هذه الفقرة خدمات الأمن الواجب تقديمها في إطار النموذج المرجعي الأساسي للتوصيل البيني للأنظمة المفتوحة (OSI)، وتوجز الطريقة التي يتعين أن تتحقق فيها. وتقديم أي خدمة أمن هو أمر اختياري يتوقف على الاحتياجات.

وحيثما تحدَّد خدمة أمن معينة في هذه الفقرة على أنها تقدَّم اختيارياً من طبقة معينة، فإن خدمة الأمن تلك تقدمها الآليات الأمنية العاملة داخل تلك الطبقة، ما لم ينص على خلاف ذلك. وعلى النحو الموضح في الفقرة 6، تعرض العديد من الطبقات تقديم خدمات أمن معينة. وقد لا تقدم هذه الطبقات دائماً خدمات الأمن من ضمنها، بل قد تستفيد من خدمات الأمن المناسبة التي يجري تقديمها في الطبقات السفلى. وحتى عند عدم تقديم أي خدمات أمن داخل طبقة ما، قد تتطلب تعاريف خدمة تلك الطبقة التعديل للسماح بتمرير طلبات خدمات الأمن إلى طبقة أدنى.

الملاحظة 1 – لا يرد بحث آليات الأمن المنتشرة (انظر الفقرة 4.5) في هذه الفقرة.

الملاحظة 2 – يرد بحث اختيار موضع آليات التشفير للتطبيقات في الملحق جيم.

1.7 *الطبقة المادية*

1.1.7 *الخدمات*

إن خدمات الأمن الوحيدة المقدَّمة في الطبقة المادية، منفردة أو مجتمعة، هي التالية:

أ) كتم التوصيل؛

ب) كتم تدفق الحركة.

ويأخذ كتم تدفق الحركة شكلين:

1) كتم تدفق الحركة الكامل الذي لا يمكن تقديمه إلا في ظروف معينة، من قبيل الإرسال في اتجاهين في وقت واحد، والمتزامن، ومن نقطة إلى نقطة؛

2) كتم تدفق الحركة المحدود الذي يمكن تقديمه لأنواع أخرى من الإرسال مثل الإرسال غير متزامن.

وتقتصر هذه الخدمات على التهديدات الأمنية المستترة ويمكن تطبيقها على الاتصالات من نقطة إلى نقطة أو متعددة النظراء.

2.1.7 *الآليات*

التشفير الكلي لتدفق البيانات هو الآلية الأمنية الرئيسية في الطبقة المادية.

وهناك شكل محدد من التشفير ينطبق على الطبقة المادية فقط، وهو أمن الإرسال (أي أمن الطيف الممتد).

وتقدَّم حماية الطبقة المادية عن طريق جهاز تشفير يعمل بشفافية. وهدف حماية الطبقة المادية هو حماية قطار بتات بيانات الخدمة المادية بأكملها وتوفير كتمان تدفق الحركة.

2.7 *طبقة وصلة البيانات*

1.2.7 *الخدمات*

إن خدمات الأمن الوحيدة المقدَّمة في طبقة وصلة البيانات هي التالية:

أ) كتم التوصيل؛

ب) الكتمان عند الاستغناء عن التوصيل.

2.2.7 *الآليات*

تُستخدم آلية التشفير لتقديم خدمات الأمن في طبقة وصلة البيانات (انظر الملحق جيم).

وتنفَّذ الخواص الوظيفية الإضافية للحماية الأمنية لطبقة الوصلة قبل وظائف الطبقة العادية للإرسال وبعد وظائف الطبقة العادية للاستقبال، أي أن آليات الأمن تبنى على جميع وظائف الطبقة العادية وتستخدمها.

وتتحسس آليات التشفير على طبقة وصلة البيانات لبروتوكول طبقة الوصلة.

3.7 *طبقة الشبكة*

تنظَّم طبقة الشبكة داخلياً لتوفير بروتوكول (أو بروتوكولات) كي تنفذ العمليات التالية:

أ) النفاذ إلى الشبكة الفرعية؛

ب) التقارب المعتمد على الشبكة الفرعية؛

ج) التقارب المستقل عن الشبكة الفرعية؛

د) الترحيل والتسيير.

1.3.7 *الخدمات*

يمكن تقديم خدمات الأمن بواسطة بروتوكول يؤدي وظائف النفاذ إلى الشبكة الفرعية المرتبطة بتقديم خدمة شبكة التوصيل البيني للأنظمة المفتوحة (OSI)، وهذه الخدمات هي كما يلي:

أ) الاستيقان من الكيان النظير؛

ب) الاستيقان من مصدر البيانات؛

ج) خدمة التحكم في النفاذ؛

د) كتم التوصيل؛

هـ) الكتمان عند الاستغناء عن التوصيل؛

و) كتم تدفق الحركة؛

ز) سلامة التوصيل دون تدارك البيانات؛

ح) السلامة بدون توصيل.

ويمكن تقديم خدمات الأمن هذه منفردة أو مجتمعة. ويمكن تقديم خدمات الأمن بواسطة بروتوكول يؤدي عمليات الترحيل والتسيير المرتبطة بتقديم خدمة شبكة التوصيل البيني للأنظمة المفتوحة (OSI)، من نظام طرفي إلى نظام طرفي، وهي نفس تلك التي يقدمها البروتوكول الذي يؤدي عمليات النفاذ إلى الشبكة الفرعية.

2.3.7 *الآليات*

1.2.3.7 يستخدم البروتوكول (أو البروتوكولات) آليات أمن متطابقة للقيام بالنفاذ إلى الشبكة الفرعية وبعمليات الترحيل والتسيير المرتبطة بتقديم خدمة شبكة التوصيل البيني للأنظمة المفتوحة (OSI)، من نظام طرفي إلى نظام طرفي. وينفَّذ التسيير في هذه الطبقة، وبالتالي يقع التحكم في التسيير داخل هذه الطبقة. وتقدَّم خدمات الأمن المحددة على النحو التالي:

أ) تقدَّم خدمة الاستيقان من الكيان النظير بتوليفة مناسبة من تبادلات الاستيقان المشتقة تجفيرياً أو المحمية، وكلمة المرور المحمية وآليات التوقيع؛

ب) يمكن تقديم خدمة الاستيقان من مصدر البيانات عن طريق آليات تشفير أو توقيع؛

ج) تقدَّم خدمة التحكم في النفاذ من خلال الاستخدام المناسب لآليات محددة للتحكم في النفاذ؛

د) تقدَّم خدمة كتم التوصيل بواسطة آلية تشفير و/أو التحكم في التسيير؛

هـ) تقدَّم خدمة الكتمان عند الاستغناء عن التوصيل بواسطة آلية تشفير و/أو التحكم في التسيير؛

و) تتحقق خدمة كتم تدفق الحركة من خلال آلية حشو الحركة، وبالاقتران مع خدمة الكتمان عند أو ما دون طبقة الشبكة و/أو التحكم في التسيير؛

ز) تقدَّم خدمة سلامة التوصيل دون تدارك البيانات باستخدام آلية سلامة البيانات، وبالاقتران أحياناً مع آلية تشفير؛

ح) تقدَّم خدمة السلامة بدون توصيل باستخدام آلية سلامة البيانات، وبالاقتران أحياناً مع آلية تشفير.

2.2.3.7 والآليات، في البروتوكول الذي ينفذ عمليات النفاذ إلى الشبكة الفرعية المرتبطة بتقديم خدمة شبكة التوصيل البيني للأنظمة المفتوحة (OSI) من نظام طرفي إلى نظام طرفي، تعرض الخدمات عبر شبكة فرعية واحدة.

وتطبَّق حماية الشبكة الفرعية المفروضة من إدارة الشبكة الفرعية وفقاً لما تمليه بروتوكولات النفاذ إلى الشبكة الفرعية، ولكنها عادة ما تطبَّق قبل وظائف الشبكة الفرعية العادية عند الإرسال وبعد وظائف الشبكة الفرعية العادية عند الاستقبال.

3.2.3.7 والآليات التي يقدمها البروتوكول الذي ينفذ عمليات الترحيل والتسيير المرتبطة بتقديم خدمة شبكة التوصيل البيني للأنظمة المفتوحة (OSI) من نظام طرفي إلى نظام طرفي، تعرض الخدمات عبر واحدة أو أكثر من الشبكات الموصولة بينياً.

وتستدعى هذه الآليات قبل وظائف الترحيل والتسيير عند الإرسال وبعد وظائف الترحيل والتسيير عند الاستقبال. وفي حالة آلية التحكم في التسيير، تُشتق قيود التسيير من قاعدة معلومات إدارة الأمن (SMIB) قبل تمرير البيانات مع قيود التسيير اللازمة إلى وظائف الترحيل والتسيير.

4.2.3.7 ويمكن للتحكم في النفاذ ضمن طبقة الشبكة أن يخدم أغراضاً كثيرة. فهو على سبيل المثال يسمح لنظام طرفي بالتحكم في إقامة توصيلات الشبكة ورفض المكالمات غير المرغوب فيها. وهو يسمح أيضاً لواحدة أو أكثر من الشبكات الفرعية بالتحكم في استخدام موارد طبقة الشبكة. وفي بعض الحالات، يرتبط هذا الغرض الأخير بفرض رسوم على استخدام الشبكة.

ملاحظة – قد يترتب على إقامة توصيل شبكة في كثير من الأحيان رسوم تفرضها إدارة الشبكة الفرعية. ويمكن الإقلال من هذه التكلفة إلى الحد الأدنى من خلال التحكم في النفاذ واختيار إسناد الرسوم إلى الجهة المتلقية للاتصال، أو غير ذلك من المعلمات الخاصة بالشبكة.

5.2.3.7 ويمكن لمتطلب من شبكة فرعية معينة أن يفرض آليات تحكم في النفاذ على البروتوكول الذي ينفذ عمليات النفاذ إلى الشبكة الفرعية المرتبطة بتقديم خدمة شبكة التوصيل البيني للأنظمة المفتوحة (OSI) من نظام طرفي إلى نظام طرفي. وعندما تقدَّم آليات التحكم في النفاذ بواسطة البروتوكول الذي ينفذ عمليات الترحيل والتسيير المرتبطة بتقديم خدمة شبكة التوصيل البيني للأنظمة المفتوحة (OSI) من نظام طرفي إلى نظام طرفي، يمكن استخدامها لتحكم كيانات الترحيل في النفاذ إلى الشبكات الفرعية وللتحكم في النفاذ إلى الأنظمة الطرفية على حد سواء. ومن الواضح أن مدى فرز التحكم في النفاذ فضفاض إلى حدٍ ما، إذ لا يميز إلا بين كيانات طبقة الشبكة.

6.2.3.7 وإن استُخدم حشو الحركة بالاقتران مع آلية تشفير في طبقة الشبكة (أو خدمة الكتمان من الطبقة المادية)، أمكن تحقيق مستوى معقول من كتمان تدفق الحركة.

4.7 *طبقة النقل*

1.4.7 *الخدمات*

إن خدمات الأمن التي يمكن تقديمها، منفردة أو مجتمعة، في طبقة النقل هي:

أ) الاستيقان من الكيان النظير؛

ب) الاستيقان من مصدر البيانات؛

ج) خدمة التحكم في النفاذ؛

د) كتم التوصيل؛

هـ) الكتمان عند الاستغناء عن التوصيل؛

و) سلامة التوصيل مع تدارك البيانات؛

ز) سلامة التوصيل دون تدارك البيانات؛

ح) السلامة بدون توصيل.

2.4.7 *الآليات*

وتقدَّم خدمات الأمن المحددة على النحو التالي:

أ) تقدَّم خدمة الاستيقان من الكيان النظير بتوليفة مناسبة من تبادلات الاستيقان المشتقة تجفيرياً أو المحمية، وكلمة المرور المحمية وآليات التوقيع؛

ب) يمكن تقديم خدمة الاستيقان من مصدر البيانات عن طريق آليات تشفير أو توقيع؛

ج) تقدَّم خدمة التحكم في النفاذ من خلال الاستخدام المناسب لآليات محددة للتحكم في النفاذ؛

د) تقدَّم خدمة كتم التوصيل بواسطة آلية تشفير؛

هـ) تقدَّم خدمة الكتمان عند الاستغناء عن التوصيل بواسطة آلية تشفير؛

و) تقدَّم خدمة سلامة التوصيل مع تدارك البيانات باستخدام آلية سلامة البيانات، وبالاقتران أحياناً مع آلية تشفير؛

ز) تقدَّم خدمة سلامة التوصيل دون تدارك البيانات باستخدام آلية سلامة البيانات، وبالاقتران أحياناً مع آلية تشفير؛

ح) تقدَّم خدمة السلامة بدون توصيل باستخدام آلية سلامة البيانات، وبالاقتران أحياناً مع آلية تشفير.

وتعمل آليات الحماية بحيث يمكن استدعاء خدمات الأمن لتوصيلات النقل الفردية. وتكون هذه الحماية بحيث يمكن عزل فرادى توصيلات النقل عن جميع توصيلات النقل الأخرى.

5.7 *طبقة الدورة*

1.5.7 *الخدمات*

لا تقدَّم أي خدمات أمن في طبقة الدورة.

6.7 *طبقة العرض التقديمي*

1.6.7 *الخدمات*

تقدِّم طبقة العرض التقديمي المرافق لدعم تقديم خدمات الأمن التالية من جانب طبقة التطبيق إلى عملية التطبيق:

أ) كتم التوصيل؛

ب) الكتمان عند الاستغناء عن التوصيل؛

ج) كتم المجالات الانتقائي.

ويمكن أيضاً للمرافق في طبقة العرض التقديمي أن تدعم تقديم خدمات الأمن التالية من جانب طبقة التطبيق إلى عملية التطبيق:

د) كتم تدفق الحركة؛

ه) الاستيقان من الكيان النظير؛

و) الاستيقان من مصدر البيانات؛

ز) سلامة التوصيل مع تدارك البيانات؛

ح) سلامة التوصيل دون تدارك البيانات؛

ط) سلامة التوصيل الانتقائية حسب المجالات؛

ي) السلامة بدون توصيل؛

ك) السلامة الانتقائية حسب المجالات دون التوصيل؛

ل) عدم التنصل بإثبات المصدر؛

م) عدم التنصل بإثبات الإيصال.

ملاحظة – إن المرافق التي تقدمها طبقة العرض التقديمي هي تلك التي تعتمد على الآليات التي يمكن أن تعمل فقط على تشفير قواعد نظم نقل البيانات وتشمل، على سبيل المثال، الآليات القائمة على تقنيات التجفير.

2.6.7 *الآليات*

في خدمات الأمن التالية، يمكن أن تقع آليات الدعم داخل طبقة العرض التقديمي، و إذا كان الأمر كذلك، قد تُستخدم إلى جانب آليات أمن طبقة التطبيق لتقدم خدمات أمن طبقة التطبيق:

أ) يمكن لآليات تحويل قواعد النظم (مثل التشفير) أن تدعم خدمة الاستيقان من الكيان النظير؛

ب) يمكن لآليات التشفير أو التوقيع أن تدعم خدمة الاستيقان من مصدر البيانات؛

ج) يمكن أن تدعم آلية تشفير خدمة كتم التوصيل؛

د) يمكن أن تدعم آلية تشفير خدمة الكتمان عند الاستغناء عن التوصيل؛

ه) يمكن أن تدعم آلية تشفير خدمة كتم المجالات الانتقائي؛

و) يمكن أن تدعم آلية تشفير خدمة كتم تدفق الحركة؛

ز) يمكن أن تدعم آلية سلامة البيانات، بالاقتران أحياناً مع آلية تشفير، خدمة سلامة التوصيل مع تدارك البيانات؛

ح) يمكن أن تدعم آلية سلامة البيانات، بالاقتران أحياناً مع آلية تشفير، خدمة سلامة التوصيل دون تدارك البيانات؛

ط) يمكن أن تدعم آلية سلامة البيانات، بالاقتران أحياناً مع آلية تشفير، خدمة سلامة التوصيل الانتقائية حسب المجالات؛

ي) يمكن أن تدعم آلية سلامة البيانات، بالاقتران أحياناً مع آلية تشفير، خدمة السلامة بدون توصيل؛

ك) يمكن أن تدعم آلية سلامة البيانات، بالاقتران أحياناً مع آلية تشفير، خدمة السلامة الانتقائية حسب المجالات دون التوصيل؛

ل) يمكن لتوليفة مناسبة من آليات سلامة البيانات والتوقيع والتوثيق أن تدعم خدمة عدم التنصل بإثبات المصدر؛

م) يمكن لتوليفة مناسبة من آليات سلامة البيانات والتوقيع والتوثيق أن تدعم خدمة عدم التنصل بإثبات الإيصال.

وآليات التشفير المطبقة على نقل البيانات، عندما تقع في الطبقات العليا، سترد في طبقة العرض التقديمي.

وبدلاً من ذلك يمكن أن تقدَّم بعض خدمات الأمن المذكورة في القائمة أعلاه بواسطة الآليات الأمنية الواردة بالكامل داخل طبقة التطبيق.

ولا يمكن من خلال الآليات الأمنية الواردة في طبقة العرض التقديمي إلا تقديم خدمات أمن الكتمان على نحو كامل.

وتعمل آليات الأمن في طبقة العرض التقديمي في المرحلة النهائية من التحويل إلى قواعد نظم النقل عند الإرسال، وكالمرحلة الأولى من عملية التحويل عند الاستقبال.

7.7 *طبقة التطبيق*

1.7.7 *الخدمات*

يمكن أن تقدم طبقة التطبيق واحدة أو أكثر من خدمات الأمن الأساسية التالية، إما منفردة أو مجتمعة:

أ) الاستيقان من الكيان النظير؛

ب) الاستيقان من مصدر البيانات؛

ج) خدمة التحكم في النفاذ؛

د) كتم التوصيل؛

ه) الكتمان عند الاستغناء عن التوصيل؛

و) كتم المجالات الانتقائي؛

ز) كتم تدفق الحركة؛

ح) سلامة التوصيل مع تدارك البيانات؛

ط) سلامة التوصيل دون تدارك البيانات؛

ي) سلامة التوصيل الانتقائية حسب المجالات؛

ك) السلامة بدون توصيل؛

ل) السلامة الانتقائية حسب المجالات دون التوصيل؛

م) عدم التنصل بإثبات المصدر؛

ن) عدم التنصل بإثبات الإيصال.

يوفر الاستيقان من شركاء الاتصالات المزمعين الدعم لعناصر التحكم في النفاذ إلى موارد التوصيل البيني للأنظمة المفتوحة (OSI) وغيرها من الموارد على حد سواء (كالملفات والبرمجيات والمطاريف والطابعات) في الأنظمة المفتوحة الحقيقية.

ويمكن تحديد متطلبات أمنية معينة في واقعة اتصالات، بما في ذلك كتمان البيانات والسلامة والاستيقان، بواسطة إدارة أمن التوصيل البيني للأنظمة المفتوحة أو إدارة طبقة التطبيق على أساس المعلومات الواردة في قاعدة معلومات إدارة الأمن (SMIB) بالإضافة إلى الطلبات المقدمة من عملية التطبيق.

2.7.7 *الآليات*

تقدَّم خدمات الأمن في طبقة التطبيق عن طريق الآليات التالية:

أ) يمكن تقديم خدمة الاستيقان من الكيان النظير باستخدام معلومات الاستيقان المنقولة بين كيانات التطبيق التي تحميها آليات تشفير العرض التقديمي أو الطبقة الأدنى؛

ب) يمكن أن تدعم خدمة الاستيقان من مصدر البيانات باستخدام آليات التوقيع أو آليات تشفير الطبقة الأدنى؛

ج) إن خدمة التحكم في النفاذ إلى تلك الجوانب من نظام مفتوح حقيقي ذات الصلة بالتوصيل البيني للأنظمة المفتوحة (OSI)، مثل القدرة على التواصل مع أنظمة معينة أو كيانات التطبيق البعيد، يمكن تقديمها من خلال مزيج من آليات التحكم في النفاذ في طبقة التطبيق وفي الطبقات الأدنى؛

د) يمكن أن تدعم خدمة كتم التوصيل باستخدام آلية تشفير الطبقة الأدنى؛

هـ) يمكن أن تدعم خدمة الكتمان عند الاستغناء عن التوصيل باستخدام آلية تشفير الطبقة الأدنى؛

و) يمكن أن تدعم خدمة كتم المجالات الانتقائي باستخدام آلية تشفير في طبقة العرض التقديمي؛

ز) يمكن أن تدعم خدمة كتم تدفق الحركة بصورة محدودة باستخدام آلية حشو الحركة عند طبقة التطبيق بالاقتران مع خدمة الكتمان في طبقة أدنى؛

ح) يمكن أن تدعم خدمة سلامة التوصيل مع تدارك البيانات باستخدام آلية سلامة البيانات في طبقة أدنى (بالاقتران في بعض الأحيان مع آلية تشفير)؛

ط) يمكن أن تدعم خدمة سلامة التوصيل دون تدارك البيانات باستخدام آلية سلامة البيانات في طبقة أدنى (بالاقتران في بعض الأحيان مع آلية تشفير)؛

ي) يمكن أن تدعم خدمة سلامة التوصيل الانتقائية حسب المجالات باستخدام آلية سلامة البيانات (بالاقتران في بعض الأحيان مع آلية تشفير) في طبقة العرض التقديمي؛

ك) يمكن أن تدعم خدمة السلامة بدون توصيل باستخدام آلية سلامة البيانات في طبقة أدنى (بالاقتران في بعض الأحيان مع آلية تشفير)؛

ل) يمكن أن تدعم خدمة السلامة الانتقائية حسب المجالات دون التوصيل باستخدام آلية سلامة البيانات (بالاقتران في بعض الأحيان مع آلية تشفير) في طبقة العرض التقديمي؛

م) يمكن أن تدعم خدمة عدم التنصل بإثبات المصدر عن طريق توليفة مناسبة من آليات التوقيع وسلامة البيانات في طبقة أدنى، بالاقتران ربما مع أطراف موثّقة ثالثة؛

ن) يمكن أن تدعم خدمة عدم التنصل بإثبات الإيصال عن طريق توليفة مناسبة من آليات التوقيع وسلامة البيانات في طبقة أدنى، بالاقتران ربما مع أطراف موثّقة ثالثة.

وإن استُخدمت آلية التوثيق لتقديم خدمة عدم التنصل، فإنها ستتصرف كطرف ثالث موثوق. وقد تمتلك سجلاً من وحدات البيانات المرحَّلة في شكلها المنقول (أي بقواعد نظم النقل) من أجل حل النزاعات. وقد تستخدم خدمات الحماية من الطبقات الأدنى.

3.7.7 *خدمات الأمن في غير التوصيل البيني للأنظمة المفتوحة* (OSI)

يمكن لعمليات التطبيق عينها أن توفر أساساً لجميع الخدمات وأن تستخدم نفس أنواع الآليات التي جاء وصفها في هذه التوصية، في تموضعها المناسب في طبقات مختلفة من المعمارية. وإذ يقع هذا الاستخدام خارج نطاق التوصية، فهو لا يتعارض مع تعاريف خدمة وبروتوكول التوصيل البيني للأنظمة المفتوحة ومع معماريته.

8.7 *بيان العلاقة بين خدمات وطبقات الأمن*

يوضح الجدول 2/X.800 طبقات النموذج المرجعي الذي يمكن تقديم خدمات الأمن الخاصة فيه. وترد أوصاف خدمات الأمن في الفقرة 2.5. وترد مبررات تموضع خدمة في طبقة معينة في الملحق باء.

الجدول 2/X.800

بيان العلاقة بين خدمات وطبقات الأمن

الخدمة	الطبقة						
	1	2	3	4	5	6	7*
الاستيقان من الكيان النظير	.	.	ن	ن	.	.	ن
الاستيقان من مصدر البيانات	.	.	ن	ن	.	.	ن
خدمة التحكم في النفاذ	.	.	ن	ن	.	.	ن
كتم التوصيل	ن	ن	ن	ن	.	ن	ن
الكتمان عند الاستغناء عن التوصيل	.	ن	ن	ن	.	ن	ن
كتم المجالات الانتقائي	.	.	.	.	.	ن	ن
كتم تدفق الحركة	ن	.	ن	.	.	.	ن
سلامة التوصيل مع تدارك البيانات	.	.	.	ن	.	.	ن
سلامة التوصيل دون تدارك البيانات	.	.	ن	ن	.	.	ن
سلامة التوصيل الانتقائية حسب المجالات	.	.	.	.	.	.	ن
السلامة بدون توصيل	.	.	ن	ن	.	.	ن
السلامة الانتقائية حسب المجالات دون التوصيل	.	.	.	.	.	.	ن
عدم التنصل بإثبات المصدر	.	.	.	.	.	.	ن
عدم التنصل بإثبات الإيصال	.	.	.	.	.	.	ن

ن نعم، ينبغي أن تدرج الخدمة في معايير للطبقة كخيار لدى مقدم الخدمة.

. غير مقدَّمة.

* تجدر الإشارة، فيما يتعلق بالطبقة 7، إلى قدرة عملية التطبيق، في حد ذاتها، على تقديم خدمات الأمن.

الملاحظة 1 – لا يسعى الجدول 2/X.800 لبيان تساوي المندرجات فيه من حيث الوزن أو الأهمية؛ بل على العكس هناك تدرج كبير للمقياس داخل المندرجات في الجدول.

الملاحظة 2 – يرد وصف تموضع خدمات الأمن داخل طبقة الشبكة في الفقرة 2.3.7. إذ إن موضع خدمات الأمن ضمن طبقة الشبكة يؤثر بشكل كبير على طبيعة ونطاق الخدمات التي ستقدَّم.

الملاحظة 3 – تحتوي طبقة العرض التقديمي على عدد من المرافق الأمنية التي تدعم تقديم طبقة التطبيق لخدمات الأمن.

8 إدارة الأمن

1.8 *اعتبارات عامة*

1.1.8 تعنى إدارة أمن التوصيل البيني للأنظمة المفتوحة (OSI) بجوانب إدارة الأمن بالنسبة إلى التوصيل البيني للأنظمة المفتوحة وبأمن إدارة التوصيل البيني للأنظمة المفتوحة. وتعنى جوانب إدارة أمن التوصيل البيني للأنظمة المفتوحة بتلك العمليات التي تقع خارج الوقائع العادية للاتصالات والتي تلزم مع ذلك للدعم والتحكم في الجوانب الأمنية لتلك الاتصالات.

ملاحظة – يتحدد توفر خدمة الاتصالات بتصميم الشبكة و/أو بروتوكولات إدارة الشبكة. وهناك حاجة إلى اختيار الخيارات المناسبة منها للحيلولة دون الحرمان من الخدمة.

2.1.8 وإذ يمكن أن تتعدد السياسات الأمنية التي تفرضها إدارة (أو إدارات) توزيع الأنظمة المفتوحة، ينبغي لتوصيات إدارة أمن التوصيل البيني للأنظمة المفتوحة أن تدعم هذه السياسات. وتُجمع في بعض الأحيان الكيانات التي تخضع لسياسة أمنية واحدة وتدار من جانب سلطة واحدة في ما يسمى "ميدان أمن". وتُعتبر ميادين الأمن وتفاعلاتها مجالاً هاماً لتوسعات المستقبل.

3.1.8 وتعنى إدارة أمن التوصيل البيني للأنظمة المفتوحة (OSI) بإدارة خدمات وآليات أمن التوصيل البيني للأنظمة المفتوحة. وتتطلب هذه الإدارة توزيع المعلومات الإدارية على هذه الخدمات والآليات فضلاً عن جمع المعلومات المتعلقة بتشغيل هذه الخدمات والآليات. ومن الأمثلة على ذلك توزيع مفاتيح التجفير وتحديد معلمات اختيار الأمن المفروضة إدارياً والإبلاغ عن كل من الأحداث الأمنية العادية وغير العادية (سجلات

التدقيق) وتفعيل الخدمة وإيقافها. ولا تتناول إدارة الأمن تمرير المعلومات ذات الصلة بالأمن في البروتوكولات التي تستدعي خدمات أمنية محددة (كما في المعلمات في طلبات التوصيل).

4.1.8 وقاعدة معلومات إدارة الأمن (SMIB) هي المستودع المفاهيمي لجميع المعلومات ذات الصلة بالأمن التي تحتاجها الأنظمة المفتوحة. ولا يوحي هذا المفهوم بأي شكل من تخزين المعلومات أو تنفيذها. بيد أن كل نظام طرفي يجب أن يحوي المعلومات المحلية اللازمة لتمكينه من إنفاذ سياسة أمنية مناسبة. وقاعدة معلومات إدارة الأمن هي قاعدة المعلومات الموزعة بالحد اللازم لإنفاذ سياسة أمنية متسقة في الفرز (المنطقي أو المادي) لأنظمة طرفية. وفي الممارسة العملية، قد تُدمج أو لا تُدمج أجزاء من قاعدة معلومات إدارة الأمن في قاعدة معلومات الإدارة (MIB).

ملاحظة – يمكن أن تتعدد سبل تنفيذ قاعدة معلومات إدارة الأمن، ومنها على سبيل المثال:

أ) جدول بيانات؛

ب) ملف؛

ج) بيانات أو قواعد مضمنة في برمجيات أو عتاد النظام المفتوح الحقيقي.

5.1.8 يمكن أن تكون بروتوكولات الإدارة، لا سيما بروتوكولات إدارة الأمن وقنوات الاتصال التي تحمل المعلومات الإدارية، عرضة للخطر. لذا يجب توخي العناية بوجه خاص للتأكد من حماية بروتوكولات الإدارة والمعلومات بحيث لا تضعف الحماية الأمنية المقدَّمة لوقائع الاتصالات المعتادة.

6.1.8 وقد تتطلب إدارة الأمن تبادل المعلومات ذات الصلة بالأمن بين مختلف إدارات النظام، بحيث يمكن تأسيس قاعدة معلومات إدارة الأمن (SMIB) أو توسيع نطاقها. وفي بعض الحالات، تُمرر المعلومات ذات الصلة بالأمن عبر مسيرات الاتصالات في غير التوصيل البيني للأنظمة المفتوحة (OSI)، ويحدِّث المشرفون المحليون على إدارة الأنظمة قاعدة معلومات إدارة الأمن بأساليب غير مقيَّسة بالتوصيل البيني للأنظمة المفتوحة. وفي حالات أخرى، قد يُستحسن تبادل مثل هذه المعلومات عبر مسير اتصالات التوصيل البيني للأنظمة المفتوحة، وعندئذ تُمرر المعلومات بين اثنين من تطبيقات إدارة الأمن يعملان في الأنظمة المفتوحة الحقيقية. ويستخدم تطبيق إدارة الأمن المعلومات المرسلة لتحديث قاعدة معلومات إدارة الأمن. وقد يتطلب هذا التحديث الحصول على إذن مسبق من مسؤول الأمن المناسب.

7.1.8 وتعرَّف بروتوكولات التطبيق لتبادل المعلومات ذات الصلة بالأمن على قنوات اتصالات التوصيل البيني للأنظمة المفتوحة.

2.8 *فئات إدارة أمن التوصيل البيني للأنظمة المفتوحة* (OSI)

هناك ثلاث فئات من أنشطة إدارة التوصيل البيني للأنظمة المفتوحة:

أ) نظام إدارة الأمن؛

ب) إدارة خدمة الأمن؛

ج) إدارة آلية الأمن.

وبالإضافة إلى ذلك، يجب النظر في إدارة التوصيل البيني للأنظمة المفتوحة نفسها (انظر الفقرة 4.2.8). وفيما يلي تلخيص الوظائف الرئيسية التي تقوم بها هذه الفئات من إدارة الأمن.

1.2.8 *إدارة أمن النظام*

تعنى إدارة أمن النظام بإدارة الجوانب الأمنية لبيئة التوصيل البيني للأنظمة المفتوحة (OSI) بشكل عام. وتمثل القائمة التالية نموذجاً نمطياً للأنشطة التي تقع ضمن هذه الفئة من إدارة الأمن:

أ) إدارة السياسة الأمنية الشاملة، بما في ذلك التحديثات وصيانة الاتساق؛

ب) التفاعل مع وظائف الإدارة الأخرى في التوصيل البيني للأنظمة المفتوحة؛

ج) التفاعل مع إدارة خدمة الأمن وإدارة آلية الأمن؛

د) إدارة التعامل مع الحدث (انظر الفقرة 1.3.8)؛

هـ) إدارة التدقيق الأمني (انظر الفقرة 2.3.8)؛

و) إدارة استعادة الأمن (انظر الفقرة 3.3.8).

2.2.8 *إدارة خدمة الأمن*

تعنى إدارة خدمة الأمن بإدارة خدمات أمن معينة. وتمثل القائمة التالية نموذجاً نمطياً للأنشطة التي يمكن القيام بها في إدارة خدمة أمن معينة:

أ) تحديد وتخصيص الحماية الأمنية المستهدفة للخدمة؛

ب) تخصيص وصيانة قواعد لاختيار آلية أمن محددة (حيث توجد البدائل) يمكن توظيفها لتقديم خدمة الأمن المطلوبة؛

ج) التفاوض (محلياً أو عن بُعد) بشأن آليات الأمن المتوفرة والتي تتطلب اتفاق إدارة مسبق؛

د) استدعاء آليات أمنية محددة عبر وظيفة إدارة آلية أمن مناسبة، كتقديم خدمات الأمن المفروضة إدارياً؛

هـ) التفاعل مع وظائف إدارة خدمة الأمن ووظائف إدارة آلية الأمن الأخرى.

3.2.8 *إدارة آلية الأمن*

تعنى إدارة آلية الأمن بإدارة آليات أمن معينة. وتُعتبر القائمة التالية من وظائف إدارة آلية الأمن نمطية ولكن ليست شاملة:

أ) إدارة المفاتيح؛

ب) إدارة التشفير؛

ج) إدارة التوقيع الرقمي؛

د) إدارة التحكم في النفاذ؛

هـ) إدارة سلامة البيانات؛

و) إدارة الاستيقان؛

ز) إدارة حشو الحركة؛

ح) إدارة التحكم في التسيير؛

ط) إدارة التوثيق.

ويرد بحث كل من وظائف إدارة آلية الأمن المدرجة بمزيد من التفصيل في الفقرة 4.8.

4.2.8 *أمن إدارة التوصيل البيني للأنظمة المفتوحة* (OSI)

إن أمن جميع وظائف إدارة التوصيل البيني للأنظمة المفتوحة وأمن تداول معلومات هذه الإدارة يشكل جزءاً مهماً من أمن التوصيل البيني للأنظمة المفتوحة. وتستدعي هذه الفئة من إدارة الأمن الخيارات المناسبة من الخدمات والآليات المدرجة لأمن التوصيل البيني للأنظمة المفتوحة لضمان الحماية الكافية لبروتوكولات ومعلومات إدارة التوصيل البيني للأنظمة المفتوحة (انظر الفقرة 5.1.8). فعلى سبيل المثال، تتطلب الاتصالات، بين الكيانات الإدارية التي تنطوي على قاعدة معلومات الإدارة، شكلاً من أشكال الحماية عموماً.

3.8 *أنشطة إدارة أمن نظام محدد*

1.3.8 *إدارة التعامل مع الحدث*

إن الجوانب الإدارية للتعامل مع الحدث المرئية في التوصيل البيني للأنظمة المفتوحة تتمثل في الإبلاغ عن بُعد عما يبدو من محاولات لانتهاك أمن النظام وتعديل عتبات تستخدم للمبادرة إلى الإبلاغ عن الحدث.

2.3.8 *إدارة التدقيق الأمني*

يمكن أن تشمل إدارة التدقيق الأمني ما يلي:

أ) اختيار الأحداث التي يتعين تسجيلها و/أو جمعها عن بُعد؛

ب) تمكين وتعطيل تسجيل سجل تدقيق الأحداث المختارة؛

ج) جمع سجلات التدقيق المختارة عن بُعد؛

د) إعداد تقارير التدقيق الأمني.

3.3.8 *إدارة استعادة الأمن*

يمكن أن تشمل إدارة استعادة الأمن ما يلي:

أ) الحفاظ على القواعد المستخدمة للرد على الانتهاكات الأمنية الحقيقية أو المشتبه فيها؛

ب) الإبلاغ عن بُعد عما يبدو من انتهاكات لأمن النظام؛

ج) تفاعلات مسؤول الأمن.

4.8 *وظائف إدارة آلية الأمن*

1.4.8 *إدارة المفاتيح*

يمكن أن تشمل إدارة المفاتيح ما يلي:

أ) توليد مفاتيح مناسبة على فترات تتناسب مع مستوى الأمن المطلوب؛

ب) تحديد الكيانات التي ينبغي أن تحصل على نسخة من كل مفتاح وفقاً لمتطلبات التحكم في النفاذ؛

ج) إتاحة أو توزيع المفاتيح بطريقة آمنة إلى حالات كيان في الأنظمة المفتوحة الحقيقية.

ومن المفهوم أن بعض وظائف إدارة المفاتيح تؤدى خارج بيئة التوصيل البيني للأنظمة المفتوحة (OSI). وهي تشمل التوزيع المادي للمفاتيح بوسائل موثوقة.

ويعد تبادل مفاتيح عاملة لاستخدامها خلال ارتباط، وظيفة عادية في بروتوكول طبقة. ويمكن أيضاً أن يتحقق اختيار المفاتيح العاملة من خلال النفاذ إلى مركز توزيع المفاتيح أو بالتوزيع المسبق عبر بروتوكولات الإدارة.

2.4.8 *إدارة التشفير*

يمكن أن تشمل إدارة التشفير ما يلي:

أ) التفاعل مع إدارة المفاتيح؛

ب) وضع معلمات التجفير؛

ج) التزامن التجفيري.

ووجود آلية تشفير يعني ضمناً استخدام إدارة المفاتيح والطرق الشائعة للإشارة إلى خوارزميات التجفير.

وتحدّد درجة تمييز الحماية التي يوفرها التشفير بماهية الكيانات التي تُسند إليها مفاتيح بشكل مستقل ضمن بيئة التوصيل البيني للأنظمة المفتوحة (OSI). وهذا هو بدوره يتحدد، بصفة عامة، بمعمارية الأمن وعلى وجه التعيين بآلية إدارة المفاتيح.

ويمكن الحصول على مرجع مشترك لخوارزميات التجفير باستخدام سجل لخوارزميات التجفير أو عن طريق الاتفاقات المسبقة بين الكيانات.

3.4.8 *إدارة التوقيع الرقمي*

يمكن أن تشمل إدارة التوقيع الرقمي ما يلي:

أ) التفاعل مع إدارة المفاتيح؛

ب) وضع معلمات وخوارزميات التجفير؛

ج) استخدام بروتوكول بين الكيانات التي تتواصل فيما بينها وربما مع طرف ثالث.

ملاحظة – توجد عموماً أوجه شبه قوية بين إدارة التوقيع الرقمي وإدارة التشفير.

4.4.8 *إدارة التحكم في النفاذ*

يمكن أن تشمل إدارة التحكم في النفاذ توزيع نعوت الأمن (بما فيها كلمات المرور) أو تحديثات لقوائم التحكم في النفاذ أو قوائم القدرات. ويمكن أن تشمل كذلك استخدام بروتوكول بين الكيانات التي تتواصل فيما بينها والكيانات الأخرى التي تقدم خدمات التحكم في النفاذ.

5.4.8 *إدارة سلامة البيانات*

يمكن أن تشمل إدارة سلامة البيانات ما يلي:

أ) التفاعل مع إدارة المفاتيح؛

ب) وضع معلمات وخوارزميات التجفير؛

ج) استخدام بروتوكول بين الكيانات التي تتواصل فيما بينها.

ملاحظة – عند استخدام تقنيات التجفير لسلامة البيانات، توجد أوجه شبه قوية بين إدارة سلامة البيانات وإدارة التشفير.

6.4.8 *إدارة الاستيقان*

يمكن أن تشمل إدارة الاستيقان توزيع معلومات وصفية، وكلمات مرور أو مفاتيح (باستخدام إدارة المفاتيح) لكيانات يلزم الاستيقان منها. ويمكن أن تشمل كذلك استخدام بروتوكول بين الكيانات التي تتواصل فيما بينها والكيانات الأخرى التي تقدم خدمات الاستيقان.

7.4.8 *إدارة حشو الحركة*

يمكن أن تشمل إدارة حشو الحركة صيانة القواعد لاستخدامها في حشو الحركة. وعلى سبيل المثال فهي قد تشمل ما يلي:

أ) معدلات بيانات محددة سلفاً؛

ب) تحديد معدلات بيانات عشوائية؛

ج) تحديد خصائص الرسالة من قبيل طولها؛

د) اختلاف التوصيف، ربما وفقاً للوقت خلال اليوم و/أو التقويم.

8.4.8 *إدارة التحكم في التسيير*

يمكن أن تشمل إدارة التحكم في التسيير تعريف الوصلات أو الشبكات الفرعية التي تعتبر إما آمنة أو موثوقة فيما يتعلق بمعايير معينة.

9.4.8 *إدارة التوثيق*

يمكن أن تشمل إدارة التوثيق ما يلي:

أ) توزيع المعلومات بشأن الجهات الموثّقة؛

ب) استخدام بروتوكول بين الجهة الموثّقة والكيانات التي تتواصل فيما بينها؛

ج) التفاعل مع الجهات الموثّقة.

الملحـــق ألـــف

معلومات أساسية عن الأمن في التوصيل البيني للأنظمة المفتوحة (OSI)

(لا يشكل هذا الملحق جزءاً أساسياً من هذه التوصية)

1.A *معلومات أساسية*

يورد هذا الملحق ما يلي:

أ) معلومات عن أمن التوصيل البيني للأنظمة المفتوحة لوضع هذه التوصية في سياقها بعض الشيء؛

ب) معلومات أساسية عن الآثار المعمارية للميزات والمتطلبات الأمنية المختلفة.

إن الأمن في بيئة التوصيل البيني للأنظمة المفتوحة (OSI) هو مجرد جانب واحد من أمن معالجة البيانات/اتصالات البيانات. وإذا أريد للتدابير الوقائية المستخدمة في بيئة التوصيل البيني للأنظمة المفتوحة أن تكون فعالة، فهي تتطلب تدابير دعم تقع خارج التوصيل البيني للأنظمة المفتوحة. فعلى سبيل المثال، إذا كانت المعلومات التي تتدفق بين الأنظمة مشفرة دون وضع قيود أمنية مادية على النفاذ إلى الأنظمة ذاتها، قد يضيع التشفير سدىً. وكذلك لا يعنى التوصيل البيني للأنظمة المفتوحة سوى بالتوصيل البيني للأنظمة. وكيما تكون التدابير الأمنية فعالة في التوصيل البيني للأنظمة المفتوحة، فإنها يجب أن تستخدم بالاقتران مع تدابير تقع خارج نطاق التوصيل البيني للأنظمة المفتوحة.

2.A *متطلب الأمن*

1.2.A *ما المقصود بالأمن؟*

يُستخدم مصطلح "الأمن" بمعنى التقليل إلى أدنى حد من مواطن ضعف الأصول والموارد. والأصل هو أي شيء له قيمة. والثغرة الأمنية هي أي نقطة يمكن أن تُستغل لانتهاك نظام ما أو المعلومات التي يتضمنها. والتهديد انتهاك محتمل للأمن.

2.2.A *الدافع للأمن في الأنظمة المفتوحة*

بينت اللجنة الاستشارية الدولية للبرق والهاتف (CCITT) الحاجة إلى سلسلة من التوصيات لتعزيز الأمن داخل معمارية الأنظمة المفتوحة. ويعود ذلك إلى ما يلي:

أ) زيادة اعتماد المجتمع على أجهزة الحاسوب التي تنفذ إليها، أو ترتبط بها، اتصالات البيانات والتي تتطلب حماية ضد التهديدات المختلفة؛

ب) ظهور تشريع "حماية البيانات" في العديد من البلدان وهو يُلزم الموردين ببيان سلامة النظام وخصوصيته؛

ج) رغبة المنظمات المختلفة باستخدام توصيات التوصيل البيني للأنظمة المفتوحة (OSI)، المعززة حسب الحاجة، لضمان أمن الأنظمة الحالية والمستقبلية.

3.2.A *ما المطلوب حمايته؟*

فيما يلي ما قد يتطلب الحماية بشكل عام:

أ) المعلومات والبيانات (بما في ذلك البرمجيات والبيانات الهامدة المتعلقة بالتدابير الأمنية مثل كلمات المرور)؛

ب) خدمات الاتصالات ومعالجة البيانات؛

ج) المعدات والمرافق.

4.2.A *التهديدات*

تتضمن التهديدات التي تواجه نظام اتصالات البيانات ما يلي:

أ) إتلاف المعلومات و/أو الموارد الأخرى؛

ب) إفساد المعلومات أو تعديلها؛

ج) سرقة المعلومات و/أو الموارد الأخرى أو إزالتها أو خسارتها؛

د) إفشاء المعلومات؛

هـ) تعطيل الخدمات.

ويمكن تصنيف التهديدات تبعاً لما إذا كانت عارضة أو متعمدة، وقد تكون نشطة أو سلبية.

1.4.2.A *التهديدات العارضة*

تحدث التهديدات العارضة دون سابق عزم. ومن أمثلة التهديدات العارضة سوء أداء النظام وأخطاء التشغيل الفادحة وأخطاء البرمجيات.

2.4.2.A *التهديدات المتعمدة*

قد تتراوح التهديدات المتعمدة من مجرد الفحص العابر، باستخدام أدوات الرصد المتيسرة بسهولة، إلى الهجمات المتطورة باستخدام المعارف الخاصة بالنظام. ويمكن اعتبار التهديد المتعمد، إذا تحقق، بمثابة "هجمة".

3.4.2.A *التهديدات السلبية*

التهديدات السلبية، إذا تحققت، لا تسفر عن أي تعديل في أي من المعلومات في النظام أو الأنظمة ولا يحدث أي تغيير في تشغيل النظام أو في حالته. كما أن التنصّت السلكي السلبي لمراقبة المعلومات التي يجري إرسالها على خط اتصالات يمثل تهديداً سلبياً.

4.4.2.A *التهديدات النشطة*

تشمل التهديدات النشطة تغيير المعلومات في النظام أو إجراء تغييرات في حالة النظام أو في تشغيله. ويعتبر التغيير المؤذي في جداول تسيير نظام ما من قِبل مستعمل غير مرخص له مثالاً لتهديد نشط.

5.2.A *بعض الأنماط المحددة من الهجمات*

فيما يلي استعراض موجز لبعض الهجمات التي تثير قلقاً خاصاً في بيئة معالجة البيانات/اتصالات البيانات. وفي الفقرات التالية يظهر مصطلحا مخوَّل وغير مخوَّل. و"التخويل" يعني "منح حقوق". وينطوي هذا التعريف ضمناً على شيئين هما: أن الحقوق هي حقوق أداء نشاط ما (مثل النفاذ إلى البيانات)؛ وعلى أن الحقوق مُنحت لعملية أو كيان أو فرد ما. إذن، السلوك المخوَّل هو أداء تلك الأنشطة التي مُنحت حقوق بشأنها (و لم تُلغَ). وللاستزادة عن مفهوم التخويل، انظر الفقرة 1.3.3.A.

1.5.2.A *انتحال الصفة*

يحصل انتحال الصفة عندما يتظاهر كيان بكونه كياناً مختلفاً. ويُستخدم انتحال الصفة عادة مع بعض أشكال أخرى من الهجوم النشط، وخاصة تكرار الرسائل وتعديلها. فعلى سبيل المثال، يمكن التقاط تتابعات استيقان وتكرارها بعد حدوث تتابع استيقان صحيح. وقد يلجأ كيان مخوَّل قليل الامتيازات إلى انتحال صفة للحصول على امتيازات إضافية عن طريق تقمص شخصية كيان يمتلك تلك الامتيازات.

2.5.2.A *التكرار*

يحدث التكرار عند تكرار رسالة أو جزء من رسالة لإنتاج أثر غير مخوَّل. فعلى سبيل المثال، يمكن لكيان آخر أن يكرر رسالة صحيحة تتضمن معلومات الاستيقان بغية الاستيقان منه (باعتباره غير ما هو حقاً).

3.5.2.A *تعديل الرسائل*

يحدث تعديل رسالة عند تغيير محتوى إرسال بيانات دون كشفه مؤدياً إلى تأثير غير مخوَّل، كما هو الحال، على سبيل المثال، عندما تغيَّر رسالة "اسمح لجون سميث بقراءة ملف الحسابات المكتوم" لتصبح "اسمح لفرِد براون بقراءة ملف الحسابات المكتوم".

4.5.2.A *الحرمان من الخدمة*

يحدث الحرمان من الخدمة عندما يقصّر كيان عن أداء وظيفته المناسبة أو يتصرف بطريقة تمنع الكيانات الأخرى من أداء وظائفها المناسبة. وقد يكون الهجوم عاماً، كما هو الحال عندما يحجب كيان كل الرسائل، أو قد يكون مستهدِفاً ، كما هو الحال عندما يحجب كيان كل الرسائل الموجهة إلى مقصد معين، مثل خدمة التدقيق الأمني. وقد ينطوي الهجوم على حجب الحركة على النحو الموضح في هذا المثال أو قد يولد حركة إضافية. ويمكن أيضاً توليد رسائل تهدف إلى تعطيل تشغيل الشبكة، وخاصة إذا كان في الشبكة كيانات ترحيل تتخذ قرارات تسيير بناءً على تقارير الحالة الواردة من كيانات الترحيل الأخرى.

5.5.2.A *الهجمات من الداخل*

تحدث هجمات من الداخل عندما يتصرف مستخدمون مشروعون للنظام بطرق غير مقصودة أو غير مخوَّل بها. وقد تضمنت جرائم الحاسوب الأكثر شهرة هجمات من الداخل عرضت أمن النظام للخطر. ومن أساليب الحماية التي يمكن استخدامها ضد الهجمات من الداخل ما يلي:

أ) التحقق الدقيق من الموظفين؛

ب) التمحيص في العتاد والبرمجيات وسياسة الأمن وتشكيلات النظام بغية بلوغ درجة من الاطمئنان من أنها ستعمل بشكل صحيح (ما يسمى بالخواص الوظيفية الموثوقة)؛

ج) تزيد سجلات التدقيق من احتمال كشف هذه الهجمات.

6.5.2.A *الهجمات من الخارج*

يمكن للهجمات من الخارج أن تستخدم تقنيات من قبيل:

أ) التنصت السلكي (النشط والسلبي)؛

ب) التقاط البث؛

ج) انتحال صفة مستخدمين مخولين للنظام أو مكونات النظام؛

د) تجاوز آليات الاستيقان أو التحكم في النفاذ.

7.5.2.A *باب التسلل*

عند تغيير أحد كيانات نظام ما للسماح لمهاجم بإحداث تأثير غير مخوَّل به في إصدار أمر أو في حدث أو سلسلة أحداث محدّدة مسبقاً، تدعى النتيجة باب تسلل. إذ يمكن مثلاً تعديل عملية إثبات صلاحية كلمة مرور بحيث يمكن، بالإضافة إلى أثرها العادي، أن تُقر أيضاً صلاحية كلمة مرور المهاجم.

8.5.2.A *حصان طروادة*

عندما يدخل حصان طروادة إلى النظام تكون له وظيفة غير مخوَّل بها بالإضافة إلى وظيفته المخوَّل بها. والترحيل الذي ينسخ أيضاً رسائل إلى قناة غير مخوَّل لها يقوم بدور حصان طروادة.

6.2.A *تقييم التهديدات والمخاطر والتدابير المضادة*

إن ميزات الأمن عادةً ما تزيد من تكاليف النظام وقد تزيد من صعوبة استخدامه. ولذا فإنه ينبغي، قبل تصميم نظام مأمون، تحديد الأخطار النوعية التي يتطلب الأمر الحماية منها. ويعرف ذلك بتقييم التهديدات. ولئن كثرت الثغرات الأمنية في النظام إلا أن بعضاً منها فقط قابل للاستغلال لأن المهاجم يفتقر إلى الفرصة المناسبة أو لأن النتيجة لا تبرر الجهد الذي يبذل ومخاطر الانكشاف. وعلى الرغم من أن المسائل التفصيلية الخاصة بتقييم التهديدات تقع خارج نطاق هذا الملحق، فإنها تشمل بصورة إجمالية ما يلي:

أ) تحديد الثغرات الأمنية التي يعاني منها النظام؛

ب) تحليل احتمالية التهديدات التي تهدف إلى استغلال الثغرات الأمنية هذه؛

ج) تقييم النتائج في حالة تنفيذ كل تهديد بنجاح؛

د) تقدير تكلفة كل هجمة؛

هـ) وضع تقدير لتكاليف التدابير المضادة المحتملة؛

و) اختيار آليات الأمن التي لها ما يبررها (ربما باستخدام تحليل المنافع مقابل التكاليف).

وقد تكون التدابير غير التقنية مثل التغطية التأمينية، من البدائل عن تدابير الأمن التقنية التي تحقق مردودية تكاليفها. ويعز الكمال في الأمن التقني كما يعز الكمال في الأمن الجسدي. لذا ينبغي أن يكون الهدف هو جعل تكلفة أي هجوم عالية بما يقلل من المخاطر إلى مستويات مقبولة.

3.A *السياسة الأمنية*

تناقش هذه الفقرة السياسة الأمنية: الحاجة إلى سياسة أمنية محددة بشكل مناسب؛ ودورها ؛ ونُهُج السياسة في الاستخدام، والتحسينات التي يتعين تطبيقها في حالات محددة. ثم تطبَّق هذه المفاهيم على أنظمة الاتصالات.

1.3.A *الحاجة إلى السياسة الأمنية والغرض منها*

إن مجال الأمن برمته معقد وبعيد المدى في آن. وأي تحليل كامل بالحد المعقول سيتمخض عن مجموعة متنوعة شاقة من التفاصيل. وينبغي للسياسة الأمنية المناسبة أن تركز الاهتمام على تلك الجوانب من الحالة التي يرى أعلى مستوى من السلطة أنها ينبغي أن تلقى اهتماماً. وفي الأساس، تحدد السياسة الأمنية، بصفة عامة، المسموح والممنوع في مجال الأمن خلال التشغيل العام للنظام قيد الاعتبار. والسياسة ليست محددة عادة، بل هي تشير إلى ما هو بالغ الأهمية دون القول على وجه الدقة بكيفية الحصول على النتائج المرجوة منها. وتحدد السياسة المستوى الأعلى من توصيف الأمن.

2.3.A *تبعات تعريف السياسة: عملية الصقل*

لأن السياسة هي محض عامة، ليس من الواضح على الإطلاق في البداية كيف يمكن أن تقترن السياسة بتطبيق معين. وفي كثير من الأحيان، تكمن أفضل طريقة لتحقيق ذلك في إخضاع السياسة لتحسينات متعاقبة تضيف المزيد من التفاصيل من التطبيق في كل مرحلة. وتتطلب معرفة الماهية التي يجب أن تكون عليها تلك التفاصيل دراسة مفصلة لمجال التطبيق في ضوء السياسة العامة. وينبغي لهذا الفحص أن يحدد المشاكل الناجمة عن محاولة فرض شروط السياسة على التطبيق. وستفضي عملية الصقل هذه إلى صيغة جديدة للسياسة العامة تتسم بعبارات دقيقة جداً مستمدة من التطبيق مباشرة. وستسهل الصيغة الجديدة للسياسة تحديد تفاصيل التنفيذ.

3.3.A *مكونات السياسة الأمنية*

هناك جانبان للسياسات الأمنية القائمة، ويتوقف كلاهما على مفهوم السلوك المخوَّل.

1.3.3.A *التخويل*

تنطوي جميع التهديدات التي سبق بحثها على مفهوم السلوك المخوَّل أو غير المخوَّل. ويتجسد بيان ما يشكل التخويل في السياسة الأمنية. ويمكن لسياسة أمنية عامة أن تنص على "عدم جواز إعطاء المعلومات أو السماح بالنفاذ إليها أو بالاستدلال عليها أو باستخدام أي مورد، لأي جهة غير مخولة أصولاً". فطبيعة التخويل هي ما تميز السياسات المختلفة. ويمكن تقسيم السياسات إلى مكونين منفصلين، استناداً إلى طبيعة التخويل المعني، فهي إما سياسات قائمة على قواعد مرعية أو سياسات قائمة على الهوية. وتستخدم أولاهما قواعد تقوم على عدد قليل من النعوت العامة أو أصناف الحساسية، ويجري إنفاذها بصورة شاملة. وتتضمن الثانية تخويل على أساس نعوت محددة ذات خصوصية فردية. ويفترض الارتباط الدائم لبعض النعوت مع الكيان الذي تنطبق عليه، وقد يكون البعض الآخر منها ممتلكات (مثل القدرات) يمكن أن تنتقل إلى كيانات أخرى. ويمكن التمييز أيضاً بين خدمة التخويل المفروض إدارياً والتخويل المختار دينامياً. فالسياسة الأمنية هي التي تحدد تلك العناصر من أمن النظام التي تُطبَّق ويسري مفعولها دائماً (مثل مكونات السياسة الأمنية القائمة على قواعد والقائمة على الهوية، إن وجدت)، وتلك التي قد يختار المستخدم استعمالها على النحو الذي يراه مناسباً.

2.3.3.A *السياسة الأمنية القائمة على الهوية*

يتوافق الجانب القائم على الهوية من السياسات الأمنية، في جزء منه، مع مفهوم الأمن المعروف باسم "الحاجة إلى المعرفة". والهدف من ذلك هو اصطفاء النفاذ إلى البيانات أو الموارد. وهناك أساساً طريقتان أساسيتان لتنفيذ السياسات القائمة على الهوية، حسبما إذا كانت المعلومات بشأن حقوق النفاذ تحتفظ بها الجهات القائمة بالنفاذ أو إذا كانت جزءاً من البيانات التي يُنفذ إليها. وتتمثل الأولى في أفكار الامتيازات أو القدرات المعطاة للمستخدمين والمستخدمة من جانب عمليات تتصرف بالنيابة عنهم. وقوائم التحكم في النفاذ (ACL) هي أمثلة على النوع الثاني من المعلومات. وفي كلتا الحالتين، يمكن أن يختلف كثيراً مقاس بند البيانات (من ملف كامل إلى عنصر بيانات) الذي قد يرد اسمه في قدرة ما أو الذي قد يحمل قائمة التحكم في النفاذ الخاصة به.

3.3.3.A *السياسة الأمنية القائمة على القواعد*

تستند السياسة الأمنية القائمة على القواعد عادة إلى الحساسية. ففي نظام آمن، ينبغي وسم البيانات و/أو الموارد بوسوم أمنية. ويمكن للعمليات التي تتصرف نيابة عن المستخدمين البشريين أن تحوز وسماً أمنياً مناسباً لُمنشئها.

4.3.A *السياسة الأمنية والاتصالات والوسوم*

إن مفهوم الوسم مهم في بيئة اتصالات البيانات. فالوسوم الحاملة للنعوت تقوم بأدوار متنوعة. فهناك بنود البيانات التي تتحرك أثناء الاتصالات، وهناك عمليات وكيانات تبادر بالاتصال وأخرى ترد، وهناك قنوات وغيرها من الموارد التي تستخدم أثناء الاتصال في النظام نفسه. ويمكن وسمها جميعاً بطريقة أو بأخرى، بالنعوت الخاصة بها. ويجب أن تبين السياسات الأمنية كيفية استخدام النعوت لكل منها لتوفير الأمن اللازم. وقد تلزم المفاوضات لوضع الدلالة الأمنية المناسبة لنعوت موسومة معينة. وعند إرفاق الوسوم الأمنية بالعمليات القائمة بالنفاذ وبالبيانات التي يجري النفاذ إليها على حد سواء، ينبغي أن تكون المعلومات الإضافية اللازمة لتطبيق التحكم في النفاذ على أساس الهوية موجودة في السمات ذات الصلة. وعندما تستند سياسة أمنية إلى هوية المستخدم الذي يقوم بالنفاذ إلى البيانات، إما مباشرة أو من خلال عملية ما، ينبغي أن تشمل وسوم الأمن معلومات عن هوية المستخدم. وينبغي التعبير عن قواعد لوسوم معينة في السياسة الأمنية في قاعدة معلومات إدارة الأمن (SMIB) و/أو التفاوض بشأنها مع الأنظمة الطرفية، على النحو المطلوب. وقد يُلحق الوسم بنعوت تعدل حساسيته، وتحدد محاذير التعاطي به وتوزيعه، وتقيد توقيته والتصرف به، وتحدد المتطلبات الخاصة بالنظام الطرفي.

1.4.3.A *وسوم العملية*

في الاستيقان، يكون عادة التحديد الكامل للعمليات أو الكيانات المبادرة والمجيبة في واقعة اتصالات إلى جانب جميع النعوت المناسبة، ذا أهمية أساسية. وبالتالي تحتوي قواعد معلومات إدارة الأمن معلومات كافية عن هذه النعوت الهامة لأي سياسة تفرضها الإدارة.

2.4.3.A *وسوم بند البيانات*

عند تحرك بنود البيانات أثناء وقائع الاتصال، يكون كل منها لصيقاً بوسمه. (وهذا الإسناد اللصيق مهم، وفي بعض الحالات تتطلب السياسات القائمة على قواعد أن يشكل الوسم جزءاً خاصاً من بند البيانات قبل تقديمه إلى التطبيق). وتقنيات الحفاظ على سلامة بند البيانات ستحافظ أيضاً على دقة الوسم واقترانه. ويمكن استخدام هذه النعوت في وظائف التحكم في التسيير في طبقة وصلة البيانات من النموذج المرجعي الأساسي للتوصيل البيني للأنظمة المفتوحة (OSI).

4.A *آليات الأمن*

يمكن تنفيذ سياسة الأمن باستخدام آليات مختلفة، منفردة أو مجتمعة، تبعاً لأهداف السياسة العامة والآليات المستخدمة. وبشكل عام، تنتمي الآلية إلى واحدة من ثلاث فئات (متداخلة) هي:

أ) الوقاية؛

ب) الكشف؛

ج) تدارك البيانات.

ويرد أدناه بحث الآليات الأمنية المناسبة لبيئة اتصالات البيانات.

1.4.A *التقنيات التجفيرية والتشفير*

يكمن التجفير وراء العديد من الخدمات والآليات الأمنية. ويمكن استخدام وظائف التجفير كجزء من التشفير وفك التشفير وسلامة البيانات وتبادلات الاستيقان، وتخزين كلمة المرور وتدقيقها، وغير ذلك، للمساعدة في تحقيق الكتمان و/أو السلامة و/أو الاستيقان. والتشفير المستخدم للكتمان يحول البيانات الحساسة (أي البيانات المراد حمايتها) إلى أشكال أقل حساسية. وعند استخدام تقنيات التجفير للسلامة أو الاستيقان، فهي تُستخدم لحساب الوظائف غير القسرية.

ويجري تنفيذ التشفير بدايةً على نص واضح (cleartext) لإنتاج النص المشفر (ciphertext). وتكون نتيجة فك التشفير إما نصاً واضحاً وإما نصاً مشفراً تحت غطاء ما. فمن الممكن حسابياً استخدام نص واضح لأغراض المعالجة العامة، حيث يرى مضمونه الدلالي. وباستثناء سبل معينة، (مثل فك التشفير في المقام الأول، أو المطابقة التامة) من غير الممكن حسابياً معالجة النص المشفر لأن محتواه الدلالي مخفي. والتشفير في بعض الأحيان لا رجعة فيه عمداً (جراء اقتطاع أو فقدان البيانات مثلاً) حيثما لا يُستحسن استخلاص النص الواضح الأصلي في أي وقت كحال كلمات المرور.

وتستخدم الدوال التجفيرية متحولات تجفير تعمل عبر المجالات و/أو وحدات البيانات و/أو قطارات من وحدات البيانات. ويشكل متحولا تجفير المفتاحَ الذي يوجه تحولات محددة، ومتحول التهيئة المطلوب في بعض بروتوكولات التجفير للحفاظ على العشوائية الظاهرية للنص المشفر. ويجبُ أن يبقى المفتاح طي الكتمان عادة. ويمكن للدالة التجفيرية ولمتحول التهيئة كليهما أن يزيدا من التأخير واستهلاك عرض النطاق. وهذا يعقد الإضافات التجفيرية "الشفافة" أو "دون ترتيب مسبق" إلى الأنظمة القائمة.

ويمكن أن تكون المتحولات التجفيرية متناظرة أو غير متناظرة خلال التشفير وفك التشفير على حد سواء. ولا يرتبط المفتاحان المستخدمان في خوارزميات غير متناظرة رياضياً؛ ولا يمكن أن يُحسب أحد المفتاحين من الآخر. وتسمى هذه الخوارزميات أحياناً خوارزميات "المفتاح العمومي" نظراً لإمكانية الإعلان عن أحد المفتاحين فيما يظل الآخر سرياً.

ويمكن تحليل النص المشفر تجفيرياً عندما يكون ذلك ممكناً حسابياً لاسترداد نص واضح دون معرفة المفتاح. وقد يحدث ذلك، إذا استُخدمت دالة تجفيرية ضعيفة أو معطوبة. ويمكن أن يؤدي اعتراض الحركة وتحليلها إلى هجمات على نظام التجفير بما في ذلك دس وحذف وتغيير رسالة/مجال، وتكرار نص مشفر صالح سابقاً وانتحال صفة.

لذا ، فقد صُممت بروتوكولات التجفير لمقاومة الهجمات ولتحليل الحركة أيضاً في بعض الأحيان. وهناك تدبير محدد من التدابير المضادة لتحليل الحركة ويدعى "كتمان تدفق الحركة"، وهو يهدف إلى إخفاء وجود أو عدم وجود البيانات وخصائصها. وإذا رُحِّل النص المشفَّر، يجب أن يكون العنوان بصيغة واضحة في المرحِّلات والبوابات. فإذا شُفرت البيانات على كل وصلة فقط، وفُكت شفرتها (وبالتالي ضعفت) في المرحِّل أو البوابة، يقال إن المعمارية تستخدم "تشفير كل وصلة على حدة". وإذا كان العنوان فقط (وبيانات التحكم المماثلة) بصيغة واضحة في المرحِّل أو البوابة، يقال إن المعمارية تستخدم "التشفير من طرف إلى طرف". والتشفير من طرف إلى طرف مرغوب أكثر من الناحية الأمنية، ولكنه أكثر تعقيداً بكثير من الناحية المعمارية، وخاصة إذا تضمن توزيع المفاتيح الإلكترونية ضمن النطاق (وظيفة من وظائف إدارة المفاتيح). ويمكن الجمع بين تشفير كل وصلة على حدة والتشفير من طرف إلى طرف لتحقيق أهداف أمنية متعددة. وكثيراً ما تتحقق سلامة البيانات بحساب قيمة التحقق (checkvalue) التجفيرية. ويمكن اشتقاق قيمة التحقق في واحدة أو أكثر من الخطوات وهي دالة رياضية من المتحولات التجفيرية والبيانات. وترتبط قيم التحقق هذه مع البيانات التي تراد حراستها. وتسمى قيم التحقق التجفيرية أحياناً شفرات كشف التلاعب.

ويمكن لتقنيات التجفير أن توفر، أو تساعد في توفير، الحماية ضد ما يلي:

أ) رصد و/أو تعديل قطار رسالة؛

ب) تحليل الحركة؛

ج) التنصل؛

د) التزوير؛

هـ) التوصيل غير المخوَّل به؛

و) تعديل الرسائل.

2.4.A *جوانب إدارة المفاتيح*

إن استخدام خوارزميات التجفير يعني ضمناً إدارة المفاتيح التي تشمل توليد مفاتيح التجفير وتوزيعها والتحكم فيها. ويستند اختيار طريقة إدارة المفاتيح إلى تقييم المشاركين للبيئة التي ستُستخدم فيها. وتشمل اعتبارات هذه البيئة التهديدات التي يتعين اتقاؤها (الداخلية للمنظمة والخارجية على السواء) والتكنولوجيات المستخدمة والهيكل المعماري وموقع خدمات التجفير المقدمة والهيكل المادي وموقع مقدمي خدمة التجفير.

والنقاط التي يتعين اعتبارها فيما يتعلق بإدارة المفاتيح هي التالية:

أ) استخدام "عمر المفتاح" على أساس الوقت أو الاستخدام أو معايير أخرى، لكل مفتاح معرَّف، ضمناً أو صراحةً؛

ب) التحديد السليم للمفاتيح وفقاً لوظيفتها بحيث يمكن أن يُقصر استخدامها على وظيفتها، فعلى سبيل المثال، المفاتيح التي يعتزم استخدامها لخدمة الكتمان ينبغي ألا تستخدم لخدمة السلامة أو بالعكس؛

ج) اعتبارات غير التوصيل البيني للأنظمة المفتوحة (OSI)، مثل التوزيع المادي للمفاتيح وأرشفة المفاتيح.

وتشمل النقاط التي يتعين اعتبارها فيما يتعلق بإدارة المفاتيح في خوارزميات المفاتيح المتناظرة ما يلي:

أ) استخدام خدمة الكتمان في بروتوكول إدارة المفاتيح لنقل المفاتيح؛

ب) استخدام تراتبية مفاتيح. وينبغي أن يسمح بحالات مختلفة مثل:

1) تراتبيات مفاتيح "ثابتة" باستخدام مفاتيح تشفر البيانات فقط، مختارة ضمناً أو صراحة من مجموعة بهوية أو مؤشر مفتاح؛

2) تراتبيات مفاتيح متعددة الطبقات؛

3) ينبغي ألا تستخدم أبداً مفاتيح تجفير المفاتيح لحماية البيانات وينبغي ألا تستخدم أبداً مفاتيح تجفير البيانات لحماية مفاتيح تجفير المفاتيح؛

ج) تقسيم المسؤوليات بحيث لا يمتلك شخص واحد نسخة كاملة من مفتاح هام.

وتشمل النقاط التي يتعين اعتبارها فيما يتعلق بإدارة المفاتيح في خوارزميات المفاتيح غير المتناظرة ما يلي:

أ) استخدام خدمة الكتمان في بروتوكول إدارة المفاتيح لنقل المفاتيح السرية؛

ب) استخدام خدمة السلامة أو خدمة عدم التنصل بإثبات المصدر في بروتوكول إدارة المفاتيح لنقل المفاتيح العمومية. ويمكن تقديم هذه الخدمات من خلال استخدام خوارزميات التجفير المتناظرة و/أو غير المتناظرة.

3.4.A *آليات التوقيع الرقمي*

يُستخدم مصطلح التوقيع الرقمي للإشارة إلى تقنية معينة يمكن استخدامها لتقديم خدمات أمن مثل عدم التنصل والاستيقان. وتتطلب آليات التوقيع الرقمي استخدام خوارزميات التجفير غير المتناظر. والسمة الأساسية لآلية التوقيع الرقمي هي أن وحدة البيانات الموقعة لا يمكن إنشاؤها بدون استخدام المفتاح الخاص. وهذا يعني أن:

أ) لا يمكن لأي فرد إلا صاحب المفتاح الخاص إنشاء وحدة البيانات الموقعة؛

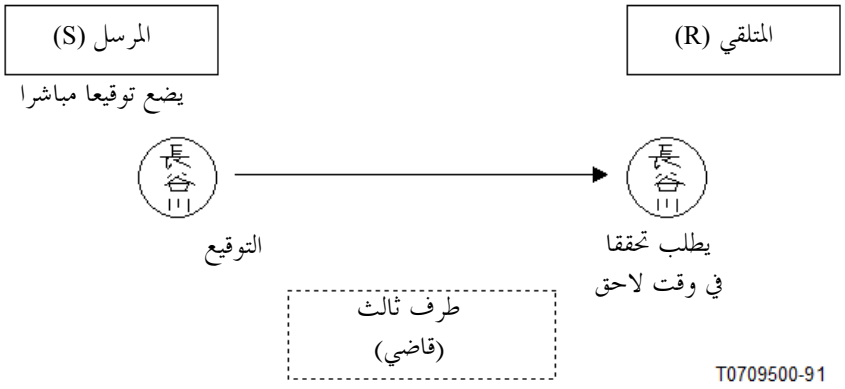
ب) لا يمكن للمتلقي إنشاء وحدة البيانات الموقعة.

لذا، باستخدام المعلومات المتاحة علناً فقط، يمكن تحديد موقِّع وحدة البيانات بشكل حصري على أنه مالك المفتاح الخاص. وفي حالة قيام نزاع بين المشاركين في وقت لاحق يمكن إثبات هوية موقِّع وحدة البيانات لطرف ثالث موثوق يدعى للحكم على صحة وحدة البيانات الموقعة. ويسمى هذا النوع من التوقيع الرقمي مخطط التوقيع المباشر (انظر الشكل A-1/X.800). وفي حالات أخرى، قد تدعو الحاجة إلى الخاصية الإضافية ج):

ج) لا يستطيع المرسل أن ينكر إرسال وحدة البيانات الموقعة.

فيثبت طرف ثالث موثوق (محكِّم) للمتلقي مصدر وسلامة المعلومات في هذه الحالة. ويسمى هذا النوع من التوقيع الرقمي مخطط التوقيع الخاضع للتحكيم (انظر الشكل A-2/X.800).

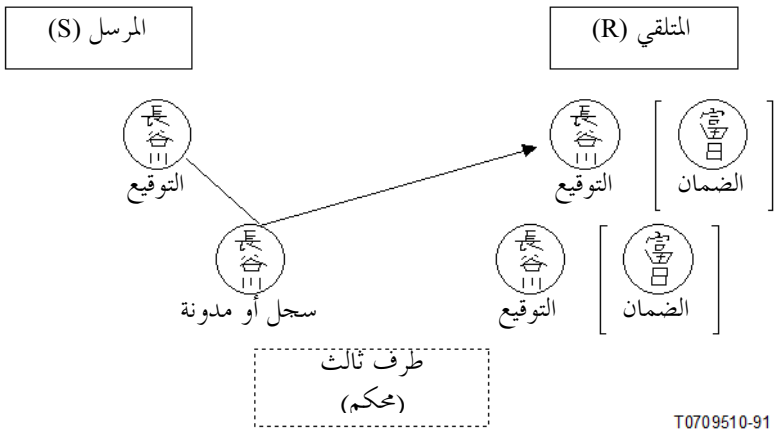
ملاحظة – قد يتطلب المرسل عجز المتلقي عن إنكار تلقي وحدة البيانات الموقعة في وقت لاحق. ويمكن أن يتحقق ذلك بخدمة عدم التنصل بإثبات الإيصال عن طريق توليفة مناسبة من التوقيع الرقمي وسلامة البيانات وآليات التوثيق.



ملاحظة – يتحقق من التوقيع عند قيام نزاع بين المشاركين (المرسل قد يكون كاذباً أو قد يكون المتلقي كاذباً)

الشكل A-1/X.800

مخطط التوقيع المباشر



ملاحظة – يستيقن طرف ثالث من المصدر (ويعطي المتلقي ضماناً (أي نتيجة إيجابية)). ويسجل طرف ثالث المعلومات اللازمة لإثبات مصدر البيانات وسلامتها. وفي هذه الحالة يعجز المرسل عن إنكار إرسال وحدة البيانات الموقَّعة لاحقاً.

الشكل A-2/X.800

مخطط التوقيع الخاضع للتحكيم

4.4.A *آليات التحكم في النفاذ*

آليات التحكم في النفاذ هي تلك الآليات التي تستخدم لإنفاذ سياسة حصر النفاذ إلى الموارد بالمستخدمين المخوَّلين. وتشمل التقنيات استخدام قوائم التحكم في النفاذ أو المصفوفات (التي عادة ما تحتوي على هويات البنود الخاضعة للرقابة والمستخدمين المخوَّلين كالناس أو العمليات)، وكلمات المرور، وقدرات، ووسوم أو تأشيرات، حيث يمكن الاستفادة من حيازتها لبيان حقوق النفاذ. وحيثما تُستخدم القدرات، ينبغي ألا تكون قسرية وينبغي نقلها بطريقة موثوقة.

5.4.A *آليات سلامة البيانات*

آليات سلامة البيانات هي على نوعين: تلك التي تستخدم لصون سلامة وحدة بيانات واحدة وتلك التي تصون سلامة وحدات بيانات أحادية وكذلك تتابع قطار كامل من وحدات البيانات على توصيل.

1.5.4.A *كشف تعديل قطار رسالة*

إن تقنيات كشف الخلل، التي ترتبط عادة مع كشف أخطاء البتات وأخطاء الكتل وأخطاء التتابع الناجمة عن وصلات وشبكات الاتصالات، يمكن أن تستخدم أيضاً لكشف تعديل قطار رسالة. ومع ذلك، إذا كانت رأسيات البروتوكول ومقطوراته غير محمية بواسطة آليات السلامة، يمكن لمتسلل مطَّلع أن يتجاوز بنجاح نقاط المراقبة هذه. وهكذا لا يمكن النجاح في تحقيق كشف تعديل قطار رسالة إلا باستخدام تقنيات كشف الخلل بالاقتران مع تتابع المعلومات. وهذا لن يمنع تعديل قطار رسالة ولكنه سيوفر إخطاراً بالهجمات.

6.4.A *آليات تبادل الاستيقان*

1.6.4.A *اختيار الآلية*

هناك العديد من الخيارات والتوليفات من آليات تبادل الاستيقان المناسبة لظروف مختلفة. ومنها على سبيل المثال:

أ) عندما تكون الكيانات النظيرة ووسائل الاتصال موثوقة على السواء، يمكن التأكد من هوية كيان نظير بواسطة كلمة مرور. فكلمة المرور التي تقي من الوقوع في الخطأ ليست منيعة ضد سوء النوايا، (على وجه التحديد، ليست منيعة ضد التكرار). ويمكن تحقيق الاستيقان المتبادل باستخدام كلمة مرور مميزة في كل اتجاه.

ب) وعندما يثق كل كيان بنظرائه من الكيانات ولكنه لا يثق في وسائل الاتصال، يمكن توفير الحماية ضد الهجمات النشطة بتوليفات من كلمات المرور والتشفير أو بأساليب تجفيرية. وتتطلب الحماية ضد هجمات التكرار تنظيماً في اتجاهين (بمعلمات الحماية) أو ختماً زمنياً (بميقاتيات موثوقة). ويمكن تحقيق الاستيقان المتبادل مع حماية من التكرار باستخدام تنظي ثلاثي.

ج) وعند عدم ثقة كيانات (أو شعورها بإمكانية عدم الثقة في المستقبل) بنظرائها أو بوسائل الاتصال، يمكن استخدام خدمات عدم التنصل. ويمكن تحقيق خدمة عدم التنصل باستخدام التوقيع الرقمي و/أو آليات التوثيق. ويمكن استخدام هذه الآليات مع الآليات الموصوفة في الفقرة ب) أعلاه.

7.4.A *آليات حشو الحركة*

إن توليد حركة هامشية ووحدات بيانات بروتوكول الحشو بطول ثابت يمكن أن يوفر حماية محدودة ضد تحليل الحركة. وللنجاح في ذلك، يجب أن يقارب مستوى الحركة الهامشية أعلى مستوى متوقع لحركة حقيقية. وبالإضافة إلى ذلك، يجب تشفير أو تمويه محتويات وحدات بيانات البروتوكول بحيث يتعذر التعرف على الحركة الهامشية وتمييزها عن حركة حقيقية.

8.4.A *آلية التحكم في التسيير*

يمكن أن يُستخدم توصيف محاذير التسيير في نقل البيانات (بما في ذلك توصيف كامل المسير) لضمان حصر نقل البيانات عبر المسيرات الآمنة مادياً أو لضمان عدم نقل المعلومات الحساسة إلا عبر المسيرات ذات المستوى المناسب من الحماية.

9.4.A *آلية التوثيق*

تستند آلية التوثيق إلى مفهوم طرف ثالث موثوق (موثِّق) لضمان خصائص معينة بشأن المعلومات المتبادلة بين اثنين من الكيانات، كأصلها أو سلامتها، أو الوقت الذي أُرسلت أو وردت فيه.

10.4.A *الأمن المادي وأمن الأفراد*

لا بد دوماً من التدابير الأمنية المادية لضمان حماية كاملة. والأمن المادي هو أمر مكلف، وكثيراً ما تجري محاولات لتقليل الحاجة إليه باستخدام غيره من التقنيات (الأرخص). وتقع اعتبارات الأمن المادي وأمن الأفراد خارج نطاق التوصيل البيني للأنظمة المفتوحة (OSI) على الرغم من أن جميع الأنظمة ستعتمد في نهاية المطاف على شكل ما من أشكال الأمن المادي وعلى جدارة الموظفين المسؤولين عن تشغيل النظام بالثقة. وينبغي تحديد إجراءات التشغيل لضمان التشغيل السليم وتوضيح مسؤوليات الموظفين.

11.4.A *العتاد الموثوق/البرمجيات الموثوقة*

تشمل الأساليب المستخدمة لاكتساب الثقة في الأداء الصحيح لكيان، الأساليب الرسمية في الإثبات والتحقق وإقرار الصلاحية والكشف، وتسجيل محاولات الهجوم المعروفة، وبناء أفراد موثوقين لكيان في بيئة آمنة. وهناك حاجة أيضاً لاحتياطات لضمان عدم تعديل الكيان بغير قصد أو عن عمد للنيل من الأمن خلال العمر التشغيلي للكيان، أثناء الصيانة أو الترقية مثلاً. ويجب الاطمئنان إلى صحة عمل بعض الكيانات في النظام، إذا أريدَ للأمن أن يدوم. أما الأساليب المستخدمة لبناء الثقة فهي خارج نطاق التوصيل البيني للأنظمة المفتوحة.

الملحـــق بـــاء

مبررات تموضع خدمة وآليات الأمن في الفقرة 7

(لا يشكل هذا الملحق جزءاً أساسياً من هذه التوصية)

1.B *اعتبارات عامة*

يوفر هذا الملحق بعض الأسباب لتقديم خدمات الأمن المحددة ضمن طبقات مختلفة على النحو المبين في الفقرة 7. وقد احتكمت عملية الاختيار هذه إلى مبادئ الطبقات الأمنية المحددة في الفقرة 1.1.6 من المعيار.

وتقدَّم خدمة أمن معينة من خلال أكثر من طبقة واحدة إذا أمكن اعتبار التأثير على أمن الاتصالات العام مختلفاً (من قبيل كتم التوصيل في الطبقتين 1 و4). ومع ذلك، نظراً للخواص الوظيفية القائمة لاتصالات بيانات التوصيل البيني للأنظمة المفتوحة (OSI) (ومثالها الإجراءات متعددة الوصلات، ووظيفة تعدد الإرسال، والسبل المختلفة لترقية الخدمة الخالية من التوصيل إلى خدمة مهيأة للتوصيل) وبغية السماح لآليات الإرسال هذه بالعمل، قد تدعو الضرورة للسماح بتقديم خدمة معينة في طبقة أخرى، على الرغم من أن تأثير ذلك على الأمن لا يمكن اعتباره مختلفاً.

2.B *الاستيقان من الكيان النظير*

- *الطبقتان 1 و2:* لا، لا يعتبر الاستيقان من الكيان النظير مفيداً في هاتين الطبقتين.
- *الطبقة 3:* نعم، عبر فرادى الشبكات الفرعية وللتسيير و/أو عبر الشبكة البينية.
- *الطبقة 4:* نعم، يمكن للاستيقان من نظام طرفي إلى نظام طرفي في الطبقة 4 أن يحقق الاستيقان المتبادل لاثنين أو أكثر من كيانات الدورة، قبل بدء توصيل، وطول مدة هذا التوصيل.
- *الطبقة 5:* لا، لا فائدة ترجى من تقديمه في الطبقة 4 و/أو طبقات أعلى.
- *الطبقة 6:* لا، ولكن آليات تشفير يمكن أن تدعم هذه الخدمة في طبقة التطبيق.
- الطبقة 7: نعم، ينبغي لطبقة التطبيق أن توفر الاستيقان من الكيان النظير.

3.B *الاستيقان من أصل البيانات*

- *الطبقتان 1 و2:* لا، لا يعتبر الاستيقان من أصل البيانات مفيداً في هاتين الطبقتين.
- *الطبقتان 3 و4:* يمكن توفير الاستيقان من أصل البيانات من طرف إلى طرف في دور الترحيل والتسيير للطبقة 3 و/أو في الطبقة 4 على النحو التالي:

أ) يوفر توفير الاستيقان من الكيان النظير في وقت إنشاء التوصيل مع الاستيقان المستمر المستند إلى تشفير خلال عمر توصيل، *بحكم الأمر الواقع*، خدمة استيقان من أصل البيانات؛

ب) حتى عند عدم تقديم الفقرة أ)، يمكن تقديم الاستيقان من أصل البيانات المستند إلى التشفير بترر يسير من الأعباء الإضافية على آليات سلامة البيانات القائمة بالفعل في هاتين الطبقتين.

- *الطبقة 5:* لا، لا فائدة ترجى من تقديمه في الطبقة 4 أو الطبقة 7.
- *الطبقة 6:* لا، ولكن آليات تشفير يمكن أن تدعم هذه الخدمة في طبقة التطبيق.
- *الطبقة 7:* نعم، وربما بالاقتران مع آليات في طبقة العرض التقديمي.

4.B *التحكم في النفاذ*

- *الطبقتان 1 و2:* لا يمكن توفير آليات التحكم في النفاذ في الطبقتين 1 أو 2 في نظام يلتزم ببروتوكولات التوصيل البيني للأنظمة المفتوحة الكاملة، حيث لا توجد مرافق طرفية متاحة لهذه الآلية.
- *الطبقة 3:* قد تُفرض آليات التحكم في النفاذ على دور النفاذ إلى الشبكة الفرعية بواسطة متطلبات خاصة للشبكة الفرعية. ويمكن استخدام آليات النفاذ في طبقة الشبكة، عندما تؤدي دور الترحيل والتسيير، للتحكم في نفاذ كيانات الترحيل إلى شبكات فرعية وللتحكم في النفاذ إلى الأنظمة الطرفية على حد سواء. ومن الواضح أن تفاصيل النفاذ فضفاضة إلى حد ما، حيث لا تمييز إلا بين كيانات طبقة الشبكة.

وكثيراً ما قد يؤدي إنشاء توصيل بشبكة إلى رسوم مستحقة لإدارة الشبكة الفرعية. ويمكن الإقلال من هذه التكلفة إلى الحد الأدنى من خلال التحكم في النفاذ واختيار إسناد الرسوم إلى الجهة المتلقية للاتصال، أو غير ذلك من المعلمات الخاصة بالشبكة أو الشبكة الفرعية.

- *الطبقة 4:* نعم، ويمكن استخدام آليات التحكم في النفاذ على أساس كل توصيل نقل من طرف إلى طرف.
- *الطبقة 5:* لا، لا فائدة ترجى من تقديمه في الطبقة 4 و/أو الطبقة 7.
- *الطبقة 6:* لا، هذا ليس مناسباً في الطبقة 6.
- *الطبقة 7:* نعم، يمكن لبروتوكولات التطبيق و/أو لعمليات التطبيق أن توفر مرافق التحكم في النفاذ ذات المنحى التطبيقي.

5.B *كتم جميع بيانات المستخدم* – (N) *على التوصيل* – (N)

- *الطبقة 1:* نعم، ينبغي أن يقدَّم، لأن الإدراج الكهربائي لأزواج شفافة من أجهزة التحويل يمكن أن يعطي الكتمان التام بعد توصيل مادي.
- *الطبقة 2:* نعم، لكنه لا يقدم أي فوائد أمنية زائدة عن الكتمان في الطبقة 1 أو الطبقة 3.
- *الطبقة 3:* نعم، لدور النفاذ إلى الشبكة الفرعية عبر فرادى الشبكات الفرعية ولدوري الترحيل والتسيير على الشبكة البينية.
- *الطبقة 4:* نعم، لأن توصيل النقل الفردي يعطي آلية النقل من طرف إلى طرف، ويمكن أن يوفر عزل توصيلات الدورة.
- *الطبقة 5:* لا، لأنه لا يقدم أي فائدة إضافية زائدة عن الكتمان في الطبقات 3 و4 و7. ولا يبدو مناسباً أن تقدَّم هذه الخدمة في هذه الطبقة.
- *الطبقة 6:* نعم، لأن آليات التشفير توفر تحويلات قواعد نظم بحتة.
- *الطبقة 7:* نعم، بالاقتران مع الآليات في الطبقات الأدنى .

6.B *كتم جميع بيانات المستخدم* – (N) *على وحدة واحدة لبيانات الخدمة* – (N) *خالية من التوصيل*

المسوغ هو على غرار كتم جميع بيانات المستخدم – *(N)* باستثناء الطبقة 1 التي لا يوجد فيها خدمة خالية من التوصيل.

7.B *الكتم الانتقائي لمجالات ضمن بيانات المستخدم* – (N) *في وحدة بيانات الخدمة* (SDU)

تقدَّم خدمة الكتمان هذه بالتشفير في طبقة العرض التقديمي وتستدعيها آليات في طبقة التطبيق وفقاً لدلالات البيانات.

8.B *كتم تدفق الحركة*

لا يمكن تحقيق كتم كامل لتدفق الحركة إلا في الطبقة 1. ويمكن تحقيق ذلك بالإدراج المادي لزوج من أجهزة التشفير في مسير الإرسال المادي. ويُفترض أن مسير الإرسال سيكون في اتجاهين في وقت واحد ومتزامناً بحيث إن إدراج الجهازين يحقق استحالة التعرف على كل الإرسالات (وحتى على وجودها) عبر الوسائط المادية.

وفوق الطبقة المادية، يتعذر الحصول على الأمن الكامل لتدفق الحركة. ويمكن إنتاج بعض من مؤثرات الأمن جزئياً باستخدام خدمة كاملة لكتم وحدة بيانات الخدمة في طبقة واحدة وبحقن حركة هامشية في طبقة عالية. وهذه الآلية مكلفة، ويمكن أن تستهلك كميات كبيرة من سعة الحمل والتبديل.

وإن قُدِّم كتم تدفق الحركة في الطبقة 3، يُستخدم حشو الحركة و/أو التحكم في التسيير. ويمكن للتحكم في التسيير أن يوفر كتماً محدوداً لتدفق الحركة بتسيير الرسائل ملتفاً حول الوصلات أو الشبكات الفرعية غير الآمنة. بيد أن إدراج حشو الحركة في الطبقة 3 يتيح استخداماً أفضل للشبكة المراد تحقيقها، عن طريق تجنب الحشو غير الضروري وازدحام الشبكة على سبيل المثال.

ويمكن توفير كتم محدود لتدفق الحركة في طبقة التطبيق بتوليد حركة هامشية، بالاقتران مع كتمان لمنع التعرف على الحركة الهامشية.

9.B *سلامة جميع بيانات المستخدم* – (N) *على التوصيل* – (N) *(مع تدارك الخطأ)*

- *الطبقتان 1 و2:* تعجز – الطبقتان 1 و2 عن تقديم هذه الخدمة. فالطبقة 1 لا تملك آليات كشف أو تدارك، ولا تعمل آلية الطبقة 2 إلا على أساس من نقطة إلى نقطة، لا على أساس من طرف إلى طرف، وبالتالي، لا يُعتبر تقديم هذه الخدمة مناسباً.
- *الطبقة 3:* لا، لأن تدارك الخطأ غير متوفر في كل مكان.
- *الطبقة 4:* نعم، لأنها توفر توصيل حقيقي للنقل من طرف إلى طرف.

- *الطبقة 5:* لا، لأن تدارك الخطأ ليس من وظائف الطبقة 5.
- *الطبقة 6:* لا، ولكن يمكن لآليات تشفير أن تدعم هذه الخدمة في طبقة التطبيق.
- *الطبقة 7:* نعم، بالاقتران مع الآليات في طبقة العرض التقديمي.

10.B *سلامة جميع بيانات المستخدم* – (N) *على التوصيل* – (N) *(دون تدارك الخطأ)*

- *الطبقتان 1 و2:* تعجز – الطبقتان 1 و2 عن تقديم هذه الخدمة. فالطبقة 1 لا تملك آليات كشف أو تدارك، ولا تعمل آلية الطبقة 2 إلا على أساس من نقطة إلى نقطة، لا على أساس من طرف إلى طرف، وبالتالي، لا يُعتبر تقديم هذه الخدمة مناسباً.
- *الطبقة 3:* نعم، لدور النفاذ إلى الشبكة الفرعية عبر فرادى الشبكات الفرعية ولدوري الترحيل والتسيير على الشبكة البينية.
- *الطبقة 4:* نعم ، بالنسبة لحالات الاستخدام حيث من المقبول إيقاف الاتصالات بعد كشف هجوم نشط.
- *الطبقة 5:* لا، لأنه لا يقدم أي فائدة زائدة على سلامة البيانات في الطبقات 3 أو 4 أو 7.
- *الطبقة 6:* لا، ولكن للآليات تشفير يمكن أن تدعم هذه الخدمة في طبقة التطبيق.
- *الطبقة 7:* نعم، بالاقتران مع الآليات في طبقة العرض التقديمي.

11.B *سلامة مجالات منتقاة ضمن بيانات المستخدم* – (N) *في وحدة بيانات الخدمة* (SDU) *المنقولة عبر التوصيل* – (N) *(دون تدارك الخطأ)*

يمكن توفير سلامة مجالات منتقاة بآليات تشفير في طبقة العرض التقديمي بالاقتران مع آليات استدعاء وتحقق في طبقة التطبيق.

12.B *سلامة جميع بيانات المستخدم* – (N) *في وحدة* – (N) *واحدة لبيانات الخدمة* (SDU) *خالية من التوصيل*

تقليلاً إلى أدنى حد من ازدواجية الوظائف، ينبغي توفير سلامة النقل الخالي من التوصيل في نفس طبقات السلامة دون التدارك حصراً، أي في طبقات الشبكة والنقل والتطبيق. وآليات السلامة هذه لا يمكن أن تكون إلا ذات فعالية محدودة للغاية، ويجب أن يكون ذلك معلوماً.

13.B *سلامة مجالات منتقاة في وحدة* – (N) *واحدة لبيانات الخدمة* (SDU) *خالية من التوصيل*

يمكن توفير سلامة مجالات منتقاة بآليات تشفير في طبقة العرض التقديمي بالاقتران مع آليات استدعاء وتحقق في طبقة التطبيق.

14.B *عدم التنصل*

يمكن تقديم خدمات عدم التنصل بإثبات المصدر وإثبات الإيصال من خلال آلية توثيق تنطوي على مرحِّل في الطبقة 7.

ويتطلب استخدام آلية التوقيع الرقمي لعدم التنصل التعاون الوثيق بين الطبقتين 6 و7.

الملحـــق جيـــم

خيار موضع التشفير في التطبيقات

(لا يشكل هذا الملحق جزءاً أساسياً من هذه التوصية)

1.C لن تتطلب التطبيقات بمعظمها استخدام تشفير في أكثر من طبقة واحدة. ويعتمد اختيار الطبقة على بعض القضايا الرئيسية على النحو الموضح أدناه:

1) إذا لزم أن يُكتم تدفق الحركة بالكامل، يُختار تشفير الطبقة المادية أو أمن الإرسال (مثل تقنيات الطيف الممتد المناسبة). ويمكن تلبية جميع متطلبات الكتمان بالأمن المادي الكافي والتسيير الموثوق والخواص الوظيفية المماثلة في المرحِّلات.

2) إذا لزمت حماية على قدر عال من تشعبات الحماية (أي بإمكانية وجود مفتاح منفصل لكل رابط تطبيق) وحماية عدم التنصل أو مجالات انتقائية، يقع الاختيار على تشفير طبقة العرض التقديمي. ويمكن أن تكون حماية المجالات الانتقائية هامة لأن خوارزميات التشفير تستهلك كميات كبيرة من قدرة المعالجة. ويمكن للتشفير في طبقة العرض التقديمي أن يوفر السلامة دون التدارك وعدم التنصل، والكتمان كله.

3) إذا لزمت حماية بسيطة بالجملة لكل الاتصالات من نظام طرفي إلى نظام طرفي و/أو جهاز تشفير خارجي (على سبيل المثال، من أجل تقديم الحماية المادية للخوارزمية والمفاتيح أو الحماية ضد البرمجيات المعطوبة)، يقع الاختيار على تشفير طبقة الشبكة. ويمكن لذلك أن يوفر الكتمان والسلامة دون التدارك.

ملاحظة – على الرغم من أن التدارك لم يوفَّر في طبقة الشبكة، يمكن استخدام آليات التدارك العادية في طبقة النقل لتدارك الهجمات التي تكشفها طبقة الشبكة.

4) إذا لزمت السلامة مع التدارك إلى جانب قدر عالٍ من تشعبات الحماية، يقع الاختيار على تشفير طبقة النقل. ويمكن لذلك أن يوفر الكتمان والسلامة مع أو من دون التدارك. ويمكنً لذلك أن يوفر الكتمان والسلامة مع أو من دون التدارك.

5) لا ينصح بالتشفير على طبقة وصلة البيانات للتطبيقات المستقبلية.

2.C عندما تكون اثنتان أو أكثر من هذه القضايا الرئيسية في دائرة الاهتمام، قد تدعو الحاجة إلى تقديم التشفير في أكثر من طبقة واحدة.