الاتحاد الدولي للاتصالات

الأمن في الاتصالات وتكنولوجيا المعلومات

نظرة عامة
على القضايا ذات الصلة
وعلى تطبيق توصيات
قطاع تقييس الاتصالات الحالية
من أجل تحقيق أمن الاتصالات

ITU-T

قطاع تقييس
الاتصالات
في الاتحاد

2009

الاتحاد الدولي للاتصالات

ITU-T

ITU-T - مكتب تقييس الاتصالات (TSB)
Place des Nations – CH-1211 Geneva 20 – Switzerland
E-mail: tsbmail@itu.int Web: www.itu.int/ITU-T

الأمـــن
في الاتصـــالات
وتكنولوجيـــا المعلومـــات

نظرة عامة على القضايا ذات الصلة
وعلى تطبيق توصيات قطاع تقييس الاتصالات الحالية
من أجل تحقيق أمن الاتصالات

سبتمبر 2009

تمهيـــد

مالكوم جونسون

مدير مكتب تقييس الاتصالات،
الاتحاد الدولي للاتصالات

كان أمن الاتصالات وتكنولوجيا المعلومات، حتى عهد قريب نسبياً، يحظى أساساً باهتمام مجالات معينة مثل الصيرفة والفضاء والتطبيقات العسكرية. ولكن سرعة النمو وسعة الانتشار في استعمال اتصالات البيانات، وخصوصاً شبكة الإنترنت، جعل من الأمن مسألة تكاد تهم كل الناس.

ولعل تزايد الاهتمام بأمن تكنولوجيا المعلومات والاتصالات يُعزى في جزء منه إلى الحوادث التي ينتشر الحديث عنها على نطاق واسع، ومنها مثلاً الفيروسات والديدان والمتسللون وما يهدد خصوصية الموظفين. والواقع أن الحوسبة والتواصل بالشبكات يشغلان اليوم قدراً لا بأس به من الحياة اليومية، لذا فإن الحاجة إلى تدابير أمن فعالة لحماية أنظمة الحواسيب والاتصالات لدى الحكومات ودوائر الصناعة والتجارة والبُنى التحتية الأساسية وفرادى المستهلكين عموماً غدت حاجة لا مناص منها الآن. أضف إلى ذلك أن عدداً متزايداً من البلدان لديها اليوم تشريعات لحماية البيانات تستوجب الامتثال لمعايير أثبتت جدواها في مجال سرية البيانات وسلامتها.

ومن المعترف به على نطاق واسع الآن أن الأمن ينبغي أن يدخل في صميم بناء الأنظمة، لا أن يُستدرك بتعديلات. ولكي يكون الأمن فعالاً حقاً، لا بد من أخذه في الاعتبار في جميع مراحل دورة حياة النظام بدءاً من التصور الأولي له وخلال تصميمه وتنفيذه ونشره وأخيراً سحبه من الخدمة. فالتقصير في دراسة الأمن بصورة وافية أثناء مرحلة تصميم المشروع وتطوير الأنظمة قد يخلّف مواطن ضعف في عملية التنفيذ. ولجان المعايير تقوم بدور حيوي في حماية أنظمة الاتصالات وتكنولوجيا المعلومات بإذكاء الوعي بمسائل الأمن وبالحرص على أن تكون اعتبارات الأمن جزءاً أساسياً من المواصفات وبتوفير المعايير التقنية والإرشاد لمساعدة المنفذين والمستعملين على جعل أنظمة الاتصالات وخدماتها متينة بما يكفي للصمود في وجه الهجمات السيبرانية.

لقد كان قطاع تقييس الاتصالات، وما زال، نشطاً في جوانب الأمن التي تخص الاتصالات وتكنولوجيا المعلومات طوال سنوات عديدة. ولكن زيادة استعمال الشبكة رافقها تعاظم في عبء العمل جراء التهديدات الجديدة منها والمستفحلة، وطلبات أعضائنا لمعايير تعينهم في التصدي لهذه التهديدات. ويقدم هذا الدليل نظرة عامة على بعض من العناصر الرئيسية لهذا العمل ويوفر مدخلاً إلى الموارد الواسعة المتاحة من قطاع تقييس الاتصالات لمساعدة جميع المستعملين في التصدي لتحديات أمن الشبكات التي نواجهها.

والتقييس هو حجر الأساس في بناء ثقافة عالمية للأمن السيبراني. وقد تهيأت لنا أسباب النصر في الحرب ضد التهديدات السيبرانية وسيكون النصر حليفنا. سننتصر خلال البناء على عمل الآلاف من الأفراد المتفانين من الإدارات العامة والقطاع الخاص والأوساط الأكاديمية ممن يلتئم شملهم في منظمات مثل الاتحاد الدولي للاتصالات ليضعوا معايير الأمن والمبادئ التوجيهية للممارسات الفضلى. ولئن كان هذا عمل ينأى عن الأضواء أو يتوارى عن الأنظار، فهو مع ذلك عمل لا غنى عنه لحماية مستقبلنا الرقمي. وأود في هذه المناسبة أن أعرب عن تقديري لمهندسي مكتب تقييس

الاتصالات في الاتحاد الذين ما برحوا يعملون دون كلل بالتآزر مع خبراء من مختلف أعضاء الاتحاد لإعداد هذه المعايير والمبادئ التوجيهية.

وقد أُعد هذا الدليل ليكون مرشداً لكبار المسؤولين التنفيذيين والمديرين ممن يقع أمن المعلومات والاتصالات في دائرة مسؤوليتهم أو اهتمامهم، وكذلك لأرباب التكنولوجيا والمنظمين وغيرهم ممن يرغبون في تحسين فهمهم لقضايا أمن تكنولوجيا المعلومات والاتصالات وما يقابلها من توصيات لقطاع تقييس الاتصالات تعالج تلك القضايا. وإنني على ثقة من أن هذا الكتيب سيكون دليلاً مفيداً لمن يسعون إلى تناول مسائل الأمن وإنني أرحب بتلقي تعليقات من القراء للاستئناس بها في طبعات قادمة.

مالكوم جونسون

مدير مكتب تقييس الاتصالات،
الاتحاد الدولي للاتصالات

المحتويات

الصفحة

الصفحة

الصفحة

الصفحة

شكـــر وتقديـــر

أُعدّ هذا الكتيب بمساهمة من مؤلفين عديدين ممن شاركوا في وضع توصيات قطاع تقييس الاتصالات المتصلة بهذا الموضوع أو شاركوا في اجتماعات لجان دراسات وحلقات العمل والحلقات الدراسية التي نظمها قطاع تقييس الاتصالات في هذا الخصوص. وينبغي توجيه الشكر إلى المقررين والمحررين ومنسقي الأمن في لجان دراسات الاتحاد الدولي للاتصالات، وإلى مستشاري الاتحاد الدولي للاتصالات/مكتب تقييس الاتصالات وعلى الأخص منهم السيد هيرب بيرتين الرئيس السابق للجنة الدراسات الرئيسية في قطاع تقييس الاتصالات المعنية بالعمل على أمن الاتصالات، ومايك هاروب المقرر السابق لمشروع الأمن.

ملخص تنفيذي

الغرض من هذا الدليل هو عرض مقدمة واسعة لعمل قطاع تقييس الاتصالات في مجال الأمن. وهو موجه إلى من يقع أمن المعلومات والاتصالات وما يتصل به من معايير في دائرة مسؤوليتهم أو اهتمامهم، وإلى من يحتاج لمجرد تحسين فهمه لقضايا الأمن في تكنولوجيا المعلومات والاتصالات وما يقابلها من توصيات لقطاع تقييس الاتصالات.

ويُستهل النص بنظرة عامة على أنشطة قطاع تقييس الاتصالات في مجال الأمن. وترد في هذا القسم وصلات إلكترونية إلى بعض الموارد الأساسية الأمنية والمعلومات التوعوية لدى قطاع تقييس الاتصالات. وبالإضافة إلى ذلك، يضم هذا الجزء التمهيدي من الدليل جدولاً موجزاً يبين كيف يمكن لفئات مختلفة من المستعملين أن تستعمل الدليل.

وبعد ذلك، تُقدَّم المتطلبات الأساسية لحماية تطبيقات تكنولوجيا المعلومات والاتصالات وخدماتها ومعلوماتها في قسم يفسر التهديدات ومواطن الضعف التي تستدعي هذه المتطلبات، ويدرس دور المعايير في تلبيتها ويوضح بعض الميزات اللازمة لحماية مختلف الأطراف ذات المصلحة الوثيقة في استعمال وتشغيل مرافق تكنولوجيا المعلومات والاتصالات. وعلاوة على ذلك، يقدم هذا القسم مسوغات معايير الأمن في تكنولوجيا المعلومات والاتصالات ويوجز تطور عمل قطاع تقييس الاتصالات في هذا المجال.

ثم تقدَّم المعماريات الأمنية التنوعية للأنظمة المفتوحة والاتصالات من طرف إلى طرف، إلى جانب بعض المعماريات الخاصة بتطبيقات محددة. وترسي كل من هذه المعماريات إطاراً يمكن تطبيق الأوجه المتعددة للأمن ضمنه على نحو متسق. كما أنها تقيّس المفاهيم الكامنة وراء خدمات الأمن وآلياته وتوفر مفردات موحدة لمصطلحات أمن تكنولوجيا المعلومات والاتصالات ومفاهيمه الأساسية. وتشكل المبادئ العامة التي تطرحها هذه المعماريات أساساً للعديد من المعايير الأخرى بشأن خدمات الأمن وآلياته وبروتوكولاته. ويقدم هذا القسم أيضاً وصلة إلكترونية إلى المبادئ التوجيهية الأمنية المتعلقة بالأنشطة الحرجة المرتبطة بدورة حياة أمن الشبكات.

ثم يجري تناول موضوعات مختارة في الإدارة الأمنية في قسم يدرس إدارة أمن المعلومات وإدارة المخاطر والاستجابة للحوادث والتعامل معها.

بعدئذ، يناقَش الدليل ودوره في دعم الخدمات الأمنية إلى جانب ما يتصل بها من مواضيع الاستيقان وإدارة الهوية. ويُعرض في هذا القسم مواضيع مثل البُنى التحتية للمفتاح العمومي والاستدلال الأحيائي عن بُعد (أي المعلومات التي يمكن تعرّف هوية أصحابها شخصياً والاستيقان باستعمال أجهزة الاستدلال الأحيائي في بيئات الاتصالات) والخصوصية. كما يغطي هذا القسم أهمية حماية قاعدة معلومات الدليل. ويلي ذلك بحث في تأمين البنية التحتية للشبكة ثم تغطى المواضيع المتصلة بإدارة الشبكة والخدمات المشتركة في إدارة الأمن.

ويرد تالياً وصف لأمثلة ونُهُج محددة في أمن الشبكات. فيبدأ القسم بنظرة على المتطلبات الأمنية لشبكات الجيل التالي يليها استعراض لشبكات الاتصالات المتنقلة التي تمر بمرحلة انتقالية من التنقل على أساس تكنولوجيا واحدة (مثل النفاذ المتعدد بتقسيم شفري (CDMA) أو النظام العالمي للاتصالات المتنقلة (GSM)) إلى التنقل عبر منصات غير متجانسة باستعمال بروتوكول الإنترنت. ويلي ذلك دراسة الأحكام الأمنية للشبكات المنـــزلية والكبل التلفزيوني. وأخيراً، يرد عرض موجز للتحديات الأمنية التي تواجه شبكات الاستشعار في كل مكان.

وعلى الرغم من أن مطوري التطبيقات اليوم يولون عناية أكبر إلى الحاجة إلى بناء الحصانة الأمنية في صلب منتجاتهم، بدلاً من استدراكها بتعديلات أمنية بعد انتقال التطبيقات إلى مرحلة الإنتاج، فإن المخاطر لا تزال محدقة بالتطبيقات

في بيئة من التهديدات المتعاظمة ومواطن الضعف الكامنة. ويستعرض القسم المعني بأمن التطبيقات عدداً من تطبيقات تكنولوجيا المعلومات والاتصالات، بما في ذلك الاتصالات الصوتية عبر بروتوكول الإنترنت والتلفزيون عبر بروتوكول الإنترنت والفاكس الآمن، مع التركيز الخاص على الميزات الأمنية المحددة في توصيات قطاع تقييس الاتصالات.

ويدرس القسم التالي كيفية مواجهة بعض التهديدات المشتركة في الشبكة مثل الرسائل الاقتحامية والشفرات الخبيثة وبرمجيات التجسس. وينظر أيضاً في أهمية الإخطار في الوقت المناسب ونشر التحديثات والحاجة للتنظيم والاتساق في التعامل مع الحوادث الأمنية.

ويرد ختاماً قسم قصير عن الاتجاهات المستقبلية المحتملة لتقييس أمن تكنولوجيا المعلومات والاتصالات، يليه استعراض لمصادر معلومات إضافية.

وترد ملحقات بشأن التعاريف والمختصرات المستعملة في الدليل، وخلاصة عن لجان الدراسات ذات الصلة بالأمن وقائمة كاملة بالتوصيات المشار إليها في هذا الدليل.

توطئة للطبعة الرابعة

خضع هيكل الدليل ومحتوياته لمراجعة لا بأس بها في الطبعة الرابعة له. فمنذ صدور الطبعة الأولى من الدليل في عام 2003، طرق قطاع تقييس الاتصالات العديد من مجالات العمل الجديدة. وبالإضافة إلى ذلك، استُكمل ونُشر عدد وافر من التوصيات الجديدة، وأعيدت هيكلة لجان الدراسات في أعقاب اجتماع الجمعية العالمية لتقييس الاتصالات عام 2008. وأية محاولة لتغطية كل هذا العمل بالتفصيل كانت ستتمخض عن وثيقة مطولة ومعقدة وغير عملية. فبعد التشاور مع أعضاء قطاع تقييس الاتصالات، وضعت بعض المبادئ التوجيهية لهذه الطبعة. وهي تشمل الأتي:

- ينبغي لهذا المنشور أن يكون قريب المأخذ لجمهور واسع وأن يسعى لتحاشي الاصطلاحات والمصطلحات المعقدة التي لا تُفهم غالباً إلا في الدوائر المتخصصة؛
- وينبغي للنص أن يكون مكملاً، لا مكرراً، للمواد القائمة المتاحة في أشكال أخرى (كالتوصيات)؛
- وينبغي أن يُكتب ليتسنى نشره كوثيقة قائمة بذاتها مطبوعة أو كوثيقة إلكترونية؛
- وينبغي للنص أن يستخدم قدر الإمكان وصلات إلكترونية إلى التوصيات وغيرها من مصادر المواد المتاحة للجمهور. إذ إن المعلومات التفصيلية الفائضة عن الحاجة لتحقيق الأهداف الأساسية ينبغي الإحالة إليها بوصلات إلكترونية؛
- وينبغي للنص أن يركز على العمل الذي أنجز ونشر، إلى أقصى حد ممكن، بدلاً من العمل المخطط أو قيد التنفيذ.

وتماشياً مع هذه الأهداف، لا يسعى الدليل لتغطية جميع أعمال قطاع تقييس الاتصالات في مجال الأمن، المنجزة منها والجارية؛ بل هو يركز على مواضيع مختارة رئيسية ويقدم وصلات إلكترونية عبر شبكة الإنترنت تتيح الاطلاع على معلومات أوفى.

ويُنشر هذا الدليل في شكل نسخة ورقية ونسخة إلكترونية على السواء. فتوفَّر لقراء النسخة الإلكترونية من النص وصلات إلكترونية مباشرة إلى التوصيات المدرجة وغيرها من الوثائق على شبكة الإنترنت. أما قراء النسخة الورقية من النص، فيجدون جميع التوصيات المشار إليها مدرجة في الملحق دال. ويمكن النفاذ إليها على العنوان الإلكتروني: www.itu.int/rec/T-REC/en.

1. مقـــدمة

1 مقدمة

1.1 غرض الدليل ونطاقه

أُعد هذا الدليل لكبار المسؤولين التنفيذيين والمديرين ممن يقع في دائرة مسؤوليتهم أو اهتمامهم أمن المعلومات والاتصالات والمعايير المتصلة به ليتعرفوا على العمل الجاري في قطاع تقييس الاتصالات في مجال أمن الاتصالات. أضف إلى ذلك أن الدليل سيسترعي اهتمام آخرين ممن يرغبون في تحسين فهمهم لقضايا أمن تكنولوجيا المعلومات والاتصالات وما يقابلها من توصيات لقطاع تقييس الاتصالات تعالج تلك القضايا.

ويلقي الدليل نظرة عامة على أمن الاتصالات وتكنولوجيا المعلومات، ويدرس بعضاً من القضايا العملية المرتبطة به، ويبين كيفية تناول الجوانب المختلفة لأمن تكنولوجيا المعلومات والاتصالات في العمل التقييسي لقطاع تقييس الاتصالات. ويوفر الدليل مادة تعليمية مشفوعة بوصلات إلكترونية للاطلاع على إرشادات بمزيد من التفصيل وعلى مواد مرجعية إضافية. وهو يوفر، على وجه الخصوص، وصلات مباشرة إلى توصيات قطاع تقييس الاتصالات وما يتصل بها من وثائق مرجعية وتوعوية. ويضم الدليل بين دفتي كتاب واحد مواد تتعلق بالأمن مختارة من توصيات قطاع تقييس الاتصالات، ويشرح العلاقات القائمة بين مختلف جوانب العمل. وترد فيه النتائج التي تحققت من التقييس المتصل بالأمن في قطاع تقييس الاتصالات منذ صدور الطبعة الثانية من الدليل. ويركز الشطر الأكبر منه على الأعمال التي استُكملت بالفعل. أما نتائج الأعمال الجارية حالياً فستتناولها الطبعات المقبلة من هذا الدليل.

وبالإضافة إلى أعمال قطاع تقييس الاتصالات، تضطلع الأمانة العامة وبعض القطاعات الأخرى في الاتحاد الدولي للاتصالات بالعمل الأمني. ومن الأمثلة على ذلك، العمل المعني بالأمن السيبراني (www.itu.int/cybersecurity) وتقرير الممارسات الفضلى لقطاع تنمية الاتصالات.

2.1 كيفية استعمال هذا الدليل

يهدف هذا الدليل إلى تقديم نظرة شاملة واسعة رفيعة المستوى على أنشطة المعايير الأمنية في قطاع تقييس الاتصالات. وتُقدَّم وصلات إلكترونية مباشرة لمن يرغبون بالتعمق في تفاصيل معلومات التوصيات المنشورة وما يتصل بها من وثائق. وتتعدد سبل استعمال الدليل. ويبين الجدول 1 كيف يمكن استعماله لمعالجة احتياجات المستعملين على اختلافهم.

الجدول 1 – كيف يعالج الدليل احتياجات المستعملين على اختلافهم

المنظمة	فئة المستعملين	الاحتياجات	كيف يمكن للدليل أن يعالج الاحتياجات
مقدمو خدمات اتصالات	كبار المسؤولين التنفيذيين/المديرون	نظرة شاملة واسعة النطاق على جهود التقييس خارطة طريق رفيعة المستوى إلى المعايير ذات الصلة	يعالج الدليل هذه الاحتياجات مباشرة
	مهندسو التصميم والنشر	خارطة طريق إلى المعايير ذات الصلة تفاصيل تقنية مرتبطة بمجالات محددة	يقدم الدليل خارطة طريق مشفوعة بوصلات إلكترونية إلى نصوص تفسيرية مفصلة توفر التوصيات تفاصيل تقنية
باعة خدمات الاتصالات	كبار المسؤولين التنفيذيين/المديرون	نظرة شاملة واسعة النطاق على جهود التقييس خارطة طريق رفيعة المستوى إلى المعايير ذات الصلة	يعالج الدليل هذه الاحتياجات مباشرة
	مديرو المنتجات	خارطة طريق إلى المعايير ذات الصلة	يقدم الدليل خارطة طريق مشفوعة بوصلات إلكترونية إلى نصوص تفسيرية مفصلة
	مصممو المنتجات	تفاصيل تقنية مرتبطة بمجالات محددة	يقدم الدليل خارطة طريق مشفوعة بوصلات إلكترونية إلى نصوص تفسيرية مفصلة توفر التوصيات تفاصيل تقنية
المستعملون النهائيون	التقنيون	إمكانية الاهتمام بتفاصيل تقنية مرتبطة بمجالات محددة	يقدم الدليل خارطة طريق مشفوعة بوصلات إلكترونية إلى نصوص تفسيرية مفصلة بشأن مجالات محددة
	غير التقنيين	إمكانية الاهتمام بنظرة شاملة واسعة النطاق على جهود التقييس	يعالج الدليل هذه الاحتياجات مباشرة
الأوساط الأكاديمية	الطلاب/المعلمون	خارطة طريق إلى المعايير ذات الصلة تفاصيل تقنية مرتبطة بمجالات محددة الاطلاع على جهود التقييس الجديدة والمقبلة	يقدم الدليل خارطة طريق مشفوعة بوصلات إلكترونية إلى نصوص تفسيرية مفصلة بشأن مجالات محددة
الحكومة	كبار المسؤولين التنفيذيين والمديرون	نظرة شاملة واسعة النطاق على جهود التقييس خارطة طريق رفيعة المستوى إلى المعايير ذات الصلة	يعالج الدليل هذه الاحتياجات مباشرة
	الهيئات التنظيمية		
	صناع السياسات		
منظمات غير حكومية	كبار المسؤولين التنفيذيين/المديرون	نظرة شاملة واسعة النطاق على جهود التقييس خارطة طريق رفيعة المستوى إلى المعايير ذات الصلة	يعالج الدليل هذه الاحتياجات مباشرة
	التطوير وبناء القدرات	خارطة طريق إلى المعايير ذات الصلة تفاصيل تقنية مرتبطة بمجالات محددة	يقدم الدليل خارطة طريق مشفوعة بوصلات إلكترونية إلى نصوص تفسيرية مفصلة بشأن مجالات محددة توفر التوصيات تفاصيل تقنية

2. نظرة شاملة على أنشطة قطاع تقييس الاتصالات في مجال الأمن

2 نظرة شاملة على أنشطة قطاع تقييس الاتصالات في مجال الأمن

1.2 مقدمة

ظل عمل قطاع تقييس الاتصالات بشأن أمن تكنولوجيا المعلومات والاتصالات جارياً منذ عقدين ونيف من الزمن، وأعدت لجان دراسات عديدة، خلال هذه الفترة، توصيات وتوجيهات في عدد من المجالات الرئيسية. وتتولى لجنة الدراسات 17 الآن المسؤولية الرئيسية عن العمل الأمني لقطاع تقييس الاتصالات، وأُسندت إليها كذلك صفة لجنة الدراسات الرئيسية في مجال الأمن. بيد أن جوانباً من الأمن تمتد إلى معظم مجالات عمل قطاع تقييس الاتصالات، وتضطلع معظم لجان الدراسات بأعمال أمن تتعلق بمجال مسؤوليتها.

وكجزء من مسؤوليتها بوصفها لجنة الدراسات الرئيسية في مجال الأمن، وضعت لجنة الدراسات 17 عدداً من المنشورات المرجعية والتوعوية. وتساعد هذه المنشورات، التي يأتي هذا الدليل في عدادها، في الجهود المبذولة لتنسيق أعمال الأمن على الصعيد الداخلي في قطاع تقييس الاتصالات فضلاً عن أنها تساعد في الترويج لهذه الأعمال بين جماعات في ميادين أوسع كثيراً وتشجع على استعمال التوصيات.

ويتضمن هذا القسم نظرة شاملة على المنشورات المرجعية والتوعوية لقطاع تقييس الاتصالات، ويقدم ملخصاً بيانياً بالأعمال الأمنية الجارية حالياً.

2.2 الوثائق المرجعية والتوعوية

يحتفظ قطاع تقييس الاتصالات بعدد من المنشورات والمواقع على شبكة الإنترنت يمكن من خلالها الاطلاع على معلومات أكثر تفصيلاً عن التوصيات وأعمال الأمن في قطاع تقييس الاتصالات.

ويوفر الموقع الإلكتروني للجنة الدراسات 17، لجنة الدراسات الرئيسية في مجال الأمن، ملخصاً لمسؤوليات اللجنة وأنشطتها. ويضم هذا الموقع أيضاً ملخصات ووصلات إلكترونية إلى وثائق ومواد توعوية، ومعلومات عن ورش عمل سابقة وعروض وأنشطة توعوية، ووصلات إلكترونية إلى توجيهات أمنية تشمل برنامجاً تعليمياً عن كتابة برامج سالمة وآمنة.

وترد في الفصل 12 معلومات أكثر تفصيلاً عن مختلف جوانب أعمال الأمن مع وصلات إلكترونية مباشرة إلى مزيد من المعلومات.

3.2 نظرة شاملة على مواضيع وتوصيات الأمن الرئيسية

يقدم الجدول 2 مرجعاً سريعاً لبعض من المواضيع الرئيسية والتوصيات المرتبطة بها التي يرد بحثها في هذا الدليل. وتوفَّر لقراء النسخة الإلكترونية من النص وصلات إلكترونية مباشرة إلى نص كل موضوع وموضوع فرعي وإلى التوصيات المدرجة. ويحوي الملحق دال قائمة كاملة بالتوصيات المشار إليها في هذا الدليل. وأُدرجت وصلات إلكترونية في الملحق دال بحيث يتمكن قارئ النسخة الإلكترونية من النص من التوصيل مباشرة لتحميل التوصيلات.

الجدول 2 – نظرة شاملة على بعض المواضيع الرئيسية والتوصيات المختارة

الموضوع	المواضيع الفرعية	أمثلة عن توصيات ومنشورات ذات صلة
3 متطلبات الأمن	2.3 التهديدات والمخاطر ومواطن الضعف 3.3 أهداف الأمن 4.3 مسوغات معايير الأمن 6.3 الموظفون ومتطلبات الأمن المادية	X.1205: لمحة عامة عن الأمن السيبراني E.408: متطلبات أمن شبكات الاتصالات X.1051: المبادئ التوجيهية لإدارة أمن المعلومات من أجل منظمات الاتصالات تكنولوجيات المنشآت الخارجية للشبكات العمومية تطبيقات الحواسيب والمعالجات الصغرية في بناء كبلات الاتصالات وتركيبها وحمايتها
4 معماريات الأمن	1.4 معمارية أمن الأنظمة المفتوحة 2.4 خدمات الأمن 3.4 معمارية أمن الأنظمة التي تكفل الاتصالات من طرف إلى طرف 2.3.4 تيسر الشبكة ومكوناتها 4.4 توجيهات التنفيذ 5.4 المعماريات الخاصة بتطبيقات محددة	X.800: معمارية أمن الأنظمة المفتوحة X.805: معمارية أمن الأنظمة التي تكفل الاتصالات من طرف إلى طرف X.810: نظرة شاملة على إطار الأمن الإضافة 3 للسلسلة X : سلسلة توصيات قطاع تقييس الاتصالات X.800- X.849 إضافة بشأن المبادئ التوجيهية لتنفيذ أمن النظام والشبكة X.1162 : معمارية وعمليات الأمن لشبكة الند إلى الند X.1161: إطار لاتصالات آمنة من ند إلى ند X.1143: معمارية الأمن لأمن الرسالة في خدمات الويب المتنقلة.
5 إدارة الأمن	1.5 إدارة أمن المعلومات 2.5 إدارة المخاطر 3.5 التعامل مع الحوادث	X.1051: المبادئ التوجيهية لإدارة أمن المعلومات من أجل منظمات الاتصالات X.1055: المبادئ التوجيهية لإدارة المخاطر ومواصفاتها في منظمات الاتصالات E.409: تنظيم الحوادث والتعامل مع الحوادث الأمنية
6 الدليل والاستيقان وإدارة الهوية	1.6 حماية معلومات الدليل 4.1.6 حماية الخصوصية 2.6 آليات أمن المفتاح العمومي 3.2.6 البنى التحتية للمفتاح العمومي 4.6 إدارة الهوية 5.6 الاستدلال الأحيائي عن بعد	X.500: الدليل: نظرة عامة على المفاهيم والنماذج والخدمات X.509: الدليل: الإطار العام لشهادات المفاتيح العمومية والنعوت X.1171: التهديدات ومتطلبات حماية المعلومات التي يمكن تعرّف هوية أصحابها شخصياً في التطبيقات التي تستعمل تعرّف الهوية على أساس الوسم Y.2720: إطار إدارة الهوية في شبكات الجيل التالي X.1081: إطار لتوصيف جوانب الأمن والسلامة للاستدلال الأحيائي عن بعد X.1089: البنية التحتية للاستيقان بالاستدلال الأحيائي عن بعد
7 تأمين البنية التحتية للشبكة	1.7 شبكة إدارة الاتصالات 2.7 معمارية إدارة الشبكة 4.7 تأمين أنشطة المراقبة والتحكم 5.7 تأمين التطبيقات القائمة على الشبكات 6.7 خدمات إدارة الأمن المشتركة 4.6.7 خدمات الأمن القائمة على معمارية CORBA	M.3010: مبادئ شبكة إدارة الاتصالات X.790: وظيفة إدارة الإشكالات في تطبيقات قطاع تقييس الاتصالات X.711: بروتوكول معلومات الإدارة المشتركة X.736: وظيفة الإبلاغ عن إنذارات الأمن X.740: وظيفة تعقب التدقيق الأمني X.780: المبادئ التوجيهية لشبكة إدارة الاتصالات في تعريف الأغراض التي تديرها معمارية CORBA
8 بعض النُهُج المحددة في أمن الشبكات	1.8 أمن شبكة الجيل التالي 2.8 أمن الاتصالات المتنقلة 3.8 أمن الشبكات المنـــزلية 4.8 متطلبات أمن الاتصالات الكبلية بواسطة بروتوكول الإنترنت (IPCablecom) 6.8 أمن شبكات الاستشعار في كل مكان	Y.2001: نظرة عامة على شبكات الجيل التالي Y.2701: متطلبات أمن شبكة الجيل التالي – الإصدار الأول X.1121: إطار تكنولوجيات الأمن لاتصالات البيانات المتنقلة من طرف إلى طرف X.1111: إطار تكنولوجيات الأمن للشبكة المنـــزلية J.170: مواصفة أمن الاتصالات الكبلية بواسطة بروتوكول الإنترنت (IPCablecom)
9 أمن التطبيقات	1.9 الصوت عبر بروتوكول الإنترنت والوسائط المتعددة 2.9 التلفزيون باستعمال بروتوكول الإنترنت 3.9 الفاكس الآمن 4.9 خدمات الويب 5.9 الخدمات القائمة على أساس العلامة	H.235: إطار الأمن في الأنظمة متعددة الوسائط من السلسلة H X.1191: المتطلبات الوظيفية لجوانب أمن التلفزيون القائم على بروتوكول الإنترنت (IPTV) ومعماريته T.36: المقدرات الأمنية المعدة للاستعمال في مطاريف فاكس الفريق 3 X.1141: لغة التشفير المتداولة في توكيد الأمن (SAML 2.0)
10 التصدي للتهديدات الشائعة في الشبكة	1.10 التصدي للرسائل الاقتحامية 2.10 الشفرة الضارة وبرمجيات التجسس والبرمجيات الخادعة 3.10 التبليغ عن تحديثات البرمجيات ونشرها	X.1231: الاستراتيجيات التقنية في التصدي للرسائل الاقتحامية X.1240: التكنولوجيات التي تنطوي عليها مكافحة البريد الإلكتروني الاقتحامي X.1244: الجوانب العامة لمكافحة الرسائل الاقتحامية في تطبيقات الوسائط المتعددة القائمة على بروتوكول الإنترنت X.1207: مبادئ توجيهية لمقدمي خدمات الاتصالات للتصدي لمخاطر برمجيات التجسس والبرمجيات المحتملة غير المطلوبة X.1206: إطار محايد تجاه البائع للتبليغ الأوتوماتي بالمعلومات المتعلقة بالأمن ونشر التحديثات
لتكملة مجموعة توصيات الأمن لقطاع تقييس الاتصالات انظر http://www.itu.int/ITU-T/recommendations/.		

3. متطلبات الأمن

3 متطلبات الأمن

1.3 مقدمة

لدى إعداد إطار أمني من أي نوع، من الأهمية بمكان أن يكون هناك فهم واضح للاحتياجات. ولا بد لاستعراض شامل لمتطلبات الأمن أن يأخذ في الاعتبار ما يلي: الأطراف المعنية والأصول التي تحتاج إلى الحماية والتهديدات التي يجب حماية هذه الأصول منها ومواطن الضعف المرتبطة بالأصول ومجمل المخاطر المحدقة بالأصول جراء هذه التهديدات ومواطن الضعف.

ويعرّف هذا القسم المتطلبات الأساسية لحماية تطبيقات تكنولوجيا المعلومات والاتصالات وخدماتها ومعلوماتها وينظر في التهديدات ومواطن الضعف التي تستدعي هذه المتطلبات، ويدرس دور المعايير في تلبيتها ويوضح بعض الميزات اللازمة لحماية مختلف الأطراف المشاركة في استعمال وتشغيل مرافق تكنولوجيا المعلومات والاتصالات.

وتتسم متطلبات الأمن بتنوعيتها، وفي آنٍ معاً، بخصوصيتها حسب السياق. وبالإضافة إلى ذلك، تظل بعض الشروط راسخة، في حين أن بعضها الآخر يواكب التطبيقات الجديدة وتغيّر بيئة التهديدات. وجل ما يتناوله هذا القسم بالبحث هو الجانب التنوعي. أما متطلبات التطبيقات والبيئات الخاصة فيأتي بحثها في أقسام لاحقة.

2.3 التهديدات والمخاطر ومواطن الضعف

بصورة عامة، في مجال أمن تكنولوجيا المعلومات والاتصالات، قد نحتاج لحماية أصول الجهات التالية:

- *الزبائن/المشتركون* الذين يحتاجون إلى الثقة في الشبكة والخدمات المقدمة، بما في ذلك تيسّر الخدمات (لا سيما خدمات الطوارئ)؛
- *المجتمعات/السلطات العامة* التي تطلب الأمن من خلال التوجيهات و/أو التشريعات من أجل ضمان تيسّر الخدمات والمنافسة العادلة وحماية الخصوصية؛
- *مشغلو الشبكات/مقدمو الخدمات* أنفسهم الذين يحتاجون إلى الأمن لصون مصالحهم التشغيلية والتجارية والوفاء بالتزاماتهم تجاه الزبائن والجمهور على الصعيد الوطني والدولي.

وتشمل الأصول التي يتعين حمايتها ما يلي:

- الاتصالات وخدمات الحوسبة؛
- المعلومات والبيانات، بما في ذلك البرمجيات والبيانات المتعلقة بخدمات الأمن؛
- ملاك الموظفين؛
- المعدات والمرافق.

ويعرَّف *التهديد الأمني* بأنه انتهاك محتمل للأمن. ومن أمثلة التهديدات ما يلي:

- الإفصاح غير المصرح به عن المعلومات؛
- تدمير أو تعديل البيانات أو المعدات أو غيرها من الموارد على نحو غير مصرح به؛
- سرقة المعلومات أو الموارد الأخرى، أو إزالتها أو فقدانها؛
- انقطاع الخدمات أو الحرمان منها؛
- تقمص شخصية كيان مخوَّل أو التنكر في هيئته.

وقد تكون التهديدات عَرَضية أو متعمدة، سافرة أو مضمرة. فالتهديد العرضي هو تهديد دون نية مبيتة من قبيل خلل في النظام أو البرمجيات أو عطل مادي. أما التهديد المتعمد فهو تهديد يُقْدِم عليه من يرتكب عملاً مقصوداً. وقد تتراوح التهديدات المتعمدة بين الفحص العارض باستعمال أدوات المراقبة المتاحة بسهولة وهجمات متطورة باستعمال معرفة خاصة بالنظام. ويدعى التهديد عند تنفيذه هجوماً. وأما التهديد السافر فهو تهديد يُسفر عن تغيير ما في حال نظام أو في عمله، كتغيير البيانات أو تدمير المعدات المادية. أما التهديد المضمر فلا ينطوي على أي تغيير في الحالة، ومن أمثلته التنصت والتجسس.

وأما *موطن الضعف الأمني* فهو خلل أو ضعف يمكن استغلاله في انتهاك النظام أو المعلومات التي يحتوي عليها. وفي حال وجود موطن ضعف، يمكن أن ينفَّذ تهديداً.

وتميّز توصيات قطاع تقييس الاتصالات أربعة أنواع من مواطن الضعف:

- مواطن ضعف إزاء نموذج تهديد تعود إلى صعوبة توقع التهديدات المحتملة في المستقبل؛
- مواطن ضعف التصميم والمواصفات جراء أخطاء أو إغفالات في تصميم النظام أو البروتوكول مما يجعل نقطة الضعف قائمة بطبيعة الحال؛
- مواطن ضعف التنفيذ تظهر جراء أخطاء أثناء تنفيذ النظام أو البروتوكول؛
- مواطن ضعف التشغيل والتشكيل جراء الاستعمال غير السليم للخيارات في عمليات التنفيذ أو ضعف سياسات وممارسات النشر (مثل عدم استخدام التشفير في شبكة لاسلكية).

والخطر الأمني هو مقياس للآثار السلبية التي يمكن أن تترتب على استغلال موطن ضعف، أي تنفيذ تهديد. وفي حين يتعذر القضاء على المخاطر تماماً، فإن أحد أهداف الأمن هو الإقلال منها إلى مستوى مقبول. ولفعل ذلك لا بد من فهم التهديدات ومواطن الضعف القائمة، ومن تطبيق التدابير المضادة المناسبة. وعادة ما تكون هناك خدمات وآليات أمنية يمكن استكمالها بتدابير غير تقنية مثل الأمن المادي وأمن الموظفين.

وفيما تتغير التهديدات ووسائطها، تظل مواطن الضعف الأمني قائمة طوال عمر نظام أو بروتوكول ما لم تتخذ خطوات محددة للتصدي لها. وإذ تُستعمل البروتوكولات المقيّسة على نطاق واسع جداً، يمكن لأي مواطن ضعف مرتبطة بها أن تستتبع تداعيات خطيرة للغاية وتكون عالمية في نطاقها. لذا تُسنَد أهمية خاصة إلى فهم مواطن الضعف في البروتوكولات وتحديد هويتها، وإلى اتخاذ خطوات للتصدي لها متى حُددت هويتها.

وتقع على عاتق هيئات المعايير مسؤولية التصدي لمواطن الضعف الأمني التي قد تكمن في مواصفات مثل المعماريات والأطر والبروتوكولات، ناهيك عن قدرة هيئات المعايير الفريدة على القيام بذلك. ويتعذر تحقيق الأمن الكافي، حتى وإن توفرت معرفة كافية بالتهديدات والمخاطر ومواطن الضعف المرتبطة بمعالجة المعلومات وشبكات الاتصالات، إلا إذا طُبقت تدابير أمنية بصورة منهجية ووفقاً للسياسات ذات الصلة. ويجب استعراض السياسات نفسها وتحديثها دورياً. كما ولا بد من توفير ما يكفي لإدارة الأمن والاستجابة للحوادث. وسيشمل ذلك إسناد المسؤوليات وتحديد الإجراءات الواجب اتخاذها لمنع وقوع أي حادث أمني وكشفه والتحقيق فيه والرد عليه.

ويمكن لخدمات وآليات الأمن أن تحمي شبكات الاتصالات ضد الهجمات الخبيثة مثل الحرمان من الخدمة والتنصت وتقمص الشخصيات والعبث بالرسائل (تعديلها أو تأخيرها أو حذفها أو إدراج مواد فيها أو تكرارها أو إعادة تسييرها أو إعادة ترتيبها) أو التنصل أو التزوير. وتشمل تقنيات الحماية الوقاية والكشف والتعافي من الهجمات فضلاً عن إدارة المعلومات المتصلة بالأمن. ويجب أن تشمل الحماية تدابير لمنع انقطاع الخدمة بسبب الأحداث الطبيعية (مثل العواصف والزلازل) والهجمات الخبيثة (أفعال متعمدة أو عنيفة). ويجب أيضاً وضع ترتيبات لتسهيل اعتراض السلطات القانونية المخولة أصولاً للاتصالات ومراقبتها.

ويتطلب أمن الشبكات أيضاً تعاوناً واسع النطاق بين مقدمي الخدمات. وتقدم توصية قطاع تقييس الاتصالات E.408 بشأن *متطلبات أمن شبكات الاتصالات* نظرة شاملة على المتطلبات الأمنية وإطاراً يحدد التهديدات الأمنية لشبكات الاتصالات عموماً (للخدمة الثابتة والمتنقلة معاً، وللصوت والبيانات) وتعطي توجيهات لتخطيط التدابير المضادة التي يمكن أن تتخذ للتخفيف من المخاطر الناجمة عن التهديدات. ومن شأن تنفيذ متطلبات قطاع تقييس الاتصالات E.408 أن يسهل التعاون الدولي في المجالات التالية المتعلقة بأمن شبكات الاتصالات:

- تبادل المعلومات ونشرها؛
- التنسيق إزاء الحوادث والرد على الأزمات؛
- توظيف المتخصصين في مجال الأمن وتدريبهم؛
- التنسيق لإنفاذ القانون؛
- حماية البنية التحتية الحرجة والخدمات الحيوية؛
- وضع التشريعات المناسبة.

ومع ذلك، فإن النجاح في الحصول على مثل هذا التعاون يقتضي تنفيذ متطلبات المكونات الوطنية للشبكة على الصعيد الوطني.

أما توصية قطاع تقييس الاتصالات X.1205 بشأن *النظرة الشاملة على الأمن السيبراني*، فهي تصنف التهديدات الأمنية من الناحية التنظيمية إلى جانب مناقشة التهديدات في مختلف طبقات الشبكة.

3.3 أهداف الأمن العامة لشبكات تكنولوجيا المعلومات والاتصالات

تتمثل الأهداف العامة لأمن شبكات الاتصالات بما يلي:

أ) ينبغي ألا ينفذ إلى شبكات الاتصالات ويستعملها إلا المستعملون المخولون؛

ب) ينبغي أن يكون بوسع المستعملين المخولين النفاذ إلى، وتشغيل، الأصول المخول لهم بالنفاذ إليها؛

ج) ينبغي لشبكات الاتصالات أن توفر الخصوصية على المستوى الذي تحدده السياسات الأمنية للشبكة؛

د) ينبغي أن يُساءل جميع المستعملين عن أفعالهم، ليس إلا، في شبكات الاتصالات؛

ه) ينبغي حماية شبكات الاتصالات مما لا تطلبه من نفاذ أو عمليات؛

و) ينبغي أن يكون من الممكن استخراج المعلومات ذات الصلة بالأمن من شبكات الاتصالات (على ألا يتمكن إلا المستعملون المخولون من استخراج مثل هذه المعلومات)؛

ز) إذا كُشفت خروقات أمنية، ينبغي التعامل معها بطريقة مضبوطة وفقاً لخطة محددة سلفاً لتطويق الأضرار المحتملة ضمن حدودها الدنيا؛

ح) بعد كشف خرق أمني، ينبغي أن يكون من الممكن استعادة مستويات الأمن العادية؛

ط) ينبغي أن يوفر الهيكل الأمني لشبكات الاتصالات درجة من المرونة لاستيعاب سياسات أمنية مختلفة وآليات أمنية متفاوتة القوة.

ويمكن تحقيق الأهداف من أ) إلى هـ) من خلال تنفيذ الخدمات الأمنية التالية:

- السرية؛
- سلامة البيانات والنظام والبرنامج؛
- المساءلة، بما في ذلك الاستيقان وعدم التنصل والتحكم بالنفاذ؛
- التيسّر.

وشبكة الجيل التالي هي نمط من شبكات تكنولوجيا المعلومات والاتصالات تزداد أهميته بسرعة. ويرد في القسم 8 بحث متطلبات وأهداف الأمن لشبكات الجيل التالي.

4.3 مسوّغات معايير الأمن

يعود أصل الدعوة لإطار تنوعي لأمن الشبكات في الاتصالات الدولية إلى مصادر مختلفة تشمل الزبائن/الأعضاء والمجتمعات/السلطات العامة ومشغلي الشبكة/مقدمي الخدمة. ويحبذ تناول المتطلبات الأمنية لشبكات الاتصالات بمعايير متفق عليها دولياً، إذ يعزز ذلك النُهُج المشتركة ويعين على التوصيل البيني، فضلاً عن كونه أكثر فعالية من حيث التكلفة من وضع نهج فردية لكل ولاية قضائية.

في بعض الحالات، يمكن أن يكون توفير الخدمات الأمنية واستعمالها مكلفاً جداً بالنسبة إلى قيمة الموجودات الجاري حمايتها، لذلك فمن المهم توفر القدرة على تفصيل خدمات وآليات الأمن على مقاس الاحتياجات المحلية. غير أن هذه القدرة قد تؤدي أيضاً إلى عدد من التوليفات الممكنة من الميزات الأمنية. لذلك، يستحسن وجود ميزات أمنية عامة تغطي مجموعة واسعة من خدمات شبكة الاتصالات لضمان مواءمة الخيارات في تطبيقات مختلفة. إذ يسهِّل التقييس واستعمال الميزات العامة المقيّسة إمكانية التشغيل البيني وتكرار استعمال الحلول والمنتجات، ومفاد ذلك إمكانية تسريع الإتيان بالأمن وبتكلفة أقل.

وتشمل الفوائد الهامة للحلول الأمنية المقيّسة لموردي الأنظمة ومستعمليها على السواء وفورات الحجم الكبير للإنتاج في تطوير المنتجات والتشغيل البيني للمكونات ضمن شبكات الاتصالات.

5.3 تطور معايير الأمن في قطاع تقييس الاتصالات

تطور العمل الأمني في قطاع تقييس الاتصالات إلى حد كبير في السنوات الأخيرة، كما سيتضح في أقسام لاحقة حيث يجري بحث العديد من التوصيات الفردية بمزيد من التفصيل. وتُبحث فيما يلي بعض الجوانب الرئيسية لهذا التطور، لا سيما ما يتصل منها بمتطلبات الأمن.

وبصفة عامة، تعرَّف متطلبات أمن تكنولوجيا المعلومات والاتصالات من حيث التهديدات التي تتعرض لها الشبكة و/أو النظام ومواطن الضعف الكامنة في الشبكة و/أو النظام والخطوات التي يجب اتخاذها لمواجهة التهديدات والحد من مواطن الضعف. وتمتد متطلبات الحماية إلى الشبكة ومكوناته. ويرد تعريف المفاهيم الأساسية للأمن، بما في ذلك التهديدات ومواطن الضعف وتدابير الأمن المضادة، في توصية قطاع تقييس الاتصالات X.800 لعام 1991 بشأن *معمارية الأمن للتوصيل بين الأنظمة المفتوحة في تطبيقات قطاع تقييس الاتصالات*. أما توصية قطاع تقييس الاتصالات E.408 التي سبق ذكرها والتي نشرت في عام 2004 فهي تستند إلى مفاهيم ومصطلحات توصية قطاع تقييس الاتصالات X.800. وإذ تتسم توصية قطاع تقييس الاتصالات E.408 بطبيعتها التنوعية، فهي لا تحدد أو تتناول متطلبات شبكات بعينها. ولا يُنظر في خدمات أمنية جديدة، بل تركز التوصية على الاستفادة من الخدمات الأمنية القائمة المحددة في توصيات قطاع تقييس الاتصالات وغيرها من المعايير ذات الصلة من الهيئات الأخرى.

وتعكس توصية قطاع تقييس الاتصالات X.1205 عام 2008، بعنوان *لمحة عامة عن الأمن السيبراني*، الحاجة لمواجهة الزيادة العددية والنوعية لتهديدات الأمن السيبراني (الفيروسات والديدان وأحصنة طروادة والهجمات المتحايلة وسرقة الهوية والرسائل الاقتحامية وغيرها من أشكال الهجوم السيبراني). وتهدف هذه التوصية إلى بناء قاعدة من المعارف يمكن أن تساعد في تأمين شبكات المستقبل. وتتوفر تكنولوجيات متنوعة لمواجهة التهديدات بما في ذلك: المسيّرات والجدران الواقية وبرمجيات الحماية من الفيروسات وأنظمة كشف الاختراق وأنظمة الحماية من الاختراق والحوسبة الآمنة والتدقيق والمراقبة. كما يرد بحث مبادئ حماية الشبكات مثل الدفاع في العمق وإدارة النفاذ. وتُستعرض استراتيجيات وتقنيات إدارة المخاطر، بما في ذلك قيمة التدريب والتعليم في حماية الشبكة. وترد كذلك أمثلة عن تأمين الشبكات المختلفة استناداً إلى تقنيات جرى بحثها.

وتعرّف توصية قطاع تقييس الاتصالات X.1205 الأمن السيبراني كمجموعة من الأدوات والسياسات والمفاهيم الأمنية والحمايات الأمنية والمبادئ التوجيهية ونهج إدارة المخاطر والإجراءات والتدريبات والممارسات الفضلى والضمانات والتكنولوجيات التي يمكن استعمالها لحماية البيئة السيبرانية والمنظمة وأصول المستعمل. وتشمل الأصول المشار إليها أجهزة الحوسبة ومستعملي الحوسبة والتطبيقات/الخدمات وأنظمة الاتصالات واتصالات الوسائط المتعددة ومجمل المعلومات المرسلة و/أو المخزنة في البيئة السيبرانية. وعلى النحو المحدد هنا، فإن الأمن السيبراني يضمن تحقيق الخصائص الأمنية للمنظمة (بما في ذلك تيسر الخدمة وسلامتها وسريتها) والحفاظ عليها، ويحمي أصول المستعمل من المخاطر الأمنية ذات الصلة في البيئة السيبرانية.

ويختفي مفهوم المحيط العازل في بيئة الأعمال اليوم، حيث تصبح الحدود بين شبكات الداخل والخارج "أرق". وتشغَّل التطبيقات فوق الشبكات بطريقة الطبقات المتعددة. ولا بد من تحقق الأمن داخل كل من هذه الطبقات وفيما بينها. وبالنهج الأمني متعدد الطبقات تتمكن المنظمات من استحداث مستويات متعددة من الدفاع ضد التهديدات.

ويمكن استعمال تقنيات الأمن السيبراني لضمان التيسر والسلامة والاستيقان والسرية وعدم التنصل، وكذلك لضمان احترام خصوصية المستعمل. كما يمكن استعمال تقنيات الأمن السيبراني للتثبت من جدارة المستعمل بالثقة.

وتحتاج المنظمات إلى وضع خطة شاملة لمعالجة الأمن في كل سياق بعينه. فالأمن ليس حلة ذات "مقاس واحد يناسب الجميع". وينبغي النظر إلى الأمن بوصفه عملية مستمرة تغطي حماية الأنظمة والشبكات والتطبيقات والموارد. كما يجب أن يكون الأمن شاملاً لجميع طبقات النظام. ولدى اقترانه بالحزم في إدارة السياسات والإنفاذ، يوفر اعتماد نهج أمني متعدد الطبقات خياراً من حلول أمنية يمكن أن تكون على وحدات تجميعية ومرنة ومتنوعة المقاييس.

وتشمل تقنيات الأمن السيبراني الحالية ما يلي:

- التجفير: تدعم هذه التكنولوجيا القوية عدداً من الخدمات الأمنية بما في ذلك تشفير البيانات أثناء الإرسال وخلال التخزين.
- ضوابط النفاذ: تهدف إلى الحد من قدرة المستعملين على النفاذ إلى المعلومات الموجودة في المواقع المضيفة أو الشبكات، أو على استعمال هذه المعلومات أو استعراضها أو تعديلها.
- سلامة النظام: تهدف إلى ضمان عدم تعديل أو إعطاب النظام والبيانات الخاصة به من جانب أطراف غير مخولة أو بطريقة غير مخوّلة.
- التدقيق والرصد والمراقبة: تساعد هذه التقنية مسؤولي النظام على جمع سجلات الشبكة واستعراضها أثناء وبعد وقوع هجوم. ويمكن استعمال البيانات لتقييم فعالية الاستراتيجية الأمنية التي تنشرها الشبكة.
- الإدارة: تساعد مسؤولي النظام في استعراض إعدادات الأمن وتشكيلها في مواقعهم المضيفة وشبكاتهم. ويمكن استعمال ضوابط الإدارة للتحقق من دقة الشبكة وإعدادات العناصر المرفقة.

6.3 متطلبات أمن الموظفين والأمن المادي

في الشطر الأكبر منها، تركز توصيات قطاع تقييس الاتصالات المتعلقة بالأمن على الجوانب التقنية للنظام والشبكة. وتُحدد بعض أوجه أمن الموظفين في توصية قطاع تقييس الاتصالات X.1051 بعنوان *مبادئ توجيهية لإدارة أمن المعلومات من أجل منظمات الاتصالات*. ورغم البعد بالغ الأهمية للأمن المادي في الحماية أيضاً، فهو يخرج إلى حد كبير عن نطاق غالبية أعمال قطاع تقييس الاتصالات. بيد أن الوثيقتين المحددتين أدناه تتناولان المتطلبات العامة للأمن المادي المحددة في توصية قطاع تقييس الاتصالات X.1051 والأمن المادي المتصل بالمنشأة الخارجية.

وتشمل متطلبات الحماية المادية للمنشأة الخارجية التأكد من أن المعدات قادرة على مقاومة خطر الحرائق والكوارث الطبيعية والأضرار غير المتعمدة أو المتعمدة. وتتناول منشورات قطاع تقييس الاتصالات أساليب تحقيق الحماية للمكونات والكابلات والوحدات المغلقة والخزانات وغيرها. كما تتناول *تكنولوجيات المنشأة الخارجية في الشبكات العامة* (1991) *والاستعانة بالحواسيب والمعالجات الصغرية في بناء كبلات الاتصالات وتركيبها وحمايتها* (1999). وتتناول هذه الوثائق أيضاً أنظمة المراقبة المعدة لاتقاء الأضرار، وتقترح سبلاً للرد على المشاكل واستعادة وظائف النظام بأسرع ما يمكن.

4. معماريات الأمن

4 معماريات الأمن

تقدم معماريات الأمن والنماذج والأُطر ذات الصلة هيكلاً وسياقاً يمكن من خلالهما إعداد المعايير التقنية ذات الصلة على نحو متسق. وفي أوائل الثمانينات من القرن المنصرم، تبينت الحاجة إلى إطار يمكن تطبيق الأمن فيه ضمن معمارية اتصالات متعددة الطبقات. وأدى ذلك إلى *وضع معمارية الأمن للأنظمة المفتوحة* (توصية قطاع تقييس الاتصالات X.800). وكانت تلك فاتحة مجموعة من المعايير المعمارية المعدة لدعم خدمات الأمن وآلياته. وقد أفضى هذا العمل الذي أُنجز معظمه بالتعاون مع منظمة المعايير الدولية (ISO) إلى مزيد من المعايير شملت نماذج الأمن وأطره ووصَّفت كيفية تطبيق أنماط محددة من الحماية في بيئات معينة.

ولاحقاً، تبينت الحاجة لمعماريات أمن تنوعية وأخرى مخصصة لتطبيقات بعينها على السواء. وأسفر ذلك عن وضع *معمارية أمن للأنظمة التي توفر الاتصالات من طرف إلى طرف* (توصية قطاع تقييس الاتصالات X.805)، فضلاً عن عدد من المعماريات المخصصة لتطبيقات بعينها. وذلك لمعالجة مجالات مثل إدارة الشبكة والاتصالات بين الأنداد ومخدمات الاتصالات المتنقلة على الويب. ويرد وصف توصية قطاع تقييس الاتصالات X.805 لاحقاً في هذا القسم، فهي تتمم توصيات أخرى من سلسلة X.800 من خلال توفير الحلول الأمنية في إطار أمن الشبكات من طرف إلى طرف. retrieval

1.4 معمارية أمن الأنظمة المفتوحة وما يتصل بها من معايير

كانت أولى معماريات أمن الاتصالات التي خضعت للتقييس في إطار التوصية ITU-T X.800 هي معمارية أمن الأنظمة المفتوحة. وتحدد هذه التوصية العناصر المعمارية المتصلة بالأمن والتي يمكن تطبيقها تبعاً للظروف التي تكون الحماية مطلوبة لها. وعلى وجه التحديد، تقدم توصية قطاع تقييس الاتصالات X.800 وصفاً عاماً لخدمات الأمن والآليات المتصلة بذلك التي يمكن استعمالها لتوفير تلك الخدمات. وتحدد أيضاً، من حيث النموذج المرجعي الأساسي سباعي الطبقات للتوصيل ما بين الأنظمة المفتوحة (OSI)، أكثر المواقع (أي الطبقات) ملاءمة لتنفيذ خدمات الأمن.

وتقتصر التوصية ITU-T X.800 على تلك الجوانب المرئية من مسار الاتصالات والتي تمكّن الأنظمة الطرفية من تحقيق النقل الآمن للمعلومات فيما بينها. وهي لا تسعى إلى تقديم أي نوع من مواصفات التنفيذ كما أنها لا توفر وسائل تقييم امتثال أي تنفيذ لهذا المعيار أو لغيره من معايير الأمن. ولا تشير كذلك، بأي درجة من التفصيل، إلى أي تدابير أمن إضافية قد تلزم في الأنظمة الطرفية لتوفير ملامح أمن الاتصالات.

وعلى الرغم من أن توصية قطاع تقييس الاتصالات X.800 صممت تحديداً بمثابة معمارية أمن للتوصيل OSI فقد تبين أن المفاهيم التي تنطوي عليها تتمتع بقدر أوسع من القبول وإمكانية التطبيق. ومعيار التوصية على جانب من الأهمية من حيث إنه يمثل أول توافق في الآراء عالمياً بشأن تعاريف خدمات الأمن الأساسية (أي *الاستيقان والتحكم في النفاذ وسرية البيانات وسلامة البيانات وعدم التنصل*) إلى جانب خدمات أكثر عمومية من قبيل *الوثوق بالوظيفة والكشف عن الحدث والتحقق من الأمن واستعادته*. كما يبين أي من آليات الأمن يمكن أي يُستعمل لتوفير خدمات الأمن. وقبل اعتماد توصية قطاع تقييس الاتصالات X.800 كانت هنالك طائفة واسعة من وجهات النظر بشأن تحديد ما هي خدمات الأمن الأساسية المطلوبة وما هو بالضبط الدور الذي يؤديه كل منها. وتعبّر توصية قطاع تقييس الاتصالات X.800 عن توافق قوي في الآراء دولياً بصدد هذه الخدمات.

وتُعزى قيمة توصية قطاع تقييس الاتصالات X.800 وإمكانية تطبيقها إلى أنها تمثل توافقاً هاما في الآراء بشأن مدلول المصطلحات المستخدمة لوصف جوانب الأمن وبشأن مجموعة خدمات الأمن اللازمة لتوفير الحماية لعمليات توصيل البيانات وبشأن طبيعة خدمات الأمن تلك.

وقد برزت الحاجة، أثناء وضع توصية قطاع تقييس الاتصالات X.800، إلى معايير أمن إضافية فيما يتعلق بالاتصالات. وتبعاً لذلك، انصبّت الجهود على عدد من المعايير الداعمة والتوصيات المعمارية التكميلية. ويناقش بعض هذه التوصيات أدناه.

2.4 خدمات الأمن

وضعت هياكل الأمن لتقديم توصيفات شاملة ومتسقة لكل من خدمات الأمن المعرفة في توصية قطاع تقييس الاتصالات X.800. والغرض من هذه المعايير تناول جميع جوانب كيفية تطبيق خدمات الأمن في سياق معمارية أمن معينة، بما في ذلك معماريات أمن ممكنة في المستقبل.

وتركز الهياكل على توفير الحماية للأنظمة وللكيانات ضمن الأنظمة والتفاعل ما بين الأنظمة. وهي لا تتناول منهجية بناء الأنظمة أو آلياتها.

وتتناول الهياكل كلا من عناصر البيانات وتعاقب العمليات (باستثناء عناصر البروتوكولات) المستخدمة لتقديم خدمات أمن معينة. وتنطبق هذه الخدمات على كيانات الاتصال في الأنظمة كما تنطبق على البيانات المتبادلة فيما بينها والبيانات التي تديرها.

يقدم المنظور الإجمالي لهيكل الأمن (توصية قطاع تقييس الاتصالات X.810) الهياكل الأخرى ويصف مفاهيم مشتركة تشمل ميادين الأمن وسلطات الأمن وسياسات الأمن المستخدمة في جميع الهياكل. كما يصف نسق بيانات عموماً يمكن استعماله لنقل كل من معلومات الاستيقان ومعلومات التحكم في النفاذ نقلاً آمناً.

الاستيقان هو توفير الضمان لصحة هوية الكيان الذي يدّعيها. ولا تقتصر الكيانات على المستعملين البشر وإنما تشمل الأجهزة والخدمات والتطبيقات. ويوفر الاستيقان أيضاً الضمان بأن أي كيان لا يحاول التنكر في هيئة اتصال سابقة أو في هيئة استعادة تسجيل غير مرخص به لاتصال سابق. وتتحدث توصية قطاع تقييس الاتصالات X.800 عن شكلين من أشكال الاستيقان: *الاستيقان من أصل البيانات* (أي البرهان على أن مصدر البيانات المتلقاة هو المصدر المزعوم) *والاستيقان من الكيان الند* (أي البرهان على أن الكيان الند في ترابط ما هو الكيان المزعوم). ويعرّف هيكل الاستيقان (توصية قطاع تقييس الاتصالات X.811) مفاهيم الاستيقان الأساسية؛ ويحدد الأصناف الممكنة من آليات الاستيقان؛ ويحدد الخدمات من أجل هذه الأصناف من الآليات؛ ويحدد المتطلبات الوظيفية للبروتوكولات التي تدعم أصناف الآليات هذه؛ ويحدد متطلبات الإدارة عموماً من أجل الاستيقان.

والتحكم في النفاذ هو الحيلولة دون استعمال غير مرخص به لمورد ما، بما في ذلك الحيلولة دون استعمال مورد ما على نحو غير مرخص به. ويضمن التحكم في النفاذ (توصية قطاع تقييس الاتصالات X.812) أن الأفراد المرخص لهم أو الأجهزة المرخص لها فقط يمكنهم ويمكنها النفاذ إلى عناصر الشبكة والمعلومات المخزنة وتدفقات المعلومات والخدمات والتطبيقات. ويصف هيكل التحكم في النفاذ نموذجاً يشكل كل جوانب النفاذ في الأنظمة المفتوحة، والعلاقة بوظائف الأمن الأخرى (مثل الاستيقان والتحقق)، ومتطلبات الإدارة من أجل التحكم في النفاذ.

وعدم التنصل هو القدرة على الحيلولة دون إنكار كيانات ما لاحقاً أنها قامت بأداء إجراء ما. ويعنى مفهوم عدم التنصل بإقامة الدليل الذي يمكن استخدامه لاحقاً لدحض أي مزاعم كاذبة. وتصف التوصية X.800 شكلين من أشكال خدمة عدم التنصل، ألا وهما *عدم التنصل مع برهان التسليم*، ويُستعمل لدحض إنكار كاذب من قبل كيان مقصود يدّعي أنه لم يتلق البيانات، و*عدم التنصل مع برهان المصدر*، ويُستعمل لدحض إنكار كاذب من قبل كيان مصدر يدّعي أنه لم يرسل البيانات. ولكن من الممكن، بصفة أعم، تطبيق مفهوم عدم التنصل على سياقات مختلفة عديدة بما في ذلك عدم التنصل من استحداث بيانات أو تقديمها أو تخزينها أو إرسالها أو تسلّمها. ومن شأن هيكل عدم التنصل (توصية قطاع تقييس الاتصالات X.813) أن يوسع مفاهيم عدم التنصل من خدمات الأمن كما هي موصوفة في توصية قطاع تقييس

الاتصالات X.800 وأن يوفر إطاراً لتطوير هذه الخدمات. كما أنه يحدد آليات ممكنة لتوفير هذه الخدمات ومتطلبات الإدارة عموماً فيما يتعلق بعدم التنصل.

والسرية هي خاصية عدم إتاحة المعلومات أو الكشف عنها لأفراد أو كيانات أو عمليات غير مرخص لهم أو لها بذلك. والغرض من خدمة السرية هو حماية المعلومات من الكشف عنها لمن لا يُرخص له بذلك. ويتناول *هيكل السرية* (توصية قطاع تقييس الاتصالات X.814) مسألة سرّية المعلومات من حيث الاستيفاء والنقل والإدارة وذلك بتعريف المفاهيم الأساسية للسرية والأصناف الممكنة من السرية والمرافق المطلوبة لكل صنف من آليات السرية. وهو يحدد أيضاً خدمات الإدارة والخدمات الداعمة المطلوبة، ومسألة التفاعل مع خدمات وآليات الأمن الأخرى.

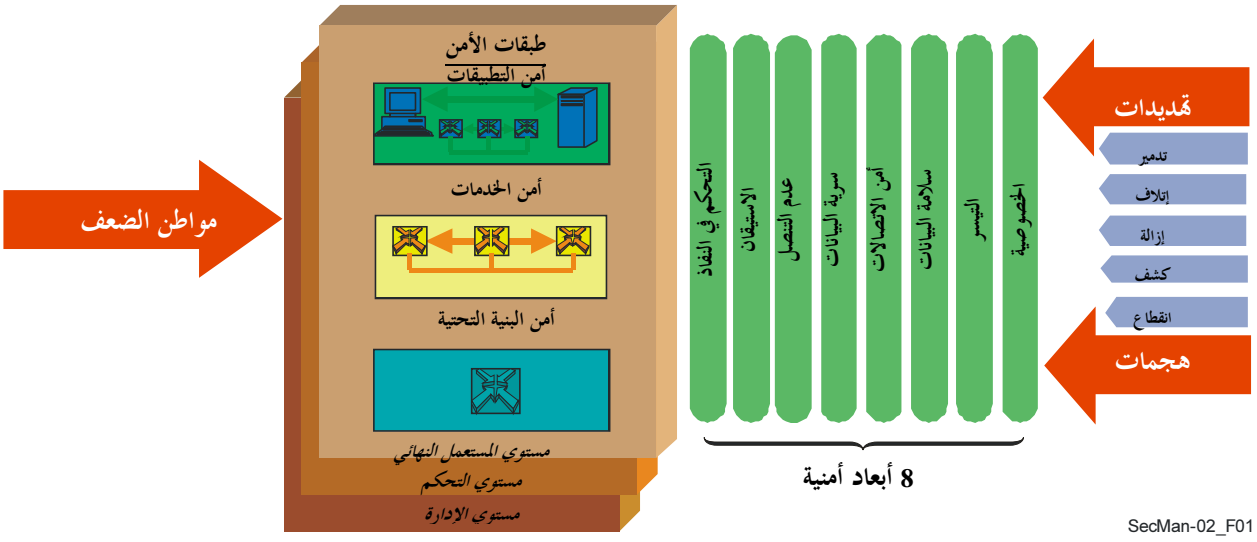
سلامة البيانات هي الخاصية التي تفيد بأن البيانات لم تخضع لأي تغيير على نحو غير مرخص به. وبصفة عامة، تتناول خدمة السلامة الحاجة إلى ضمان عدم تحريف البيانات أو إذا حدث أن حرّفت أن يكون المستعمل على علم بذلك. ويتناول *هيكل السلامة* (توصية قطاع تقييس الاتصالات X.815) سلامة البيانات لدى استخراج المعلومات ونقلها وإدارتها. وهو يحدد المفاهيم الأساسية للسلامة ويحدد الأصناف الممكنة لآلية السلامة ومرافقها، ومتطلبات الإدارة والخدمات ذات الصلة اللازمة لدعم صنف الآلية. (علماً بأن جوانب أخرى من السلامة، مثل سلامة النظام، هي أيضاً مهمة للأمن؛ رغم تركيز معايير معمارية الأمن على سلامة البيانات في المقام الأول).

3.4 معمارية الأمن للأنظمة التي توفر الاتصالات من طرف إلى طرف

في عام 2003، وبعد النظر ملياً في معمارية الأمن للشبكات، تمت الموافقة على توصية قطاع تقييس الاتصالات X.805 بشأن *معمارية الأمن للأنظمة التي توفر الاتصالات من طرف إلى طرف*. وهذه المعمارية التي تبني على، وتوسع، مفاهيم توصية قطاع تقييس الاتصالات X.800 والهياكل الأمنية التي ورد بحثها أعلاه، يمكن تطبيقها على مختلف أنواع الشبكات وهي حيادية من حيث التكنولوجيا المستعملة.

1.3.4 عناصر معمارية الأمن في توصية قطاع تقييس الاتصالات X.805

تعرّف معمارية توصية قطاع تقييس الاتصالات X.805 على أساس ثلاثة مفاهيم رئيسية، هي طبقات الأمن ومستوياته وأبعاده لشبكة من طرف إلى طرف. ويُعتمد في ذلك منهج تراتبـــي في تقسيم متطلبات الأمن عبر الطبقات والمستويات حتى يمكن تحقيق الأمن من طرف إلى طرف بتصميم إجراءات أمنية في كل بعد من الأبعاد لمواجهة تهديدات محددة. ويبيّن الشكل 1 عناصر هذه المعمارية.



الشكل 1 – عناصر معمارية الأمن في توصية قطاع تقييس الاتصالات X.805

البُعد الأمني في توصية قطاع تقييس الاتصالات X.805 هو مجموعة من التدابير الأمنية الرامية إلى معالجة جانب معين من أمن الشبكات. وتطابق وظائف خدمات الأمن الأساسية في توصية قطاع تقييس الاتصالات X.800 (*التحكم في النفاذ*، *والاستيقان*، *وسرية البيانات*، *وسلامة البيانات*، *وعدم التنصل*) وظائف أبعاد الأمن المقابلة في توصية قطاع تقييس الاتصالات X.805 (المرسومة في الشكل 1). وعلاوة على ذلك، تطرح توصية قطاع تقييس الاتصالات X.805 ثلاثة أبعاد (*أمن الاتصال والتيسر والخصوصية*) لا ترد في توصية قطاع تقييس الاتصالات X.800. وتوفر هذه الأبعاد حماية إضافية للشبكة ضد جميع التهديدات الأمنية الكبرى. ولا تقتصر هذه الأبعاد على الشبكة، بل تمتد أيضاً إلى التطبيقات ومعلومات المستعمل النهائي. وتنطبق الأبعاد الأمنية على مقدمي الخدمات أو الشركات التي تقدم خدمات الأمن لعملائها.

أما أبعاد الأمن الثمانية في توصية قطاع تقييس الاتصالات X.805 فهي كما يلي:

- *بُعد التحكم في النفاذ* الذي يحمي من استخدام موارد الشبكة دون ترخيص. ويضمن التحكم في النفاذ أن يقتصر النفاذ إلى عناصر الشبكة والمعلومات المخزنة وتدفقات المعلومات والخدمات والتطبيقات على الأشخاص أو الأجهزة المرخص لهم أو لها بذلك؛
- *بُعد الاستيقان* الذي يؤكد صحة هويات الكيانات لدى الاتصال. ويضمن الاستيقان صلاحية الهويات التي تدعيها الكيانات المشاركة في الاتصال (كالأشخاص أو الأجهزة أو الخدمات أو التطبيقات) ويوفر الضمان بأن أي كيان لا يحاول التنكر في هيئة اتصال سابق أو في هيئة استعادة تسجيل غير مرخص له لاتصال سابق؛
- *بُعد عدم التنصل* الذي يوفر سبل الحيلولة دون إنكار فرد أو كيان أنه قام بأداء إجراء ما يتعلق بالبيانات وذلك بإتاحة البرهان عن مختلف الإجراءات المتصلة بالشبكة (من قبيل البرهان على الالتزام أو القصد أو الواجب، والبرهان على منشأ البيانات، والبرهان على الملكية، والبرهان على استعمال المورد). وهو يضمن تيسر الإثبات الذي يمكن تقديمه إلى طرف ثالث واستخدامه برهاناً على أن حدثاً ما، أو إجراءً ما قد حدث فعلاً؛
- *بُعد سرية البيانات* الذي يحمي البيانات من الكشف عنها لمن لا يرخص له بذلك. وتضمن سرية البيانات أن محتوى البيانات لا تستطيع أن تفهمه كيانات غير مرخص لها بذلك؛
- *بُعد أمن الاتصال* الذي يضمن أن المعلومات تتدفق حصراً بين النقاط الطرفية المرخص لها بذلك، أي أن المعلومات لا تحوَّل أو تُعترض عندما تتدفق بين هذه النقاط؛
- *بُعد سلامة البيانات* الذي يضمن أن البيانات محمية من أي تعديل أو حذف أو استحداث أو استنساخ غير مرخص، ويوفر إنذاراً في حال قيام أنشطة يمكن أن تنال من سلامة البيانات؛
- *بُعد التيسر* الذي يضمن عدم رفض النفاذ المصرح به إلى عناصر الشبكة والمعلومات المخزنة وتدفق المعلومات والخدمات والتطبيقات نتيجة أحداث تؤثر على الشبكة؛
- *بُعد الخصوصية* يؤمن حماية المعلومات التي يمكن أن تُستخلص من مراقبة أنشطة الشبكة. ومن أمثلة هذه المعلومات مواقع شبكة الويب التي يكون قد زارها المستعمل، والموقع الجغرافي للمستعمل، وعناوين بروتوكول الإنترنت وأسماء ميادين الأجهزة في شبكة مقدم خدمات ما.

كما هو مبين في الشكل رقم 1، بالإضافة إلى الأبعاد الأمنية، تحدد توصية قطاع تقييس الاتصالات X.805 ثلاث طبقات أمن وثلاثة مستويات. ولتوفير حل أمني من طرف إلى طرف، يجب أن تطبق الأبعاد الأمنية على تراتبية معدات الشبكة وعلى تجميعات المنشأة، وهو ما يشار إليه *بالطبقات الأمنية*. ويمثل *المستوى الأمني* نمطاً معيناً من نشاط الشبكة يحظى بحماية الأبعاد الأمنية. ويمثل كل مستوى أمني نمطاً محمياً من نشاط الشبكة.

وتتناول طبقات الأمن المتطلبات السارية على عناصر وأنظمة الشبكة وعلى الخدمات والتطبيقات المرتبطة بتلك العناصر. ومن بين مزايا تحديد الطبقات أنه يسمح بإعادة الاستخدام عبر تطبيقات مختلفة عند توفير الأمن من طرف إلى طرف. وتختلف جوانب الضعف في كل طبقة، وبالتالي يجب تحديد تدابير التغلب عليها لتلبية حاجات كل طبقة.

أما الطبقات الثلاث فهي:

- *طبقة البنية التحتية* التي تتألف من مرافق الإرسال في الشبكة وكذلك من العناصر المنفردة للشبكة. ومن أمثلة العناصر التي تتكون منها طبقة البنية التحتية أجهزة التسيير والبدالات والمخدمات ووصلات الاتصال فيما بينها.
- طبقة *الخدمات* التي تتناول أمن خدمات الشبكة المقدَّمة إلى الزبائن. وتتراوح هذه الخدمات بين عروض التوصيلية الأساسية مثل خدمات الخطوط المؤجرة وخدمات القيمة المضافة مثل التبادل الفوري للرسائل.
- طبقة *التطبيقات* التي تتناول متطلبات التطبيقات القائمة على الشبكة التي يستخدمها الزبائن. وقد تكون هذه التطبيقات بسيطة مثل البريد الإلكتروني أو متطورة مثل التطبيقات المرئية المتآزرة التي تستخدم فيها تقنيات النقل بالفيديو عالي الوضوح في استكشاف النفط أو تصميم السيارات.

وتتناول مستويات الأمن حاجات الأمن المحددة المرتبطة بأنشطة إدارة الشبكة، أو التحكم في الشبكة أو أنشطة التشوير، وأنشطة المستعمل النهائي. وينبغي تصميم الشبكات بحيث تُعزل الأحداث الأمنية في مستوٍ أمني ما عن المستويات الأمنية الأخرى.

أما المستويات الأمنية فهي:

- مستوي *الإدارة* الذي يتعلق بأنشطة العمليات والإدارة والصيانة وتوفير الخدمات مثل توفير الخدمات اللازمة لمستعمل أو لشبكة.
- مستوي *التحكم* الذي يرتبط بجوانب التشوير لإقامة (وتعديل) الاتصالات من طرف إلى طرف عبر الشبكة، بغض النظر عن الوسط أو التكنولوجيا المستخدمة في الشبكة.
- مستوي *المستعمل النهائي* الذي يتناول أمن النفاذ واستعمال المشتركين للشبكة، وكذلك حماية تدفق بيانات المستعمِل النهائي.

ويمكن استعمال معمارية توصية قطاع تقييس الاتصالات X.805 لتوجيه وضع سياسة أمن ومعماريات التكنولوجيا وخطط الاستجابة لأي حادث والتعافي منه.

كما يمكن استعمال المعمارية أساساً لتقييم الأمن. وحالما ينشر برنامج أمن ما يتعين صيانته لكي يبقى صالحاً في بيئة تهديدات ما فتئت تتغير. وبإمكان معمارية أمن X.805 أن تساعد في صيانة برنامج الأمن بالحرص على أن التعديلات التي تطرأ عليه تتناول أبعاد الأمن المرعية في كل طبقة ومستوي من طبقات ومستويات الأمن.

ورغم أن توصية قطاع تقييس الاتصالات X.805 هي معمارية أمن الشبكة، يمكن لبعض المفاهيم أن تشمل أجهزة المستعمل النهائي. وتتناول توصية قطاع تقييس الاتصالات X.1031 هذا الموضوع، أي *أدوار المستعملين النهائيين وشبكات الاتصالات ضمن معمارية الأمن*.

2.3.4 تيسّر الشبكة ومكوناتها

يُعد تيسّر الشبكة جانباً مهماً من أمن تكنولوجيا المعلومات والاتصالات. وكما ذُكر أعلاه، فإن الغرض من البعد الأمني *للتيسّر* في توصية قطاع تقييس الاتصالات X.805 هو ضمان استمرارية الخدمة والنفاذ المخوَّل إلى عناصر الشبكة ومعلوماتها وتطبيقاتها. وتُدرج في هذا البعد أيضاً حلول التعافي من الكوارث.

وتتألف طبقة أمن البنية التحتية من مرافق الإرسال في الشبكة فضلاً عن عناصر الشبكة الفردية المحمية بالأبعاد الأمنية. وتمثل طبقة البنية التحتية اللبنات الأساسية لبناء الشبكات والخدمات والتطبيقات. ومن أمثلة المكونات التي تنتمي إلى طبقة البنية التحتية، المسيرات والمبدلات والمخدمات، فضلاً عن وصلات الاتصال فيما بينها.

وتتعدد وتتنوع المتطلبات الوظيفية والتنفيذية والتشغيلية للحد من المخاطر والعواقب المترتبة على عدم تيسّر موارد الشبكة. وإذ تكثر العوامل التي يتعين النظر فيها، فهي تشمل أداء الأخطاء والتحكم في الازدحام والتبليغ عن الأعطال واتخاذ الإجراءات التصحيحية. أما توصية قطاع تقييس الاتصالات G.827 بشأن *أداء التيسّر ومعلماته وأهدافه على المسيرات الرقمية الدولية ذات معدل البتات الثابت من طرف إلى طرف*، فهي تعرّف معلمات أداء الشبكة وأهدافه لعناصر المسير وتيسر المسيرات الرقمية الدولية ذات معدل البتات الثابت من طرف إلى طرف. ولا ترتبط هذه المعلمات بنمط الشبكة المادية الداعمة للمسير من طرف إلى طرف. ويقدم الملحق ألف بتوصية قطاع تقييس الاتصالات G.827 توجيهات مفصلة بشأن منهجيات تقييم التيسر من طرف إلى طرف، ويورد أمثلة على طبولوجيات المسير وحسابات تيسر المسير من طرف إلى طرف. ومن التوصيات الأخرى التي تتناول أداء الشبكة: توصية قطاع تقييس الاتصالات G.1000 بعنوان *نوعية خدمة الاتصالات: إطار وتعاريف*؛ وتوصية قطاع تقييس الاتصالات G.1030 بعنوان *تقدير الأداء من طرف إلى طرف في شبكات بروتوكول الإنترنت لتطبيقات البيانات*؛ وتوصية قطاع تقييس الاتصالات G.1050 بعنوان *نموذج شبكة لتقييم أداء الإرسال المتعدد الوسائط باستعمال بروتوكول الإنترنت*؛ وتوصية قطاع تقييس الاتصالات G.1081 بعنوان *نقاط مراقبة نوعية أداء تلفزيون بروتوكول الإنترنت*.

4.4 توجيهات التنفيذ

تشكل معايير معمارية الأمن لقطاع تقييس الاتصالات بمجملها جزءاً من توصيات الأمن في سلسلة توصيات قطاع تقييس الاتصالات X.849-X.800. وترد توجيهات التنفيذ في إضافة لهذه السلسلة من التوصيات (X الإضافة 3، سلسلة توصيات قطاع تقييس الاتصالات X.849-X.800 – *إضافة بشأن المبادئ التوجيهية لتنفيذ النظام وأمن الشبكة*). وتوفر هذه الإضافة مبادئ توجيهية بشأن الأنشطة الحرجة خلال دورة حياة أمن الشبكة. وتتناول هذه المبادئ التوجيهية أربعة مجالات هي: سياسة الأمن التقنية؛ وتحديد تراتبية الأصول؛ والتهديدات ومواطن الضعف والتخفيف منها على أساس تراتبية الأصول. تهدف هذه المبادئ التوجيهية وما يرتبط بها من قوالب جاهزة إلى تمكين التنفيذ المنهجي لتخطيط أمن الشبكة وتحليله وتقييمه.

5.4 بعض المعماريات الخاصة بتطبيقات محددة

يعرّف هذا القسم جوانب من بعض المعماريات المتعلقة بتطبيقات محددة.

1.5.4 الاتصالات من الند إلى الند

تجسّد الاتصالات من الند إلى الند (P2P) مثالاً ملموساً على معماريات الشبكة التي يتساوى فيها جميع الأنداد في الصلاحيات والمسؤوليات، على النقيض من نموذج الزبون/المخدّم. ففي حالة الاتصالات من الند إلى الند، يمكن لند أن يكون المخدّم والزبون في آن معاً. وعند تبادل البيانات أو الرسائل في شبكة الند إلى الند، يمكن لند أن يتواصل مع غيره من الأنداد مباشرةً. وبما أن الحركة والمعالجة موزعتان على كل ند من الأنداد، لا تتطلب شبكة الند إلى الند قدرة حوسبة عالية الأداء أو شبكة عريضة النطاق.

فشبكة الند إلى الند إنما هي شبكة تراكب على شبكة الاتصالات والإنترنت. فهي تستفيد من تنوع التوصيلية بين العقد ومن قدرة الحوسبة والتخزين المتاحة في كل عقدة، بدلاً من الموارد المركزية التقليدية.

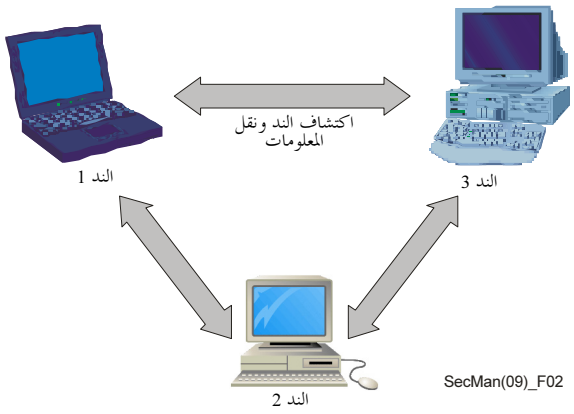
ومع سرعة التقدم في شبكات الاتصالات وتكنولوجيا الحوسبة، يمكن أن يتوفر في العقد الموزعة قدر أكبر بكثير من المعلومات وموارد الحوسبة مما هو متاح في عدد محدود من المخدمات المركزية.

وتُستعمل شبكات الند إلى الند عادةً لتوصيل العقد عبر توصيلات مخصصة. ويستفاد من مثل هذه الشبكات لأغراض عديدة. فيشيع كثيراً التشارك في ملفات البيانات الحاوية على بيانات سمعية أو فيديوية أو نصية أو على أي شيء بنسق رقمي. كما تستفيد بيانات الاتصالات في الوقت الفعلي، من قبيل حركة المهاتفة، من تكنولوجيا الاتصالات من الند إلى الند.

1.1.5.4 معمارية الأمن في شبكات الند إلى الند والتشغيلات في هذه الشبكات

يرد في توصية قطاع تقييس الاتصالات X.1162 وصف لنموذج معماري عام يتعلق بالأمن يمكن تطبيقه في مختلف شبكات الند إلى الند.

ويبين الشكل 2 المعمارية الأساسية للخدمة من الند إلى الند. ويجري تبادل المعلومات التي يعالجها كل ند مباشرة بين المستعملين. ونظراً لغياب مخدم مركزي يخزن المعلومات، يحتاج كل ند للعثور على الأنداد ممن بحوزتهم البيانات المستهدفة قبل أن يتمكن من استخراجها. أضف إلى ذلك أن كل ند يجب أن يسمح بنفاذ الأنداد الآخرين إليه ليتاح تبادل البيانات.

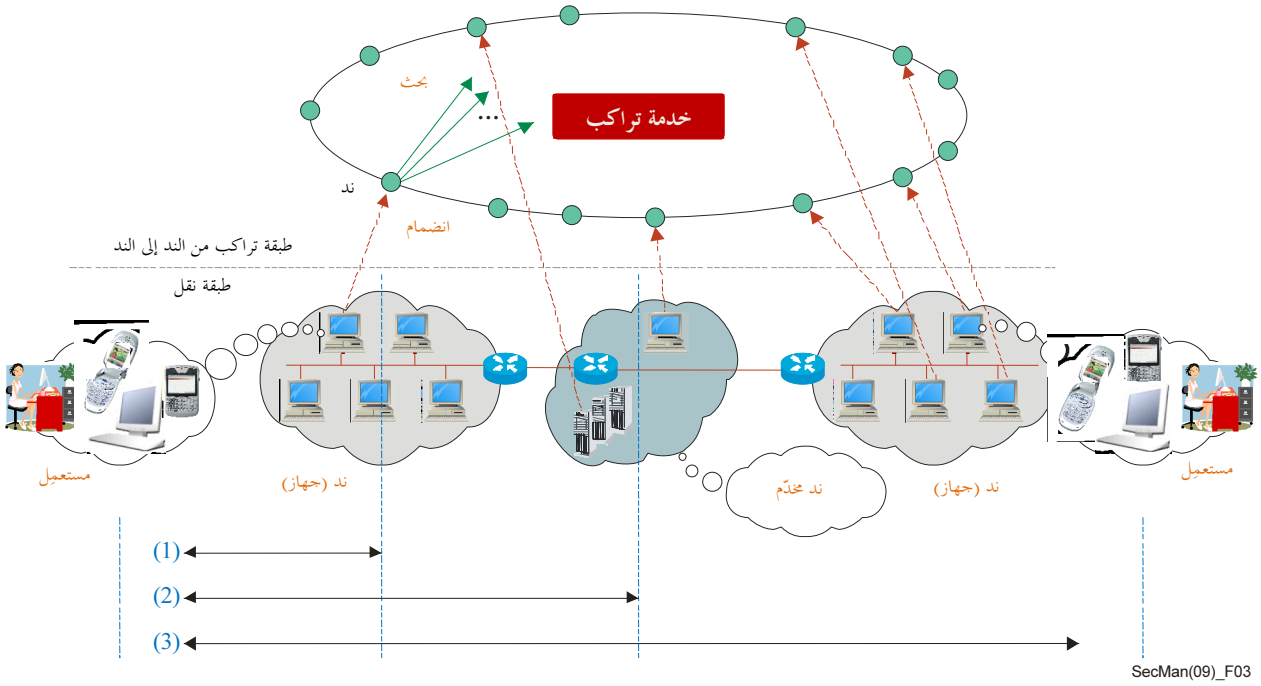


الشكل 2 – معمارية الخدمة من الند إلى الند

ويبين الشكل 3 المعمارية المادية والمنطقية لشبكة الند إلى الند. ففي الشبكة المادية من الند إلى الند، يمكن لمستعمل أن ينضم إلى خدمات الند إلى الند عن طريق جهاز. ويُستعمل مصطلح "الند" عموماً لتمثيل مستعمل أو جهاز يملكه المستعمل. ويمكن تصنيف أنماط التوصيل بين الكيانات في شبكة الند إلى الند على النحو التالي:

- التوصيل مع ند داخل الميدان؛
- التوصيل مع ند بين الميادين؛
- التوصيل مع ند مقدم خدمة يقع في ميدان شبكة أخرى.

ويبين الشكل 3 أيضاً المعمارية المنطقية لشبكة الند إلى الند باعتبارها شبكة افتراضية عبر طبقة النقل. ويُفترض ألا يُحدَّ تشغيل كل ند بمعمارية الشبكة المادية، وأن يتمكن الند من الاتصال بأي ند آخر بغض النظر عن موقعه (من خلال مساعدة ند فائق، إذا اقتضى الأمر). وتنقسم بنية شبكة الند إلى الند إلى طبقتين: طبقة تراكب الند إلى الند وطبقة النقل التي تتولى مسؤولية نقل الرزم من/إلى الطبقة العليا، فيما تتولى طبقة التراكب مسؤولية تقديم خدمات الند إلى الند.



الشكل 3 – نموذج المرجع المعماري لشبكة الند إلى الند

2.1.5.4 هيكل الاتصالات الآمنة من الند إلى الند

في توصية قطاع تقييس الاتصالات X.1161 بعنوان: *"إطار لاتصالات آمنة من ند إلى ند"*، توصَّف متطلبات الأمن لشبكات الند إلى الند مع الخدمات والآليات اللازمة لتلبية هذه المتطلبات.

وتشمل التهديدات التي تتعرض لها الاتصالات من الند إلى الند، التنصت والتشويش والدس والتعديل والنفاذ غير المرخص وهجمات طرف متوسط بين طرفين والهجمات بهويات مزورة. وترد في الجدول 3 التدابير المضادة للتهديدات التي تتعرض لها شبكات الند إلى الند.

الجدول 3 – العلاقة بين متطلبات الأمن لشبكات الند إلى الند والتدابير المضادة

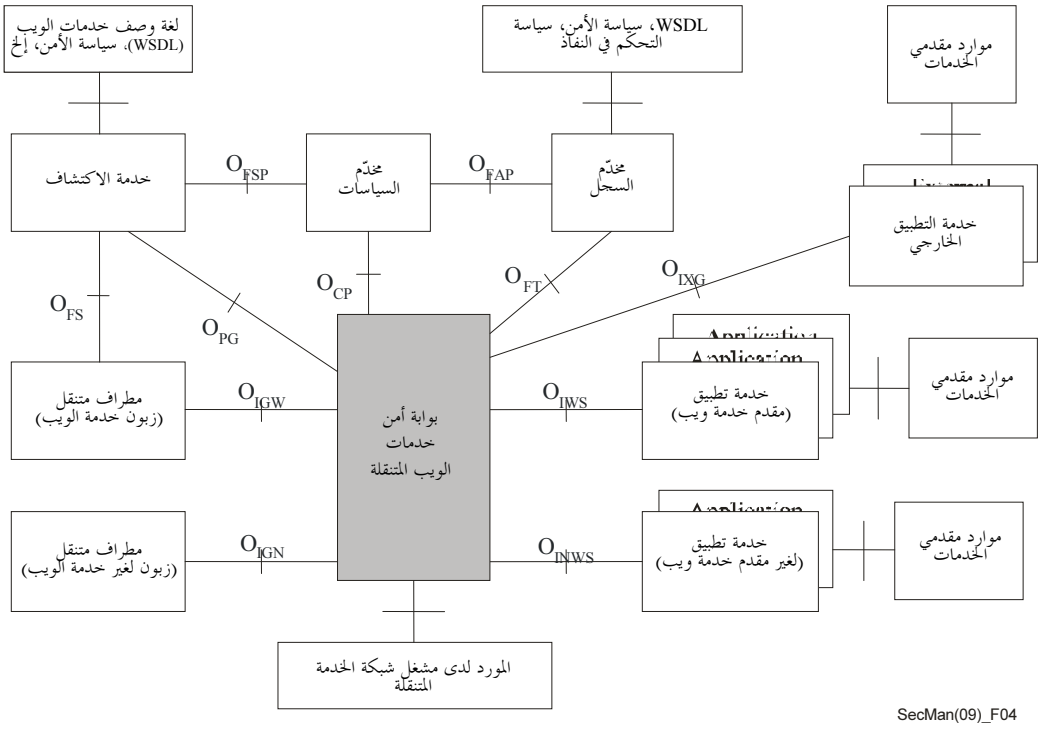
الوظائف / المتطلبات	التحفير	تبادل المفاتيح	التوقيع الرقمي	إدارة الثقة	التحكم في النفاذ	آلية سلامة البيانات	تبادل الاستيقان	التوثيق	التسيير الآمن	آلية التحكم في الحركة	تخصيص الهوية
الاستيقان من المستعمل	X	X	X	X	X		X				X
الإغفال	X			X							X
الخصوصية	X				X		X				
سلامة البيانات	X	X	X		X	X	X				
سرية البيانات	X	X			X		X				
التحكم في النفاذ					X		X				X
عدم التنصل			X				X	X			X
إمكانية الاستعمال					X						
التيسّر					X		X		X	X	
إمكانية التتبع			X						X		X
التحكم في الحركة		X								X	

2.5.4 معمارية الأمن لأمن الرسائل في خدمات الويب المتنقلة

في توصية قطاع تقييس الاتصالات X.1143 بعنوان: *معمارية الأمن لأمن الرسالة في خدمات الويب المتنقلة*، يرد وصف لمعمارية الأمن وسيناريوهاته لأمن الرسائل في خدمات الويب المتنقلة. ويوفر هذا المعيار ما يلي:

- معمارية الأمن لأمن الرسائل تعتمد على آليات مناسبة لسياسات خدمة الويب؛
- آليات عمل بيني وسيناريوهات خدمة بين التطبيقات تدعم كامل أكداس بروتوكول أمن خدمات الويب والتطبيقات التقليدية التي لا تدعم الكدسة الكاملة لبروتوكول أمن خدمات الويب؛
- آليات الاستيقان من الرسائل وسلامتها وسريتها؛
- آلية ترشيح رسائل تقوم على محتويات الرسالة؛
- معمارية مرجعية لأمن الرسائل وسيناريوهات خدمة الأمن.

ويبين الشكل 4 معمارية الأمن في خدمات الويب المتنقلة.



الشكل 4 – معمارية الأمن في خدمات الويب المتنقلة

تتألف معمارية الأمن من المكونات التالية:

- مطاريف الخدمة المتنقلة الخاصة، وهي بمثابة زبائن خدمات الويب المتنقلة؛
- بوابة الأمن لخدمات الويب المتنقلة (MWSSG). وتُرسل جميع الطلبات من زبائن الخدمة المتنقلة إلى هذه البوابة مما يفرض أيضاً التحكم في النفاذ؛
- مخدّم السياسات الذي يدير سياسات الأمن المتصلة بالمعالجة الآمنة للرسائل وسياسات التحكم في النفاذ للرسائل؛
- خدمة التطبيقات التي توفر مختلف الخدمات ذات القيمة المضافة إلى الزبائن؛
- خدمة الاكتشاف التي تخزن معلومات السطح البيني لخدمات التطبيقات وما يتصل بها من سياسات أمن كي ينفذ الزبائن إلى خدمات التطبيقات؛
- مخدِّم السجل الكائن في الميدان الداخلي لمشغّل الخدمة المتنقلة والذي يدير معلومات السطح البيني لخدمات التطبيقات وما يتصل بها من سياسات أمن كي ينفذ الزبائن إلى خدمات التطبيقات وإلى سياسات التحكم بالنفاذ المتصلة بالخدمات المستهدفة.

6.4 المعماريات والنماذج الأخرى لأمن الشبكة

تغطى جوانب إضافية من معماريات أمن الشبكة لاحقاً في هذا النص. ويرجى على وجه الخصوص مراجعة الفقرات 2.7 معمارية إدارة الشبكة و1.8 أمن شبكة الجيل التالي و1.4.8 معمارية الاتصالات الكبلية بواسطة بروتوكول الإنترنت (IPCablecom) و1.5.8 معمارية الاتصالات الكبلية بواسطة بروتوكول الإنترنت 2 (IPCablecom2) و2.9 التلفزيون القائم على بروتوكول الإنترنت (IPTV).

5. جوانب إدارة الأمن

5 جوانب إدارة الأمن

يتسع موضوع إدارة الأمن ليشمل العديد من الأنشطة المرتبطة بالتحكم في النفاذ إلى النظام وموارد الشبكة، وبحماية هذا النفاذ، وبمراقبة الحدث والتبليغ والسياسات والتحقق، فضلاً عن إدارة المعلومات المتعلقة بهذه المهام والأنشطة. ويتناول هذا القسم بعضاً من الأنشطة العامة بإدارة الأمن، وهي أنشطة ترتبط بتأمين البنية التحتية للشبكة، ويرد بحثها في القسم 7.

1.5 إدارة أمن المعلومات

تساهم المعلومات، شأنها شأن الأصول الأخرى، مساهمة أساسية في أعمال المنظمة. ويمكن طباعة المعلومات وتخزينها إلكترونياً ونقلها عن طريق البريد وتداولها إلكترونياً وعرضها على فيلم والتكلم بها في معرض الحديث أو نقلها بسبل أخرى. وأياً ما كان شكل المعلومات أو وظيفتها، وأياً ما كانت وسيلة تداولها أو تخزينها، ينبغي أن تحمى المعلومات دوماً حماية مناسبة.

وما أن يُنتهك أمن المعلومات، مثلاً بالنفاذ غير المصرح به إلى نظام معالجة معلومات منظمة ما، فقد يلحق بتلك المنظمة ضرر كبير. ولذلك لا بد للمنظمات من أن تضمن أمن معلوماتها من خلال تنفيذ عملية مهيكلة لإدارة الأمن.

وتتحقق الإدارة الفعالة لأمن المعلومات من خلال تنفيذ مجموعة مناسبة من الضوابط تسري على مرافق الاتصالات وخدماتها وتطبيقاتها. ويتعين وضع هذه الضوابط وتنفيذها ومراقبتها ومراجعتها وتحسينها باستمرار. إذ يمكن أن يؤدي التقاعس عن إنجاح نشر ضوابط أمنية فعالة إلى عجز المنظمة عن تحقيق أهدافها الأمنية والتجارية.

أما منظمات الاتصالات التي يستعمل مشتركون مرافقها لمعالجة معلومات قد تشمل البيانات الشخصية والبيانات السرية وبيانات الأعمال الحساسة، فهي تحتاج إلى ضمان مستوى مناسب من الحماية للحيلولة دون اختراق المعلومات، أي أنها تحتاج إلى إنشاء نظام فعال لإدارة معلومات الأمن (ISMS).

وأشهر مواصفة لنظام فعال لإدارة معلومات الأمن هي تلك المعرّفة في سلسلة معايير النظام الفعال لإدارة معلومات الأمن ISO/IEC 27000 التي تشمل معايير لأسس النظام الفعال لإدارة معلومات الأمن ومتطلباته ومدونة قواعد الممارسة وتوجيهات التنفيذ والمواضيع ذات الصلة. وقد وضع قطاع تقييس الاتصالات بالاشتراك مع المنظمة الدولية للتوحيد القياسي (ISO)/اللجنة الكهرتقنية الدولية (IEC) توصية قطاع تقييس الاتصالات المعيار ITU-T X.1051 | ISO/IEC 27011 بشأن *المبادئ التوجيهية لإدارة أمن المعلومات في منظمات الاتصالات*، استناداً إلى معيار ISO/IEC 27002 بشأن مدونة قواعد الممارسة في نظام فعال لإدارة معلومات الأمن (ISMS).

وتضع توصية قطاع تقييس الاتصالات X.1051 المبادئ التوجيهية والمبادئ العامة للشروع بإدارة أمن المعلومات في منظمات الاتصالات وتنفيذها وصيانتها وتحسينها، وتقدم الأساس المرجعي لتنفيذ إدارة أمن المعلومات بحيث تضمن السرية والنـــزاهة والتيسّر في مرافق الاتصالات وخدماتها. وترد توجيهات محددة لقطاع الاتصالات في المواضيع التالية:

- تنظيم أمن المعلومات؛
- إدارة الأصول؛
- أمن الموارد البشرية؛

- الأمن المادي والبيئي؛
- إدارة الاتصالات والتشغيلات؛
- التحكم في النفاذ؛
- حيازة أنظمة المعلومات؛
- التطوير والصيانة؛
- إدارة الحوادث؛
- إدارة استمرارية الأعمال.

وبالإضافة إلى تطبيق أهداف الأمن والضوابط المبينة في توصية قطاع تقييس الاتصالات X.1051، يجب أن تأخذ منظمات الاتصالات في الاعتبار أيضاً الشواغل الأمنية التالية على وجه التحديد:

- يجب حماية المعلومات المتصلة بمنظمات الاتصالات من الإفصاح غير المصرح به. ومفاد ذلك عدم الإفصاح عن المعلومات المتداولة من حيث وجودها ومحتواها ومصدرها ومقصدها وتاريخها ووقتها.
- ينبغي التحكم في تركيب مرافق الاتصالات وفي استعمالها ضماناً لصحة ودقة واكتمال المعلومات المرسلة والمنقولة والمتلقاة سلكياً أو لاسلكياً أو بأية طريقة أخرى؛
- لا بد من الحصول على تصريح لجميع أنواع النفاذ إلى معلومات الاتصالات ومرافقها ووسائط تقديم خدماتها، وينبغي ألا يُمنح هذا التصريح إلا عند الضرورة. وتوسعاً بأحكام التيسر، ينبغي لمنظمات الاتصالات أن تولي الأولوية للاتصالات الضرورية في الحالات الطارئة وأن تلتزم بالمتطلبات التنظيمية.

وتلزم إدارة أمن المعلومات في منظمات الاتصالات بغض النظر عن وسيلة الإرسال أو واسطته. فإن لم تنفَّذ إدارة أمن المعلومات على الوجه المناسب، ستزداد المخاطر المرتبطة باستخدام النظام.

وتقدم منظمات الاتصالات خدماتها من خلال العمل كوسيط في نقل بيانات المستعملين: منظمات وأفراد. ولذلك، ينبغي أن يؤخذ في الحسبان أن النفاذ إلى مرافق معالجة المعلومات واستخدامها داخل منظمة اتصالات ليس حكراً على موظفي المنظمة ومقاوليها، بل إن الأمر متاح أيضاً لمستعملين شتى من خارج المنظمة.

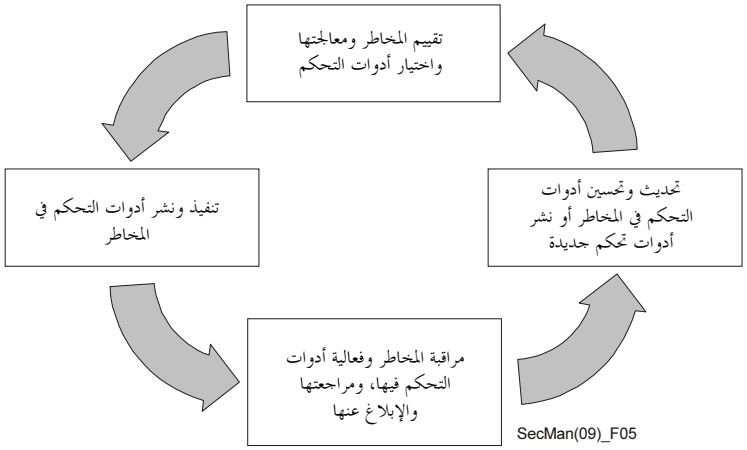
وإذ توضع في الاعتبار إمكانية التشارك و/أو التوصيل البيني مع مقدمي الخدمة الآخرين في خدمات الاتصالات ومرافقها، لا مناص من أن يمتد أمن المعلومات في منظمات الاتصالات ليشمل أياً من، وجميع، مجالات البنية التحتية للشبكة وتطبيقات الخدمات ومرافقها.

2.5 إدارة المخاطر

إدارة المخاطر هي عملية تقييم وقياس كمي للمخاطر واتخاذ للإجراءات اللازمة لضمان بقاء سائر المخاطر دون مستوىً مقبول محدد سلفاً. وقد جرى التطرق سريعاً إلى هذا الموضوع في القسم 3 في معرض بحث توصية قطاع تقييس الاتصالات X.1205 التي تقدم *لمحة عامة عن الأمن السيبراني*. وترد في توصية قطاع تقييس الاتصالات X.1055، بعنوان *المبادئ التوجيهية لإدارة المخاطر ومواصفاتها في منظمات الاتصالات*، مبادئ توجيهية أوفى بتفاصيلها لإدارة المخاطر. فهي تحدد العمليات والتقنيات الكفيلة بالحد من المخاطر المحيطة بأمن المعلومات. ويمكن استعمال هذه العمليات والتقنيات لتقييم المتطلبات الأمنية للاتصالات والمخاطر التي تتهددها، وللمساعدة في انتقاء الضوابط المناسبة للحفاظ على المستوى الأمني المطلوب وفي تنفيذها وتحديثها.

وقد وضعت العديد من المنهجيات المحددة لمعالجة إدارة المخاطر. وتوفر توصية قطاع تقييس الاتصالات X.1055 معايير لتقييم وانتقاء المنهجيات المناسبة في منظمة اتصالات. بيد أنها لا تقترح أي منهجية محددة لإدارة المخاطر.

وتُبيَّن عملية إدارة المخاطر في الشكل 5.



الشكل 5 – عملية إدارة المخاطر في توصية قطاع تقييس الاتصالات X.1055

وتُستعمل مواصفات المخاطر لتوجيه العملية الشاملة لإدارة المخاطر. فهي تُستعمل على وجه التحديد للمساعدة في عملية صنع القرار والمساعدة في إسناد أولويات للمخاطر من حيث حراجتها، فضلاً عن المساعدة في تحديد توزيع الموارد والتدابير المضادة. ويمكن أن تساعد أيضاً في وضع المقاييس المناسبة واستعمالها إلى جانب أدوات أخرى مثل منهجيات تحليل الثغرات. وتقدم توصية قطاع تقييس الاتصالات X.1055 توجيهات لوضع مواصفات المخاطر ويرد فيها قالب جاهز وبعض الأمثلة عن مواصفات المخاطر.

3.5 التعامل مع الحوادث

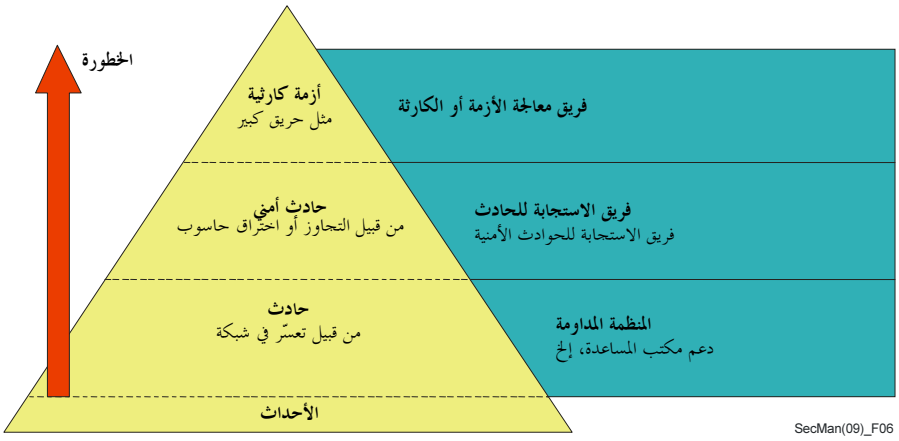
يعدّ الثبات في كشف معلومات بشأن حوادث ذات صلة بالأمن، وفي التجاوب مع هذه المعلومات ونشرها، من الأوجه المعتادة لإدارة الأمن. وما لم تقيَّم حوادث من هذا القبيل تقييماً صحيحاً ويُتعامل معها على النحو المناسب، ستكون المنظمات عرضة لهجمات لاحقة قد تزداد خطورتها.

وما لم يكن هناك إجراء متبع للتعامل مع حادث ذي صلة بالأمن لدى كشفه، يتعذر وضع تقرير أو تحليل للحادث بصورة صحيحة. ويتعذر أيضاً وجود إجراءات لرفع التقارير أو الحصول على مساعدة تقنية أو توجيه من الإدارة، رغم أن القضايا التي تثيرها مثل هذه الحوادث لها في كثير من الأحيان تداعيات تتجاوز بكثير تكنولوجيا المعلومات أو الربط الشبكي. فالحوادث على سبيل المثال قد تنطوي على مخاطر قانونية أو مالية أو مخاطر أخرى تنال من السمعة، أو قد تنطوي على أمور من اختصاص سلطات إنفاذ القانون. فغياب إجراءات التعامل مع الحوادث قد يكون مدعاةً "للارتجال" أو للالتفاف على المشكلة بدلاً من معالجتها وتوثيقها والإبلاغ عنها على الوجه الصحيح، وفي هذه الحالة تظل إمكانية وقوع مشاكل أخطر لاحقاً قائمة.

وإذ تتنبه المنظمات إلى الحاجة إلى إدارة أمنية متسقة وفعالة للشبكات والعمليات، تغدو معالجة الحوادث من الممارسات المعتادة. فيمكن لوحدة أو مجموعة مدربة تدريباً مناسباً أن تتولى أمر حوادث الأمن بصورة سريعة وصحيحة. وللنجاح في التعامل مع الحادث والإبلاغ عنه، لا بد من فهم كيفية الكشف عن الحوادث وإدارتها وحلها. فبوضع هيكل عام للتعامل مع الحوادث (أي الحوادث المادية أو الإدارية أو التنظيمية والمنطقية) يمكن رسم صورة عامة لهيكل الحادث وتوالي فصوله. فتوصية قطاع تقييس الاتصالات E.409،

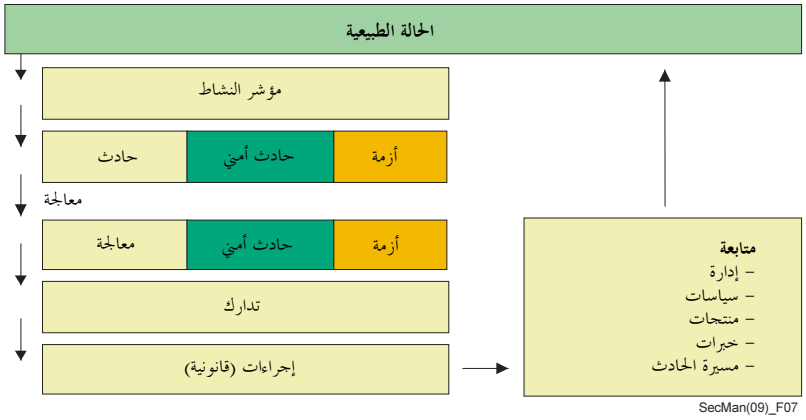
بعنوان *تنظيم الحوادث والتعامل مع الحوادث الأمنية: مبادئ توجيهية لمنظمات الاتصالات*، توفر نظرة عامة وإطاراً يعطي إرشادات بشأن التخطيط في منظمة لكشف الحوادث ذات الصلة بالأمن والتعامل معها. والتوصية عمومية في طابعها ولا تحدد أو تتناول متطلبات من أجل شبكات معينة.

ومن الضرورة بمكان توحيد المصطلحات عند الإبلاغ عن حادث أو التعامل معه. إذ يمكن لاستعمال مصطلحات مختلفة أن يؤدي إلى سوء تفاهم قد يفضي إلى وقوع حادث أمني لا يسترعي العناية المناسبة ولا التعامل السريع الواجب لاحتوائه والحؤول دون تكراره. ناهيك عن أن تعريف ما يعتبر حادثاً يمكن أن يختلف على اختلاف المهن والمنظمات والناس. وتسعى توصية قطاع تقييس الاتصالات E.409 إلى توحيد مصطلحات الكشف عن الحادث والإبلاغ عنه، وكذلك إلى تصنيف الحوادث وفقاً لدرجة خطورتها كما هو موضح في الشكل 6.



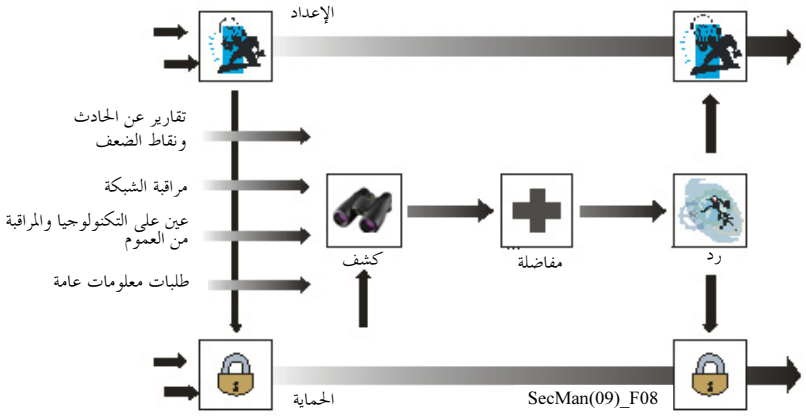
الشكل 6 – هرم الأحداث والحوادث في توصية قطاع تقييس الاتصالات E.409

كما تعرّف توصية قطاع تقييس الاتصالات E.409 هيكلاً للتعامل مع الحوادث (كما هو موضح في الشكل 7) وتحدد إجراءات لكشفها وتصنيفها وتقييمها والتعامل معها ومتابعتها.



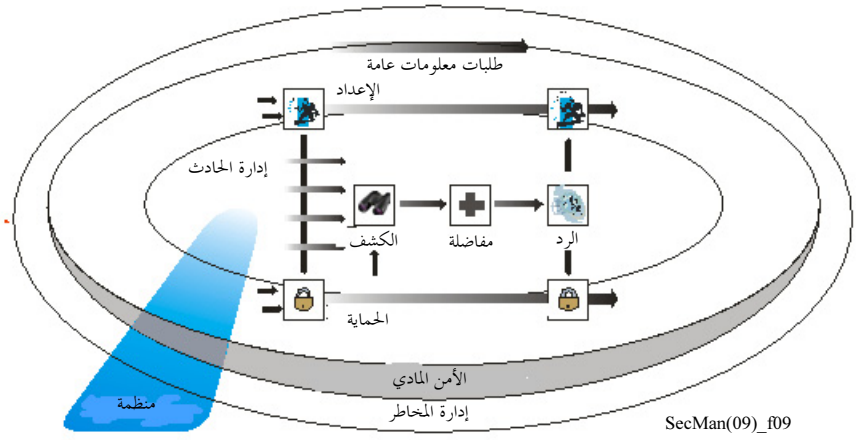
الشكل 7 – هيكل التعامل مع الحوادث في توصية قطاع تقييس الاتصالات E.409

أما توصية قطاع تقييس الاتصالات X.1056 التي تمت الموافقة عليها مؤخراً بعنوان *المبادئ التوجيهية لإدارة حوادث الأمن في منظمات الاتصالات*، فهي تؤسس على التوجيهات الواردة في توصية قطاع تقييس الاتصالات E.409. إذ تحتاج منظمات الاتصالات لعمليات جاهزة في متناولها للتعامل مع الحوادث ومنع تكرارها. ويرد في توصية قطاع تقييس الاتصالات X.1056 وصف لخمس عمليات رفيعة المستوى لإدارة الحوادث ولعلاقتها بإدارة الأمن، وهي مبيّنة في الشكلين 8 و9.



الشكل 8 – خمس عمليات رفيعة المستوى لإدارة الحوادث

(المصدر: لمحة عامة تنفيذية عن معايير SEI MOSAIC: التقرير التقني CMU/SEI-2004-TR-015 – تحديد عمليات إدارة الحوادث لأفرقة الاستجابة للحوادث الحاسوبية (CSIRTs): عمل جارٍ)



الشكل 9 – مقارنة بين إدارة الحوادث وإدارة الأمن

(المصدر: لمحة عامة تنفيذية عن معايير SEI MOSAIC: التقرير التقني CMU/SEI-2004-TR-015 – تحديد عمليات إدارة الحوادث لأفرقة الاستجابة للحوادث الحاسوبية (CSIRTs): عمل جارٍ)

وبالإضافة إلى ذلك، تحدد توصية قطاع تقييس الاتصالات X.1056 طائفة من الخدمات الارتكاسية والاستباقية وخدمات إدارة جودة الأمن التي يمكن لفريق إدارة الحوادث الأمنية أن يقدمها.

6. الدليل والاستيقان وإدارة الهوية

6 الدليل والاستيقان وإدارة الهوية

يُستعمل مصطلح الدليل عموماً للإشارة إلى مجموعة منظمة من المعلومات أو الملفات التي يمكن الاستعلام منها للحصول على معلومات محددة. وفي قطاع تقييس الاتصالات، وفي سياق الأمن وتقييس الاتصالات بصفة أعم، يشير مصطلح *دليل* إلى مكان محفوظات المعلومات القائمة على أساس سلسلة X.500 من توصيات قطاع تقييس الاتصالات التي وُضعت بالاشتراك مع المنظمة الدولية للتوحيد القياسي (ISO)/اللجنة الكهرتقنية الدولية (IEC). فيُعرَّف بالدليل في توصية قطاع تقييس الاتصالات X.500 بعنوان، *الدليل: نظرة عامة على المفاهيم والنماذج والخدمات*، ويُستفاض بشرحه في توصيات قطاع تقييس الاتصالات X.501 بعنوان، *الدليل: نماذج*، وX.509 بعنوان، *الدليل: الإطار العام لشهادات المفاتيح العمومية والنعوت*، وX.519 بعنوان، *الدليل: مواصفات البروتوكول*. وتوفر هذه التوصيات خدمات الدليل لتسهيل الاتصال وتبادل المعلومات بين الكيانات والناس والمطاريف وقوائم التوزيع وما إلى ذلك. وبالإضافة إلى خدمات الدليل التقليدية مثل التسمية وإقران اسم بعنوان والسماح بإقامة إسناد بين الأشياء وموقعها، يؤدي الدليل دوراً مهماً في دعم خدمات الأمن من خلال تعريف مستندات إثباتية للاستيقان والاحتفاظ بها في شكل شهادات الأمنية. وعلى وجه الخصوص، تغطي سلسلة X.500 من توصيات قطاع تقييس الاتصالات جانبين أمنين:

- حماية معلومات الدليل على النحو المحدد في توصيتي قطاع تقييس الاتصالات X.501 وX.509 أولاً؛
- المبادئ الأساسية للبنية التحتية للمفاتيح العمومية (PKI) والبنية التحتية لإدارة الامتيازات (PMI) على النحو المحدد في توصية قطاع تقييس الاتصالات X.509.

ويُستهل هذا القسم بمناقشة أهمية أمن الدليل نفسه والحاجة إلى حماية معلومات الدليل. ثم يُستعرض دور الدليل في دعم متانة الاستيقان والبنى التحتية للمفاتيح العمومية وإدارة الهوية والاستدلال الأحيائي عن بعد.

1.6 حماية معلومات الدليل

1.1.6 أهداف حماية الدليل

تظل حماية البيانات التي تُعتبر عاملاً رئيسياً في إدارة الهوية في محور أعمال الدليل دوماً. ولئن كانت حماية بيانات الدليل قضية خصوصية في المقام الأول (أي حماية ضد الإفصاح غير المصرح به عن المعلومات الشخصية الحساسة)، فهي تنطوي أيضاً على ضمان سلامة البيانات وحماية الأصول التي تمثلها البيانات.

ويحتفظ الدليل بمعلومات عن الكيانات قد تكون حساسة، وينبغي ألا يُكشف عنها إلا لمن يحق له *ويحتاج إلى الاطلاع عليها*.

وهناك ثلاثة جوانب حماية البيانات:

- الاستيقان من المستعمل الساعي للنفاذ إلى المعلومات؛
- التحكم في النفاذ لحماية البيانات من النفاذ غير المصرح به (ملاحظة – التحكم بالنفاذ يعتمد على الاستيقان الصحيح)؛
- حماية خصوصية البيانات التي تعتمد على التحكم المناسب في النفاذ.

ومنذ البداية تقريباً، كانت ميزات حماية البيانات جزءاً هاماً من توصية قطاع تقييس الاتصالات X.500 فهي بمثابة المواصفة الوحيدة للدليل التي تضم هذه الميزات الهامة.

2.1.6 الاستيقان من مستعملي الدليل

يمكن لدليل توصية قطاع تقييس الاتصالات X.500 أن يسمح بالنفاذ المغفل إلى بعض المعلومات غير الحساسة الواردة فيه. بيد أن النفاذ إلى بيانات أكثر حساسية يستلزم الاستيقان من المستعملين. وتتيح توصية قطاع تقييس الاتصالات X.500 عدة مستويات من الاستيقان، ومنها ما يلي:

أ) اسم فقط؛

ب) اسم بالإضافة إلى كلمة المرور غير المحمية (أي يُرسَل اسم وكلمة المرور في نص التصريح)؛

ج) اسم وكلمة المرور المحمية (أي كلمة المرور المفرومة مع بعض المعلومات الإضافية لضمان كشف أي محاولة للنفاذ إلى الدليل بتكرار القيمة المفرومة)؛

د) الاستيقان القوي، حيث يوقّع المرسل معلومات معينة رقمياً. وتتألف المعلومات الموقعة من اسم المستلم وبعض المعلومات الإضافية التي تسمح أيضاً بكشف محاولة تكرارها.

وتلزم مستويات مختلفة من حماية البيانات على اختلاف أنماط المستعملين النافذين إليها. كما أن مستوى الاستيقان لمستعمل يؤثر في حقوق نفاذه.

3.1.6 التحكم في النفاذ إلى الدليل

يُستعمل التحكم في النفاذ للسماح بإجراء عمليات على معلومات في الدليل أو لمنعها. وتتسم توصية قطاع تقييس الاتصالات X.500 بمرونة كبيرة بشأن كيفية تقسيم معلومات الدليل والمستعملين لأغراض التحكم في النفاذ. وتدعى المعلومة المُزمع حمايتها بنداً محمياً. ويمكن تجميع البنود المحمية ذات الخصائص المشتركة في التحكم في النفاذ. وبالمثل، يمكن تجميع المستعملين وفقاً لمن يُسمح له بالنفاذ ومن يُمنع منه.

وتعتمد حقوق النفاذ لمستعمل أو مجموعة من المستعملين على مستوى الاستيقان. فاستخراج المعلومات الحساسة أو تحديثها سيتطلب عادة مستوى أعلى من الاستيقان من استخراج معلومات أقل حساسية.

كما أن التحكم في النفاذ يأخذ في الحسبان أيضاً نمط النفاذ إلى البيانات، على سبيل المثال، القراءة والإضافة والحذف والتحديث وتغيير الأسماء. في بعض الحالات، قد لا يعلم المستعملون حتى بوجود معلومات معينة.

ولئن كان التحكم في النفاذ مرادفاً لحق المعرفة، فإن حق المعرفة يتجاوز التحكم في النفاذ. فالتمتع بحق المعرفة لا يسمح للمستعمل باستخراج معلومات ما لم تُثبت الحاجة إلى المعرفة، فإن لم تُثبت، يمكن أن يشكل الكشف عن المعلومات انتهاكاً للخصوصية.

وهناك أمثلة أخرى عديدة لا يكون فيها حق المعرفة كافياً. مثلاً:

- حتى وإن كان للمستعمل حق باستخراج عناوين بريدية فردية، فقد لا يكون مناسباً السماح باستخراج عناوين بريدية بالجملة؛
- إذا كان لمستعمل حقوق نفاذ إلى بعض المعلومات، فقد تكون غير ذات صلة بالتطبيق المحدد الذي تُستخرج من أجله، وفي هذه الحالة ليست هناك حاجة إلى المعرفة ولا ينبغي الكشف عن المعلومات.

4.1.6 حماية الخصوصية

إن حماية خصوصية البيانات الواردة في توصية قطاع تقييس الاتصالات X.500 فريدة من نوعها وقوية جداً. وتصبح حماية خصوصية البيانات قضية في الأساس عندما يقوم المستعمل بالبحث في الدليل من خلال تقديم معايير البحث العامة التي يمكن أن تؤدي إلى استخراج كمية كبيرة من المعلومات. (تسمى عمليات البحث هذه أحياناً بتجريف البيانات).

ويرد في توصية قطاع تقييس الاتصالات X.500 مفهوم إدارة الخدمات انطلاقاً من جدول الذي يوفر قدرات حماية خصوصية البيانات علاوة على إدارة الخدمات العامة. إذ يُنشئ المدير جدولاً أو أكثر لكل توليفة من نمط الخدمات وجماعة من المستعملين. ويستلزم نجاح استخراج البيانات تطابق جدول بالكامل مع نمط الخدمة ونمط جماعة المستعملين. غير أن ذلك لا يكفي. فالجدول محمي بالتحكم في النفاذ، أي لا بد أن يؤذَن للمستعمل بالنفاذ إلى الجدول ذي الصلة.

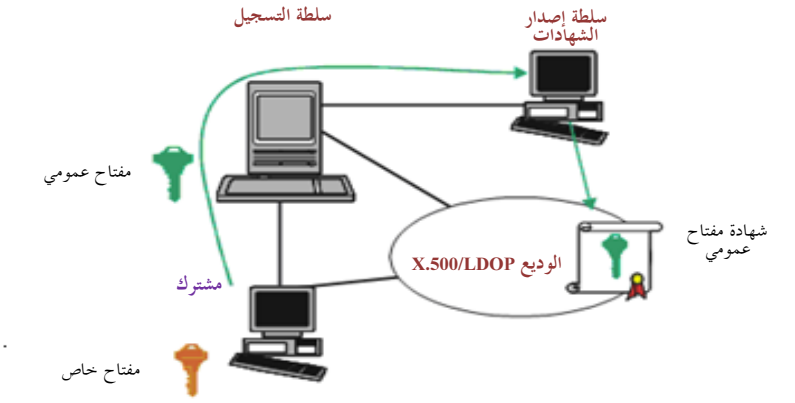
ويدعى الجدول أيضاً قاعدة بحث، ويمكن أن يضم معلومات على النحو التالي:

- معايير البحث المطلوبة لضمان أن البحث مستهدف بحيث يستخرج معلومات عن واحد أو عدد قليل جداً من الكيانات. ويحول ذلك دون عمليات البحث التي تستخرج كما كبيراً من المعلومات، ويحمي من تجريف البيانات؛
- قائمة المعلومات ذات الصلة بنمط الخدمة؛
- معلومات التحكم للكيانات الفردية الممثلة في الدليل. فيتفاعل الجدول المستعمل مع معلومات التحكم لكيان لتقييد المعلومات المقدمة لذلك الكيان. وهذا يسمح بتفصيل البيانات على مقاس معايير حماية الخصوصية لكل كيان على حدة. فقد تكون لكيان ما متطلبات خاصة مثل عدم الكشف عن العنوان البريدي، وربما الرد بتقديم عنوان وهمي بدلاً من ذلك. وقد لا ترغب كيانات أخرى بكشف عناوين بريدها الإلكتروني لمجموعات معينة من المستعملين.

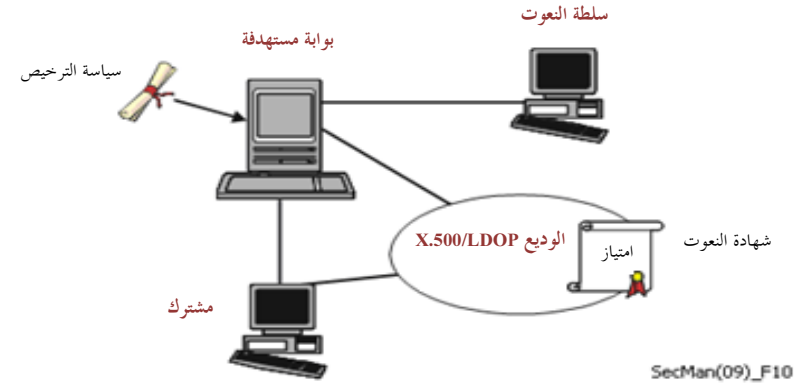
وتتعدد أسباب الانشغال بحماية المعلومات الشخصية الحساسة. فالعديد من معايير الأمن، ولا سيما تلك المتعلقة بالاستيقان من الأفراد وإدارة الهوية، تنطوي على جمع وتخزين معلومات حساسة تعرّف هوية أصحابها شخصياً. ويتزايد عدد الولايات القضائية التي تضع شروطاً قانونية على جمع مثل هذه المعلومات واستعمالها. وإذ تقوم العديد من خدمات الأمن وآلياته على أساس معايير قطاع تقييس الاتصالات، فهي تعمل كآليات لحماية المعلومات الحساسة من ناحية الخصوصية. ويجري تناول الخصوصية في عدد من التوصيات التي يعالج بعضها مباشرة تأثير تكنولوجيات معينة على الخصوصية. ومن الأمثلة توصية قطاع تقييس الاتصالات X.1171 التي تمت الموافقة عليها مؤخراً، وهي بعنوان: *التهديدات ومتطلبات حماية المعلومات التي يمكن تعرّف هوية أصحابها شخصياً في التطبيقات التي تستعمل تعرّف الهوية على أساس العلامة*. وتناقّش هذه التوصية بمزيد من التفصيل في القسم 5.9 عن الخدمات القائمة على أساس العلامة، وكذلك المبادئ التوجيهية بشأن حماية المعلومات التي يمكن تعرّف هوية أصحابها شخصياً في تطبيقات التعرف بواسطة الترددات الراديوية (RFID) التي تقوم لجنة الدراسات 17 بإعدادها الآن كجانب من أعمال إدارة الهوية (IDM) (انظر القسم 4.6).

2.6 الاستيقان القوي: آليات أمن المفاتيح العمومية

تسهل البنية التحتية للمفاتيح العمومية إدارة هذه المفاتيح لدعم خدمات الاستيقان والتجفير والسلامة وعدم التنصل. والتكنولوجيا الأساسية في البنية التحتية للمفاتيح العمومية هي تجفير المفاتيح العمومية الموصوفة أدناه. أما توصية قطاع تقييس الاتصالات X.509 بعنوان الدليل: *الإطار العام لشهادات المفاتيح العمومية والنعوت*، فهي معيار للبنية التحتية للمفاتيح العمومية (PKI) في الاستيقان القوي القائم على شهادات المفاتيح العمومية وسلطات منح الشهادات. وبالإضافة إلى تحديد هيكل استيقان من أجل البنية التحتية للمفاتيح العمومية تتناول التوصية X.509 أيضاً بنية تحتية لإدارة الامتيازات (PMI) والتي تُستخدم للتأكد من حقوق ومزايا المستعملين في سياق الاستيقان القوي الذي يقوم على أساس شهادات النعوت وسلطات النعوت. ويتضمن الشكل 10 مكونات البنية التحتية للمفاتيح العمومية (PKI) والبنية التحتية لإدارة الامتيازات (PMI).



(أ) مكونات البنية التحتية لمفتاح عمومي



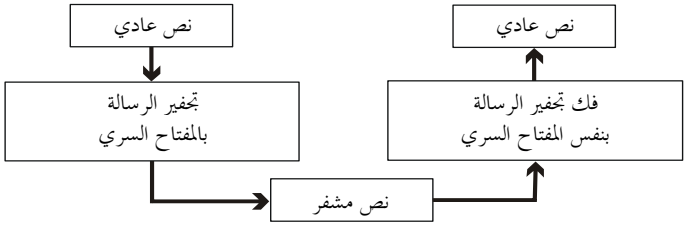
(ب) مكونات البنية التحتية لإدارة الامتيازات

الشكل 10 – مكونات البنية التحتية للمفاتيح العمومية (PKI) والبنية التحتية لإدارة الامتيازات (PMI)

1.2.6 تجفير المفاتيح السرية والمفاتيح العمومية

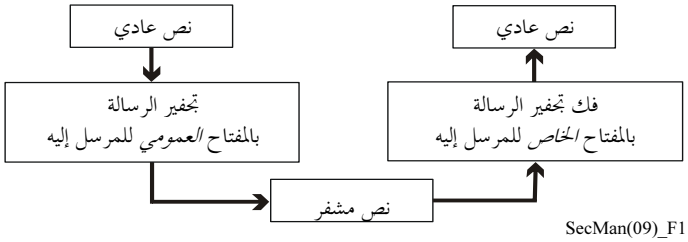
يشير التجفير *التناظري* (أو تجفير *المفتاح السري*) إلى نظام تجفير يُستخدم فيه نفس المفتاح لكل من عملية التشفير وفك التشفير على السواء كما يوضح الشكل 11(أ). ويتقاسم الأفراد في أنظمة التجفير التناظرية مفتاحاً سرياً واحداً. وينبغي أن يكون المفتاح موزعاً على الأفراد عبر وسائل آمنة لأن معرفة مفتاح التشفير تعني معرفة مفتاح فك التشفير والعكس بالعكس.

ويقوم نظام التجفير *اللاتناظري* (أو تجفير *المفتاح العمومي*) على زوج من المفاتيح – مفتاح عمومي ومفتاح خاص كما هو مبين في الشكل 11(ب). ويمكن توزيع المفاتيح العمومية على نطاق واسع ولكن المفتاح الخاص يجب أن يبقى سرياً دوماً. ويُحتفظ بالمفتاح الخاص عادة في بطاقة ذكية أو في علامة خاصة. ويتولد المفتاح العمومي انطلاقاً من المفتاح الخاص، وعلى الرغم من أن هذين المفتاحين مترابطان رياضياً، ليس هنالك من وسيلة ممكنة بغية عكس العملية لاشتقاق المفتاح الخاص من المفتاح العمومي. ولإرسال بيانات سرية إلى شخص ما على نحو آمن باستعمال تجفير المفاتيح العمومية يقوم المرسل بتجفير البيانات مستعملاً المفتاح العمومي لدى المرسل إليه. ثم يقوم المرسل إليه بفك تجفير البيانات مستعملاً المفتاح الخاص المقابل. ومن الممكن أيضاً استعمال تجفير المفاتيح العمومية لوسم بيانات معينة بتوقيع رقمي يقدم تأكيداً على أن وثيقة أو رسالة ما قد صدرت عن الشخص الذي يدّعي أنه المرسل (أو مصدر الرسالة). والتوقيع الرقمي هو في الواقع خلاصة للبيانات المنتجة باستعمال المفتاح الخاص لصاحب التوقيع وهي تذيّل الوثيقة أو الرسالة. أما المرسل إليه فيستعمل المفتاح العمومي لصاحب التوقيع لكي يتأكد من صحة التوقيع الرقمي. (**ملاحظة** – تستخدم بعض أنظمة المفاتيح العمومية زوجين مميزين من أزواج المفاتيح العمومية/الخاصة، زوج للتجفير/لفك التجفير، والآخر للتوقيع/للتحقق الرقمي.)



- يتقاسم الطرفان مفتاحاً سرياً واحداً
- المشكلة: تبادل المفاتيح بسرية كاملة صعب ولا يقبل اتساع النطاق، أي غير عملي لمجموعة كبيرة من المستعملين.
- أفضل مثال معروف: معيار تجفير البيانات (DES)

(أ) تجفير المفتاح التناظري (أو السري)



SecMan(09)_F11

- يوجد لدى كل مشارك
- مفتاح خاص لا يتقاسمه أحد، إضافة إلى
- مفتاح عمومي معروف للجميع
- المشكلة: أبطأ من تجفير المفتاح السري
- أفضل مثال معروف: خوارزمية ريفست وشامير وأدلمان (RSA)

(ب) تجفير مفتاح لا تناظري (أو عمومي)

الشكل 11 – مخطط عمليتي تجفير مفتاح سري ومفتاح عمومي

في حالة التجفير التناظري يجب أن يكون لدى كل زوج من المستعملين مفاتيح مختلفة ويجب أن توزع أزواج المفاتيح هذه ويُحتفظ بها على نحو آمن. أما في حالة التجفير اللاتناظري فيمكن نشر مفاتيح التجفير العمومية في الدليل ويمكن لأي طرف أن يستعمل نفس مفتاح التجفير (العمومي) لكي يرسل بيانات على نحو آمن إلى أي مستعمل يريد. وهذا ما يجعل التجفير اللاتناظري أكثر قابلية لإمكانية اتساع النطاق مما هو الحال في التجفير التناظري. بيد أن التجفير اللاتناظري مكلف من حيث زمن الحوسبة ولذلك ليس من الكفاءة تجفير رسائل بأكملها باستخدام التجفير اللاتناظري. ومن ثم فإن التجفير اللاتناظري يُستخدم عملياً لتوزيع مفاتيح التجفير المتناظرة على نحو آمن. ثم تستخدم المفاتيح المتناظرة بعدئذ لتجفير متن الرسالة باستخدام خوارزمية تناظرية أكثر كفاءة من حيث زمن الحوسبة. وعندما يتطلب الأمر توقيعاً رقمياً تُعد رسالة ملخصة (أو مفرومة) باستخدام وظيفة فرم آمنة في اتجاه واحد مثل خوارزمية الفرم الآمنة SHA1 أو خوارزمية تلخيص الرسالة MD5 ثم يتم تجفير البتات الناتجة باستخدام المفتاح الخاص لدى المرسل وتذيّل الرسالة بهذا التوقيع. ويستطيع المتلقي تأكيد صحة التوقيع الرقمي بفك تجفير التوقيع الرقمي بواسطة المفتاح العمومي للمرسل للحصول على الفرم الذي يولده المرسل ثم باستحداث فرمه الخاص للرسالة المتلقاة. ويجب أن يتطابق الفرمان ليكون التوقيع صالحاً.

وسواء استخدم التجفير التناظري أم اللاتناظري، فإنه ليس من الممكن تسيير الرسائل إلى أصحابها إذا كانت الرسالة بأكملها (مع رأسيتها) مجفرة، إذ إن العقد الوسيطة لن تكون قادرة على معرفة عنوان المرسل إليه. ولذلك لا بد من أن تكون رأسيات الرسائل غير مجفرة عموماً.

ويعتمد التشغيل الآمن لأي نظام من أنظمة المفاتيح العمومية كل الاعتماد على صلاحية هذه المفاتيح العمومية. وتنشر المفاتيح العمومية عادة في شكل شهادات رقمية يُحتفظ بها في دليل بموجب توصية قطاع تقييس الاتصالات X.500. ولا تحتوي الشهادة على مفتاح التجفير العمومي، وعند الاقتضاء مفتاح التحقق من توقيع فرد ما، فحسب وإنما تحتوي على معلومات إضافية ومنها صلاحية الشهادة. والشهادات التي تبطل لأي سبب كان تُدرج كذلك عادة في الدليل في

قائمة إبطال الشهادات (CRL). وقبل استخدام المفاتيح العمومية يجري التحقق عادة من صلاحيتها باستشارة قائمة إبطال الشهادات.

2.2.6 شهادات المفاتيح العمومية

شهادة المفتاح العمومي (التي تسمى أحياناً "الشهادة الرقمية") هي إحدى طرق التحقق من أهلية صاحب زوج من المفاتيح اللاتناظرية. وتقيم هذه الشهادة رابطة وثيقة بين المفتاح العمومي وصاحبه، وهي موقّعة رقمياً من قبل سلطة موثوق بها تشهد على هذه الرابطة. وتعرف هذه السلطة باسم سلطة إصدار الشهادات (CA). وتحدد توصية قطاع تقييس الاتصالات X.509 نسق المعيار القياسي المعترف به دولياً لشهادات المفاتيح العمومية. وتتألف شهادة المفتاح العمومي بموجب توصية قطاع تقييس الاتصالات X.509 من مفتاح عمومي ومُعرِّف للخوارزمية اللاتناظرية التي يتعين أن يستخدم معها المفتاح، واسم صاحب زوج المفاتيح واسم سلطة إصدار الشهادات التي تشهد بهذه الملكية والرقم المسلسل ومدة صلاحية الشهادة ورقم صيغة توصية قطاع تقييس الاتصالات X.509 التي تمتثل لها هذه الشهادة ومجموعة اختيارية من مجالات فرعية تحتوي معلومات عن السياسة التي تطبقها سلطة إصدار الشهادات. ويتم توقيع الشهادة بأكملها رقمياً باستخدام المفتاح الخاص لدى سلطة إصدار الشهادات. ويمكن نشر أي شهادة بموجب توصية قطاع تقييس الاتصالات X.509 على نطاق واسع، كأن تنشر مثلاً على موقع الويب، في دليل بروتوكول النفاذ السريع (LDAP)، أو في البطاقة Vcard[1] المرفقة برسائل البريد الإلكتروني. ويضمن توقيع سلطة إصدار الشهادات أن محتويات الشهادة لا يمكن تعديلها دون علمها.

وللتحقق من صلاحية شهادة ما يحتاج الأمر إلى النفاذ إلى المفتاح العمومي للسلطة التي أصدرت الشهادة وذلك للتحقق من توقيع السلطة على الشهادة. وبما أنه يجوز لسلطة ما أن تُشهد سلطة أخرى (أعلى منها) على مفتاحها العمومي، فقد ينطوي التحقق من المفاتيح العمومية على سلسلة من الشهادات وسلطات إصدار الشهادات. ولا بد أن تنتهي هذه السلسلة في نقطة ما، وهي شهادة من جانب سلطة تكون بمثابة "الأصل الموثوق". ويتم توزيع المفاتيح العمومية لدى هذه السلطة الأصل في شكل شهادات موقعة ذاتياً (يشهد فيها الأصل الموثوق بأن ذلك هو مفتاحه العمومي). ويضمن التوقيع للمستعمل التأكد من أن المفتاح واسم سلطة إصدار الشهادات لم يتم التلاعب فيهما منذ أن صدرت الشهادة. ومع ذلك، لا يمكن الافتراض تلقائياً صحة اسم سلطة إصدار الشهادات المبيّت في شهادة موقعة ذاتياً لأن السلطة أدرجت الاسم في الشهادة بنفسها. ولذلك فإن المكون الحرج في البنية التحتية للمفاتيح العمومية هو التوزيع الآمن للمفاتيح العمومية من جانب سلطة الأصل الموثوق، بحيث يُطمأن إلى أن المفتاح العمومي ينتمي حقاً إلى سلطة الأصل الموثوق المبين اسمها في الشهادة الموقعة ذاتياً. ولولا ذلك، لا يمكن الكشف عن انتحال كيان ما هوية سلطة الأصل الموثوق لإصدار الشهادات.

3.2.6 البُنى التحتية للمفاتيح العمومية

الغرض الرئيسي من البنية التحتية للمفاتيح العمومية هو إصدار شهادات المفاتيح العمومية وإدارتها، بما في ذلك شهادات الأصل الموثوق لسلطة إصدار الشهادات. وتشمل إدارة المفاتيح استحداث أزواج المفاتيح، وإصدار شهادات المفاتيح العمومية، وإبطال شهادات المفاتيح العمومية (عندما تكون سرّية المفتاح الخاص موضع شك مثلاً)، وتخزين وأرشفة المفاتيح والشهادات، وإتلافها عندما ينقضي أجل استعمالها. وتعمل كل سلطة من سلطات إصدار الشهادات طبقاً لمجموعة من السياسات. وتحدد توصية قطاع تقييس الاتصالات X.509 آليات لتوزيع بعض معلومات هذه السياسات في مجالات التمديد في شهادات توصية قطاع تقييس الاتصالات X.509 التي تصدرها سلطة إصدار الشهادات. وتكون قواعد وإجراءات السياسات التي تتبعها سلطة إصدار الشهادات مبينة عادة في سياسة الشهادات وفي بيان ممارسات الإشهاد، وهما من الوثائق التي تنشرها السلطة. ومن شأن هاتين الوثيقتين ضمان أساس مشترك لتقييم درجة الثقة التي يمكن أن توضع في شهادات

[1] بطاقة vCard هي بطاقة الأعمال الإلكترونية ذات النسق المعياري التي يجري تبادلها في كثير من الأحيان عن طريق البريد الالكتروني.

المفاتيح العمومية التي تصدرها السلطات سواء على المستوى الدولي أم عبر القطاعات. كما توفران (جزءاً من) الإطار القانوني الضروري لبناء الثقة فيما بين المنظمات وتضعان قيوداً على استخدام الشهادات الصادرة.

وقد حددت الصيغ الأولى من توصية قطاع تقييس الاتصالات X.509 (1988 و1993 و1997)، العناصر الأساسية اللازمة للبنى التحتية للمفاتيح العمومية. ويشمل ذلك تعريف شهادات المفاتيح العمومية. وتحتوي توصية قطاع تقييس الاتصالات X.509 المراجعة التي اعتُمدت في عام 2001 (وجرى تحديثها في عامي 2005 و2008) تعزيزاً هاماً لشهادات النعوت وإطاراً لبنية تحتية لإدارة الامتيازات (PMI).

4.2.6 البنية التحتية لإدارة الامتيازات

تقوم البنية التحتية لإدارة الامتيازات بإدارة الامتيازات بدعم خدمة ترخيص شاملة فيما يتعلق بالبنية التحتية للمفاتيح العمومية. وتسمح الآليات الموصوفة بتحديد امتيازات نفاذ المستعملين في بيئة متعددة البائعين والتطبيقات. ومفاهيم البنية التحتية لإدارة الامتيازات (PMI) والبنية التحتية للمفاتيح العمومية (PKI) متماثلة، إلا أن البنية التحتية لإدارة الامتيازات تتناول الترخيص بينما تركز البنية التحتية للمفاتيح العمومية على الاستيقان. ويوضح الجدول 4 التماثل بين البنيتين التحتيتين.

الجدول 4 – مقارنة بين خصائص البنية التحتية لإدارة الامتيازات والبنية التحتية للمفاتيح العمومية

البنية التحتية لإدارة الامتيازات	البنية التحتية للمفاتيح العمومية
مصدر السلطة	السلطة الأصل لإصدار الشهادات (مرتكز الثقة)
سلطة تحديد النعوت	سلطة إصدار الشهادات
شهادة النعوت	شهادة المفتاح العمومي
قائمة إبطال شهادات النعوت	قائمة إبطال الشهادات
قائمة إبطال السلطات بالنسبة إلى البنية التحتية لإدارة الامتيازات	قائمة إبطال السلطات بالنسبة إلى البنية التحتية للمفاتيح العمومية

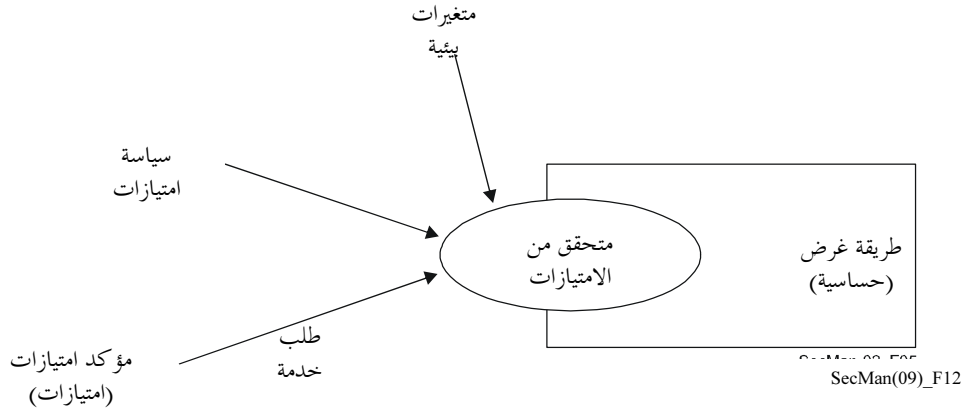
والغرض من تعيين امتيازات للمستعملين هو ضمان اتباعهم لسياسة أمن مقررة يضعها مصدر السلطة. وترتبط تلك المعلومات المتعلقة بالسياسة باسم المستعمل في شهادة النعوت، وتتألف من عدد من العناصر المبينة في الجدول 5.

الجدول 5 – هيكل شهادة النعوت بموجب توصية قطاع تقييس الاتصالات X.509

الصيغة
صاحب الشهادة
جهة الإصدار
التوقيع (شفرة تعريف خوارزمية)
الرقم المسلسل للشهادة
مدة الصلاحية
النعوت
شفرة تعريف فريدة لجهة الإصدار
التمديدات

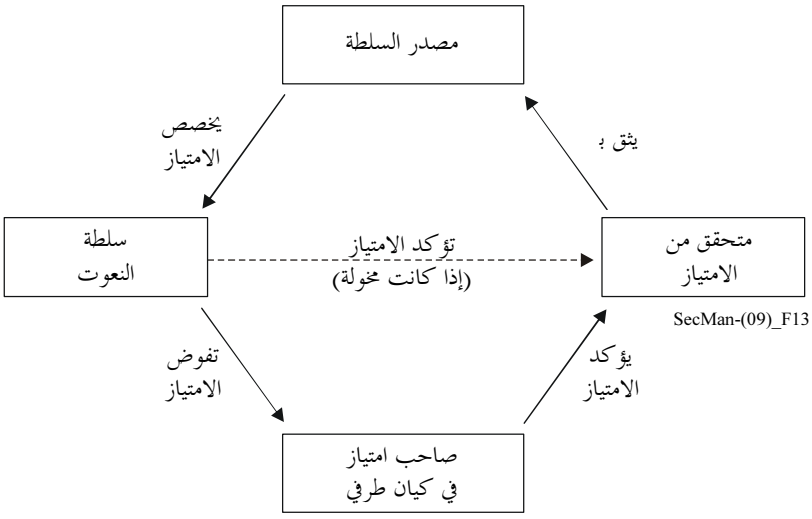
كما تُستعمل شهادات النعوت في الاستدلال الأحيائي عن بعد (انظر القسم 5.6) لإنشاء شهادات استدلال أحيائي لإسناد مستعمل إلى معلومات الاستدلال الأحيائي الخاصة به. وتعرّف شهادات أجهزة الاستدلال الأحيائي قدراتها وحدودها. وتحدد شهادات سياسة الاستدلال الأحيائي العلاقة بين مستوى الأمن ومعلمات خوارزمية الاستدلال الأحيائي.

هنالك خمسة مكونات للتحكم في البنية التحتية لإدارة الامتيازات (PMI) موصوفة في توصية قطاع تقييس الاتصالات X.509، وهي: مؤكد الامتياز، والمتحقق من الامتياز، وطريقة الغرض، وسياسة الامتيازات، والمتغيرات البيئية (انظر الشكل 12). ويمكن للمتحقق من الامتياز أن يتحكم في النفاذ إلى طريقة الغرض بواسطة مؤكد الامتياز طبقاً لسياسة الامتيازات.



الشكل 12 – نموذج تحكم في البنية التحتية لإدارة الامتيازات X.509

وعندما يكون تفويض الامتياز ضرورياً من أجل التنفيذ، تُبحث أربعة مكونات لنموذج التفويض بالنسبة إلى البنية التحتية لإدارة الامتياز في توصية قطاع تقييس الاتصالات X.509 وهي: متحقق من الامتياز، ومصدر السلطة، وسلطة النعوت، ومؤكد الامتياز (انظر الشكل 13).



الشكل 13 – نموذج تفويض البنية التحتية لإدارة الامتيازات X.509

وتعتبر عمليات التنفيذ الحديثة لمخططات الترخيص طبقاً لنموذج التحكم في النفاذ القائم على الدور (RBAC) أن للمستعمل دوراً. وترتبط سياسة الترخيص ما بين مجموعة من التصاريح ودور ما. وعند النفاذ إلى مورد يتم التأكد من دور المستعمل طبقاً للسياسة المقررة لتمكين أي إجراء لاحق.

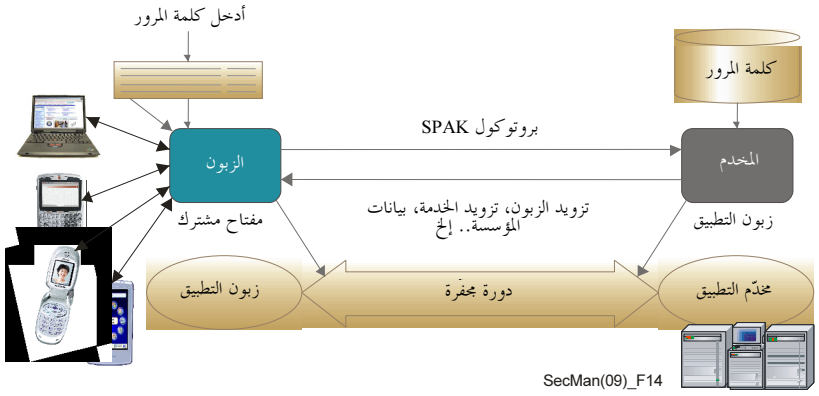
3.6 المبادئ التوجيهية للاستيقان

وُضع عدد من المبادئ التوجيهية التي تتناول جوانب محددة من الاستيقان. ويرد أدناه ملخص عنها.

1.3.6 بروتوكول الاستيقان الآمن القائم على كلمة مرور مع تبادل المفاتيح

بروتوكول الاستيقان الآمن القائم على كلمة مرور مع تبادل المفاتيح (SPAK) هو بروتوكول استيقان بسيط يؤدي فيه استعمال كلمة مرور تحفظها ذاكرة بشرية بين زبون ومخدّم إلى استيقان متبادل وسر مشترك يمكن استعماله كمفاتيح الدورة في الدورة التالية.

وتحدَد في توصية قطاع تقييس الاتصالات X.1151 متطلبات بروتوكول الاستيقان الآمن القائم على كلمة مرور مع تبادل المفاتيح (SPAK) إلى جانب المبادئ التوجيهية لاختيار أنسب بروتوكول SPAK من مختلف بروتوكولات الاستيقان الآمن القائم على كلمة مرور، *والمبدأ التوجيهي بشأن بروتوكول الاستيقان الآمن القائم على كلمة مرور مع تبادل المفاتيح*. ويتميز هذا البروتوكول ببساطته الشديدة. إذ يسهل تنفيذه واستعماله، ولا يحتاج إلى بنية تحتية أخرى (مثل البنية التحتية للمفاتيح العمومية (PKI)). ويُتوقع أن تتزايد أهميته في العديد من التطبيقات في المستقبل القريب. ويوفر بروتوكول SPAK الاستيقان من المستعمل وتبادل مفاتيح قوي على السواء بكلمة مرور بسيطة بحيث يمكن حماية دورة الاتصال اللاحقة بسر يباح به أثناء إجراء الاستيقان (انظر الشكل 14).



الشكل 14 – التشغيل النمطي بروتوكول الاستيقان الآمن القائم على كلمة مرور مع تبادل المفاتيح (SPAK)

2.3.6 بروتوكول الاستيقان القابل للتوسيع

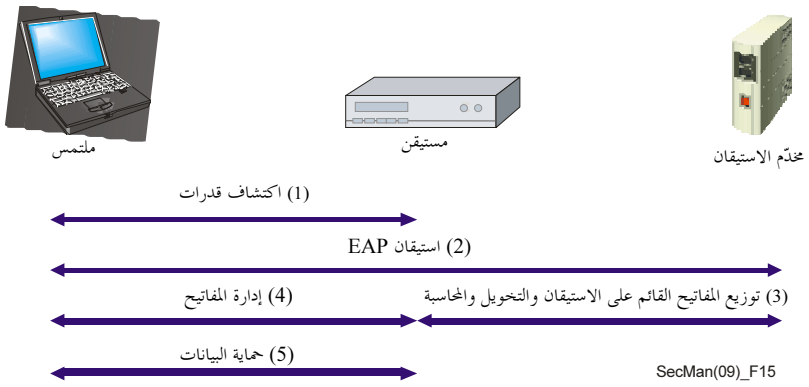
يدعم بروتوكول الاستيقان القابل للتوسيع (EAP) آليات استيقان متعددة بين ملتمس ومخدّم استيقان في شبكة اتصالات بيانات. ويمكن استعمال هذا البروتوكول كأداة أساسية للتمكين من الاستيقان من المستعمل ولتوزيع مفاتيح الدورة. فيمكنه أداء الاستيقان من الجهاز ليؤسس توصيل آمن من نقطة إلى نقطة وليمنع نفاذ جهاز غير مصرح به.

وتصف توصية قطاع تقييس الاتصالات X.1034 إطاراً للاستيقان وإدارة المفاتيح على أساس بروتوكول الاستيقان القابل للتوسيع (EAP) لتأمين الطبقات السفلى في شبكة الاتصالات. وهي توفر توجيهاً بشأن اختيار طرائق هذا البروتوكول وتصف آلية لإدارة المفاتيح للطبقات السفلى في شبكة اتصالات البيانات. وينطبق الإطار على كل من شبكات النفاذ السلكية وشبكات النفاذ اللاسلكية بوسيط مشترك.

وتلزم ثلاثة كيانات للاستيقان وإدارة المفاتيح: ملتمِس (أو ند) ومستيقن ومخدّم استيقان على النحو المبين في الشكل 15. ويعمل الملتمس كمستعمل نهائي نافذاً إلى الشبكة من محطة مستعمل نهائي. بينما يعمل المستيقن كنقطة إنفاذ للسياسة

المرعية متوسطاً رسائل بروتوكول الاستيقان القابل للتوسيع (EAP) بين الملتمس ومخدّم الاستيقان الذي يستيقن من الملتمس ويطلعه اختيارياً على سر يمكن استعماله لاستخلاص مفاتيح التجفير، ويوافي المستيقن بنتيجة الاستيقان من مستعمل نهائي ويرسل إلى المستيقن السر المشترك الذي يمكن استعماله لاستخلاص مفاتيح التجفير بين المستيقن والملتمس لضمان السرية والسلامة وتمكين الاستيقان من الرسالة.

ويتألف الاستيقان وإدارة المفاتيح بصفة عامة من أربع مراحل تشغيلية: اكتشاف قدرات الأمن واستيقان بروتوكول الاستيقان القابل للتوسيع (EAP) وتوزيع المفاتيح وإدارة المفاتيح (انظر الشكل 15). ففي مرحلة قدرات الأمن، يتفاوض الملتمس بشأن قدرات الأمن ومختلف معلمات البروتوكول المزمع استعمالها مع المستيقن. وفي مرحلة بروتوكول الاستيقان القابل للتوسيع، يستيقن مخدم الاستيقان من الملتمس ويستخلص السر الرئيسي المشترك مع الملتمس نتيجةً للبروتوكول. وفي مرحلة توزيع المفاتيح، ينقل مخدم الاستيقان السر الرئيسي إلى المستيقن للسماح للاستيقان باستخراج مختلف مفاتيح التجفير لدورة لاحقة بين ملتمس ومستيقن. ومنعاً لتكرار استعمال المفتاح السري نفسه، ينبغي استعمال مفاتيح تجفير جديدة في كل دورة. وأخيراً، في مرحلة إدارة المفاتيح، يتبادل المستيقن أرقاماً عشوائية مع الملتمس للحصول على مفتاح تجفير جديد مما يؤدي إلى سرية مسبقة كاملة.



الشكل 15 – المراحل التشغيلية الأربع للاستيقان وإدارة المفاتيح في الطبقة السفلى

4.6 إدارة الهوية

1.4.6 نظرة عامة على إدارة الهوية

إدارة الهوية (IdM) هي عملية إدارة معلومات الهوية (مثل مستندات إثباتية ومعرّفات هوية ونعوت وسمات) والتحكم فيها بصورة آمنة. وتُستعمل هذه المعلومات لتمثل كيانات (مثل مقدمي خدمات ومنظمات مستعمل نهائي والناس وأجهزة الشبكة وتطبيقات وخدمات البرمجيات) في عملية الاتصالات. وقد تتعدد الهويات الرقمية لكيان واحد بغية النفاذ إلى خدمات مختلفة ذات متطلبات مختلفة، وهذه قد تكون موجودة في مواقع متعددة. وتدعم إدارة الهوية الاستيقانَ من كيان. ولأغراض قطاع تقييس الاتصالات، يمثل تأكيد كيان لهوية تفرّد ذلك الكيان في سياق معين.

وتعد إدارة الهوية مكوناً رئيسياً من مكونات الأمن السيبراني لأنها توفر القدرة على إقامة وإدامة الاتصالات الموثوقة بين الكيانات وتمكّن من النفاذ عند الترحال والنفاذ حسب الطلب إلى الشبكات والخدمات الإلكترونية. كما تمكن من منح مجموعة من الامتيازات (بدلاً من كل الامتيازات أو لا شيء) وتسهل تغيير الامتيازات إذا تغيّر دور الكيان. وإذ تعزز إدارة الهوية قدرة المنظمة على تطبيق السياسات الأمنية بتمكين مراقبة نشاط الكيان على الشبكة والتحقق منه، يمكنها أن توفر إمكانية النفاذ إلى كيانات داخل وخارج المنظمة على السواء.

وتضمن إدارةُ الهوية معلومات الهوية على نحو يدعم تحكم آمن وموثوق في النفاذ. وتتحقق هذه القدرة بتحكم المستعمل في المعلومات التي يمكن تعرّف هوية أصحابها شخصياً من خلال تشغيل واحد/إيقاف واحد، وبتمكن المستعمل من اختيار مزود هوية ينوب عنه في وظائف التحقق والتفويض، على النقيض من تقديم مستندات إثباتية لكل مقدم خدمة. وتدعم إدارة الهوية العديد من الخدمات القائمة على أساس الهوية، بما في ذلك: الإعلانات المستهدفة والخدمات الشخصية القائمة على أساس الموقع الجغرافي والاهتمامات والخدمات المستيقن منها الرامية للحد من الاحتيال وسرقة الهوية.

وتنطوي إدارة الهوية على تكنولوجيا معقدة تشمل ما يلي:

- إنشاء معلومات الهوية وتعديلها وتجميد العمل بها وحفظها وإنهاؤها؛
- الاعتراف بالهويات الجزئية التي تمثل الكيانات في سياق أو دور محدد؛
- إرساء الثقة وتقييمها بين الكيانات؛
- الحصول على معلومات عن هوية كيان (مثلاً، عن طريق مقدم هويات موثوق يتولى المسؤولية القانونية عن الحفاظ على معرّفات الهوية والمستندات الإثباتية وبعض نعوت الكيان أو كلها).

أما الإضافة على سلسلة توصيات قطاع تقييس الاتصالات X.1250 بعنوان: لمحة عامة عن إدارة الهوية في سياق الأمن السيبراني، فهي تقدم مقدمة موجزة إلى موضوع إدارة الهوية.

2.4.6 أعمال إدارة الهوية في قطاع تقييس الاتصالات

لئن كان النقاش ما زال دائراً حول بعض المفاهيم الأساسية والمفردات الأساسية، فإن العمل ماضٍ في عدد من المجالات في لجنة الدراسات 17 (لجنة الدراسات الرئيسية في مجال إدارة الهوية) وكذلك في لجنة الدراسات 2 (المعنية بالجوانب التشغيلية لتوفير الخدمات وإدارة الاتصالات) ولجنة الدراسات 13 (المعنية بشبكات المستقبل بما فيها شبكات الخدمة المتنقلة وشبكات الجيل التالي).

وتتولى لجنة الدراسات 2 مسؤولية الدراسات المتصلة بضمان اتساق نسق معرّفات إدارة الهوية وهيكلها وبتحديد السطوح البينية لأنظمة الإدارة لدعم توصيل معلومات الهوية ضمن الميادين التنظيمية أو فيما بينها.

أما لجنة الدراسات 13 فهي المسؤولة عن المعمارية الوظيفية لإدارة الهوية الخاصة بشبكات الجيل التالي والتي تدعم خدمات الهوية ذات القيمة المضافة والتبادل الآمن لمعلومات الهوية وتطبيق سد الثغرات/قابلية التشغيل البيني ما بين مجموعة متنوعة من أنساق معلومات الهوية. كما تتولى لجنة الدراسات 13 مسؤولية تحديد أي تهديدات تتعرض لها إدارة الهوية ضمن شبكات الجيل التالي وآليات للتصدي لها. وقد تمت الموافقة بالفعل على توصية قطاع تقييس الاتصالات Y.2720 بعنوان *إطار إدارة الهوية في شبكات الجيل التالي*. ويصف هذا المعيار نهج مهيكل لتصميم حلول إدارة الهوية وتحديدها وتنفيذها، ولتسهيل التشغيل البيني في بيئات غير متجانسة.

وتضطلع لجنة الدراسات 17 بمسؤولية الدراسات المتصلة بوضع نموذج عام لإدارة الهوية مستقل عن تكنولوجيات الشبكة ويدعم التبادل الآمن لمعلومات الهوية بين الكيانات. ويشمل هذا العمل أيضاً دراسة عملية اكتشاف المصادر الموثوقة لمعلومات الهوية؛ والآليات التنوعية لسد الثغرات/قابلية التشغيل البيني بين مجموعة متنوعة من أنساق معلومات الهوية؛ وتهديدات إدارة الهوية وآليات مكافحتها وحماية المعلومات التي يمكن تعرّف هوية أصحابها شخصياً (PII) ووضع آليات لضمان ترخيص النفاذ إلى هذه المعلومات عند الاقتضاء فقط. وفي سبتمبر 2009، تمت الموافقة على توصيتين لقطاع تقييس الاتصالات: X.1250 بعنوان *مقدرات مرجعية للإدارة العالمية المعززة للهوية وإمكانية التشغيل البيني*، وX.1251 بعنوان *إطار لتحكم المستعمل في الهوية الرقمية*. وبالإضافة إلى ذلك، يجري إعداد مجموعة مرجعية من التعاريف المتصلة بإدارة الهوية للمساعدة في ضمان توحيد المصطلحات واتساقها ضمن معايير إدارة الهوية في قطاع تقييس الاتصالات.

وتأسس نشاط تنسيق مشترك لإدارة الهوية (JCA-IdM) لتنسيق أعمال قطاع تقييس الاتصالات في إدارة الهوية. كما أُطلقت مبادرة المعايير الدولية لإدارة الهوية (IdM-GSI) بغية مواءمة النُهُج المختلفة في جميع أنحاء العالم إزاء إدارة الهوية والتعاون مع الهيئات الأخرى العاملة في هذا الموضوع. وتقدم لجنة الدراسات الرئيسية المعنية بإدارة الهوية معلومات مستفيضة عن أنشطة إدارة الهوية، وقد وافقت على توصيات بشأن إدارة الهوية وهي بصدد إعداد غيرها إلى جانب معلومات أخرى تتصل بأعمال إدارة الهوية.

5.6 الاستدلال الأحيائي عن بعد

يركز الاستدلال الأحيائي عن بعد على التعرّف الشخصي والاستيقان باستعمال أجهزة الاستدلال الأحيائي عن بعد في بيئات الاتصالات. وينصرف التركيز بصورة خاصة إلى كيفية تحسين التعرّف على المستعملين والاستيقان منهم باستعمال طرائق استدلال إحيائي عن بعد توفر السلامة والأمن. ويجري عمل قطاع تقييس الاتصالات بشأن هذا الموضوع بالتعاون الوثيق مع المنظمات الأخرى المعنية بوضع المعايير، وهو عمل يغطي مواضيع تشمل ما يلي: التفاعل بين الإنسان والبيئة؛ ومفاتيح الاستدلال الأحيائي الرقمية؛ وملحقات الاستدلال الأحيائي بشهادات X.509؛ والاستيقان بالاستدلال الأحيائي في شبكة مفتوحة.

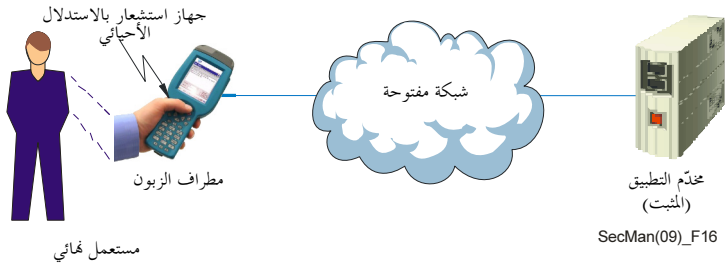
1.5.6 الاستيقان بالاستدلال الأحيائي

يستطيع الاستدلال الأحيائي أن يدعم خدمات استيقان آمنة إلى درجة عالية، إلا أن تقييس الاستيقان بالاستدلال الأحيائي على شبكة مفتوحة يواجه عدداً من التحديات:

- فقد لا تتوفر لدى مقدمي الخدمات أية معلومات بشأن ماهية أجهزة الاستدلال الأحيائي المستعملة في بيئة المستعمل النهائي، ومستوى/إعدادات الأمن في مثل هذه الأجهزة وكيفية تشغيلها؛
- وتختلف الدقة (معدل القبول الخاطئ) المحددة بمعلمة العتبة على اختلاف منتجات الاستدلال الأحيائي. لذلك، يتعذر على مقدم الخدمة أن يدعي الحفاظ على مستوى دقة ثابت؛
- وقد تتراجع دقة التحقق بالاستدلال الأحيائي مع تقدم المستعملين النهائيين بالعمر، لأن الاستدلال الأحيائي يستخدم خصائص الجسم البشري.

وفي توصية قطاع تقييس الاتصالات X.1084 بعنوان *البروتوكول العام للاستيقان بالاستدلال الأحيائي وملامح نموذج النظام العامة لأنظمة الاتصالات في شبكة مفتوحة*، يرد توصيف البروتوكولات العامة للاستيقان بالاستدلال الأحيائي وملامحها العامة لأنظمة الاتصالات في شبكة مفتوحة.

ويبيّن الشكل 16 الاستيقان من مستعمل نهائي عبر شبكة مفتوحة دون مقابلته وجهاً لوجه.

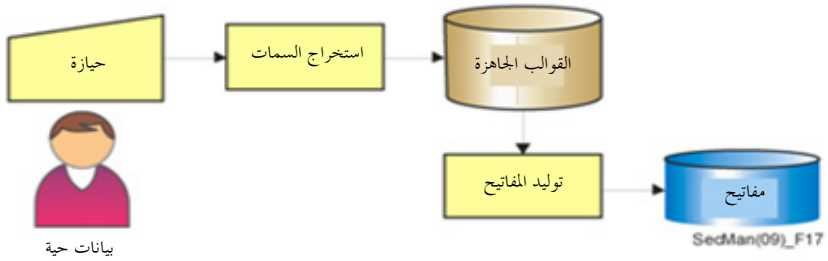


الشكل 16 – الاستيقان من مستعمل نهائي بالاستدلال الأحيائي

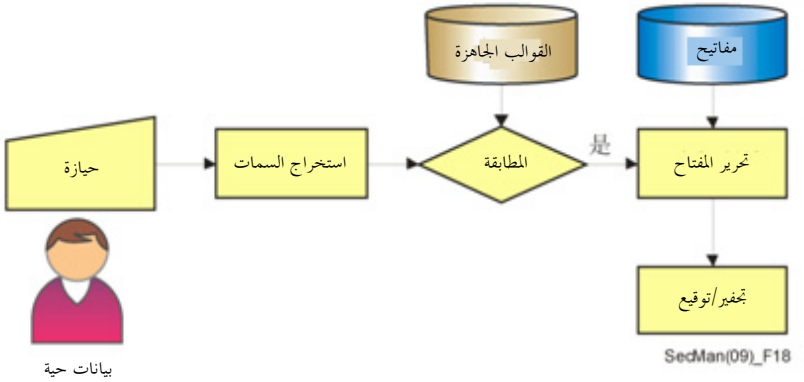
2.5.6 توليد المفاتيح الرقمية بالاستدلال الأحيائي وحمايتها

حُدد إطار لتوليد المفاتيح الرقمية بالاستدلال الأحيائي في توصية قطاع تقييس الاتصالات X.1088 بعنوان: *إطار لتوليد المفاتيح الرقمية بالاستدلال الأحيائي وحمايتها*. ويحدد هذا الإطار الحماية باستعمال أنموذج استدلال أحيائي مع شهادة مفتاح عمومي وشهادة استدلال أحيائي ليوفر استيقاناً آمناً من الناحية التجفيرية واتصالات آمنة على شبكات مفتوحة. كما تُحدَد متطلبات الأمن لتوليد المفاتيح الرقمية وحمايتها. ويمكن تطبيق هذا الإطار على التجفير والتوقيع الرقمي بالاستدلال الأحيائي. وتُقترح طريقتان هما:

- توليد مفاتيح الاستدلال الأحيائي، حيث يُنشأ المفتاح من أنموذج استدلال أحيائي (الشكل 17)؛
- إسناد/استعادة مفتاح استدلال أحيائي حيث يُخزن المفتاح في قاعدة بيانات ويمكن استخراجه باستيقان بالاستدلال الأحيائي (الشكل 18).



الشكل 17 – توليد مفاتيح الاستدلال الأحيائي



الشكل 18 – إسناد/استعادة مفتاح استدلال أحيائي

3.5.6 جوانب الأمن والسلامة في الاستدلال الأحيائي عن بعد

حُدد في نموذج الاستدلال الأحيائي عن بعد المتعدد الأساليب (توصية قطاع تقييس الاتصالات X.1081، بعنوان *إطار لتوصيف جوانب الأمن والسلامة للاستدلال الأحيائي عن بُعد*) إطار لجوانب الأمن والسلامة في الاستدلال الأحيائي عن بعد يحدد التفاعلات بين الإنسان والبيئة وكذلك الكميات والوحدات المستخدمة لقياس هذه التفاعلات. ولا يقتصر

نموذج الاستدلال الأحيائي عن بُعد المتعدد الأساليب على النظر في التفاعلات المادية البحتة، بل يعترف أيضاً بالتفاعلات السلوكية التي لا تقاس كمياً بوحدات معيارية في الوقت الراهن.

4.5.6 الاستدلال الأحيائي عن بعد ذو الصلة بالفيزيولوجيا البشرية

يجري تناول جوانب الأمن والسلامة أيضاً في توصية قطاع تقييس الاتصالات X.1082 بشأن *الاستدلال الأحيائي عن بعد ذي الصلة بالفيزيولوجيا البشرية* والتي تحدد كميات ووحدات للخصائص الفيزيولوجية أو البيولوجية أو السلوكية التي يمكن أن توفر دخلاً أو خرجاً للتعرف بالاستدلال الأحيائي أو أنظمة التحقق (أنظمة الإدراك)، بما في ذلك أية عتبات كشف أو سلامة. وتعطي التوصية أسماء وتعاريف ورموز لكميات ووحدات الاستدلال الأحيائي عن بعد ذات الصلة بالفيزيولوجيا البشرية (أي الخصائص البشرية والانبعاثات التي يمكن كشفها بواسطة جهاز استشعار). وتشمل أيضاً الكميات والوحدات المعنية بآثار استعمال أجهزة الاستدلال الأحيائي عن بعد على الإنسان.

5.5.6 تطورات أخرى في معايير الاستدلال الأحيائي عن بعد

لإنتاج شهادات الاستدلال الأحيائي، حُددت التوسعات في شهادات توصية قطاع تقييس الاتصالات X.509 المستعملة في البنى التحتية للمفاتيح العمومية أو البنى التحتية لإدارة الامتيازات. ويرد توصيفها في توصية قطاع تقييس الاتصالات X.1089 بشأن *البنية التحتية للاستيقان بالاستدلال الأحيائي عن بُعد*.

أما توصية قطاع تقييس الاتصالات X.1083 بشأن *بروتوكول العمل البيني للسطوح البينية لبرمجة تطبيقات الاستدلال الأحيائي (BioAPI)* فهي توصّف قواعد التركيب (باستعمال قواعد التركيب المجردة رقم 1 (ASN.1)) والدلالات اللغوية وترميزات الرسائل التي تمكن تطبيق مطابق للسطح البيني لبرمجة تطبيقات الاستدلال الأحيائي من طلب عمليات استدلال أحيائي لدى مقدمي خدمة الاستدلال الأحيائي المطابقة للسطح البيني لبرمجة تطبيقات الاستدلال الأحيائي (BSPs) في جميع أنحاء العقدة أو على امتداد تخوم العملية، ومن التبليغ عن الأحداث المتأتية عن مقدمي الخدمة البعيدين هؤلاء.

7. تأمين البنية التحتية للشبكة

7 تأمين البنية التحتية للشبكة

تستخدم البيانات لرصد شبكة الاتصالات والتحكم فيها. وغالباً ما تُرسل حركة الإدارة على شبكة منفصلة لا تحمل سوى حركة إدارة الشبكة وليس حركة المستعملين. ويشار غالباً إلى هذه الشبكة باسم شبكة إدارة الاتصالات (TMN) الوارد وصفها في توصية قطاع تقييس الاتصالات M.3010 بشأن *المبادئ المتعلقة بشبكة إدارة الاتصالات*. ولا بد من تأمين هذه الحركة. وتقسم حركة الإدارة عادة إلى فئات على أساس المعلومات المطلوبة لوظائف التعامل مع الأعطال والتشكيل والأداء والمحاسبة وإدارة الأمن. وتتولى إدارة أمن الشبكة إقامة شبكة إدارة آمنة وكذلك إدارة أمن المعلومات المتصلة بالمستويات الثلاثة لمعمارية الأمن X.805.

يجب الاضطلاع دوماً بنشاط الإدارة المتصل بعناصر البنية التحتية لشبكة على نحو آمن. فعلى سبيل المثال، يجب ألا يقوم بأنشطة الشبكة إلا مستعمل مصرح له. ولتقديم حل من طرف إلى طرف، ينبغي تطبيق تدابير أمنية (من قبيل التحكم في النفاذ والاستيقان) على كل نمط من أنشطة الشبكة في البنية التحتية للشبكة وخدمات الشبكة وتطبيقات الشبكة. وهناك عدد من توصيات قطاع تقييس الاتصالات تركز تحديداً على الجانب الأمني من مستوي الإدارة لعناصر الشبكة وأنظمة الإدارة التي تشكل جزءاً من البنية التحتية للشبكة.

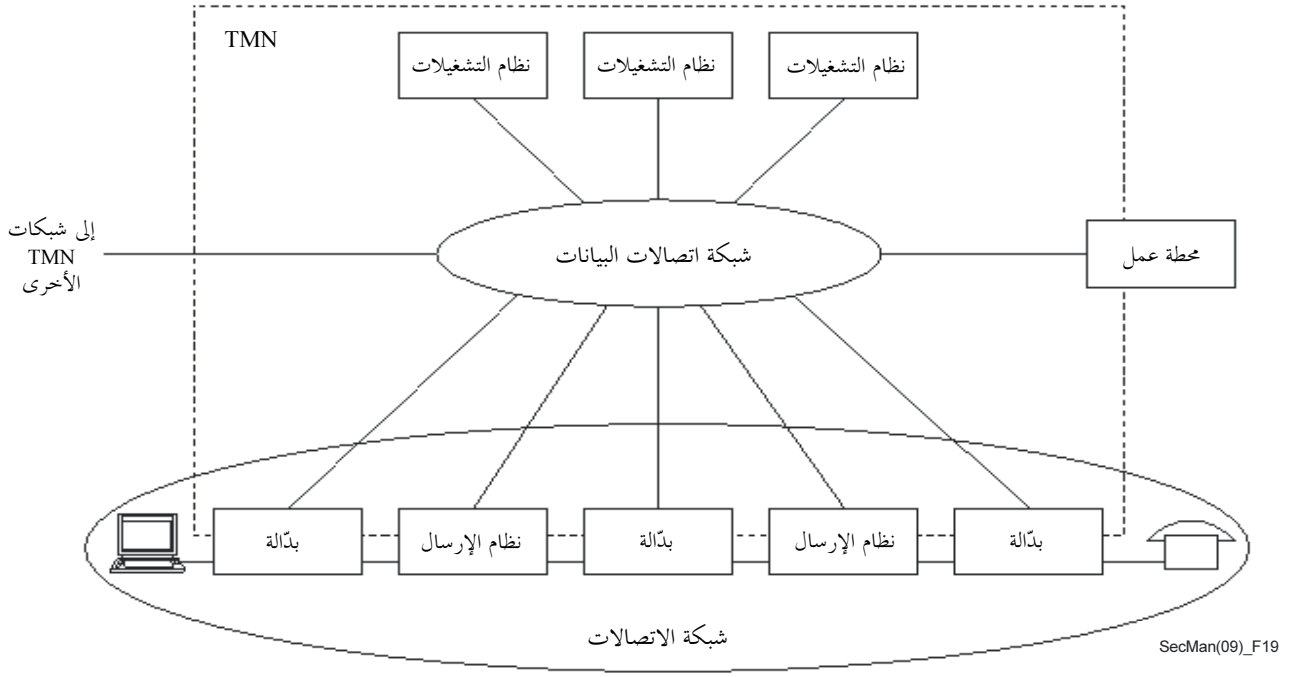
وتشمل تطبيقات إدارة الشبكة الأخرى تلك المتصلة بالبيئات حيث يحتاج مقدمو الخدمة المختلفون للتفاعل فيما بينهم كي يعرضوا خدمات من طرف إلى طرف. ومن الأمثلة على ذلك، المرافق المقدمة إلى المؤسسات التنظيمية أو الحكومية دعماً للتعافي من الكوارث، والحالات التي تقدم فيها الخطوط المؤجرة إلى الزبائن عبر الحدود الجغرافية.

1.7 شبكة إدارة الاتصالات

وتكون شبكة إدارة الاتصالات منفصلة ومعزولة عن البنية التحتية للشبكة العمومية بحيث لا يصل إليها أي عطل نتيجة تهديد أمني في مستوى المستعمل النهائي في الشبكة العمومية. ونتيجة لهذا الانفصال، من السهل نسبياً تأمين حركة شبكة الإدارة لأن النفاذ إلى هذا المستوى مقصور على مديري الشبكة المرخص لهم بذلك، ومن ثم تقتصر الحركة على أنشطة الإدارة الصحيحة. ولكن في إطار شبكات الجيل التالي، قد يتم أحياناً الجمع بين تطبيق حركة مستعمل نهائي وتطبيق حركة الإدارة. ولئن كان هذا النهج يساعد على تقليل التكاليف إلى أدنى حد، لأنه لا يتطلب سوى بنية تحتية لشبكة متكاملة وحيدة، فإنه يؤدي أيضاً إلى ظهور كثير من تحديات الأمن الجديدة. إذ تصبح التهديدات في مستوى المستعمل النهائي تهديدات على مستويات الإدارة والتحكم. وإذ يصبح مستوى الإدارة مفتوحاً لنفاذ العديد من المستعملين النهائيين، يصبح من الممكن حدوث أنواع كثيرة من الأنشطة المؤذية.

2.7 معمارية إدارة الشبكة

يرد في توصية قطاع تقييس الاتصالات M.3010 تعريف معمارية تحديد إدارة الشبكة في شبكة اتصالات ما. ويوضح الشكل 19 علاقة شبكة إدارة الاتصالات (TMN) بشبكة الاتصالات. وتحدد معمارية شبكة الإدارة السطوح البينية التي تقرر التبادلات المطلوبة لأداء وظائف العمليات والإدارة والصيانة وتوفير الخدمة.



ملاحظة – يمكن التوسّع بحدود شبكة إدارة الاتصالات الممثلة بخط متقطع لتشمل خدمات الزبون/المستعمل والمعدات وإدارتها

الشكل 19 – علاقة شبكة إدارة الاتصالات (TMN) بشبكة الاتصالات

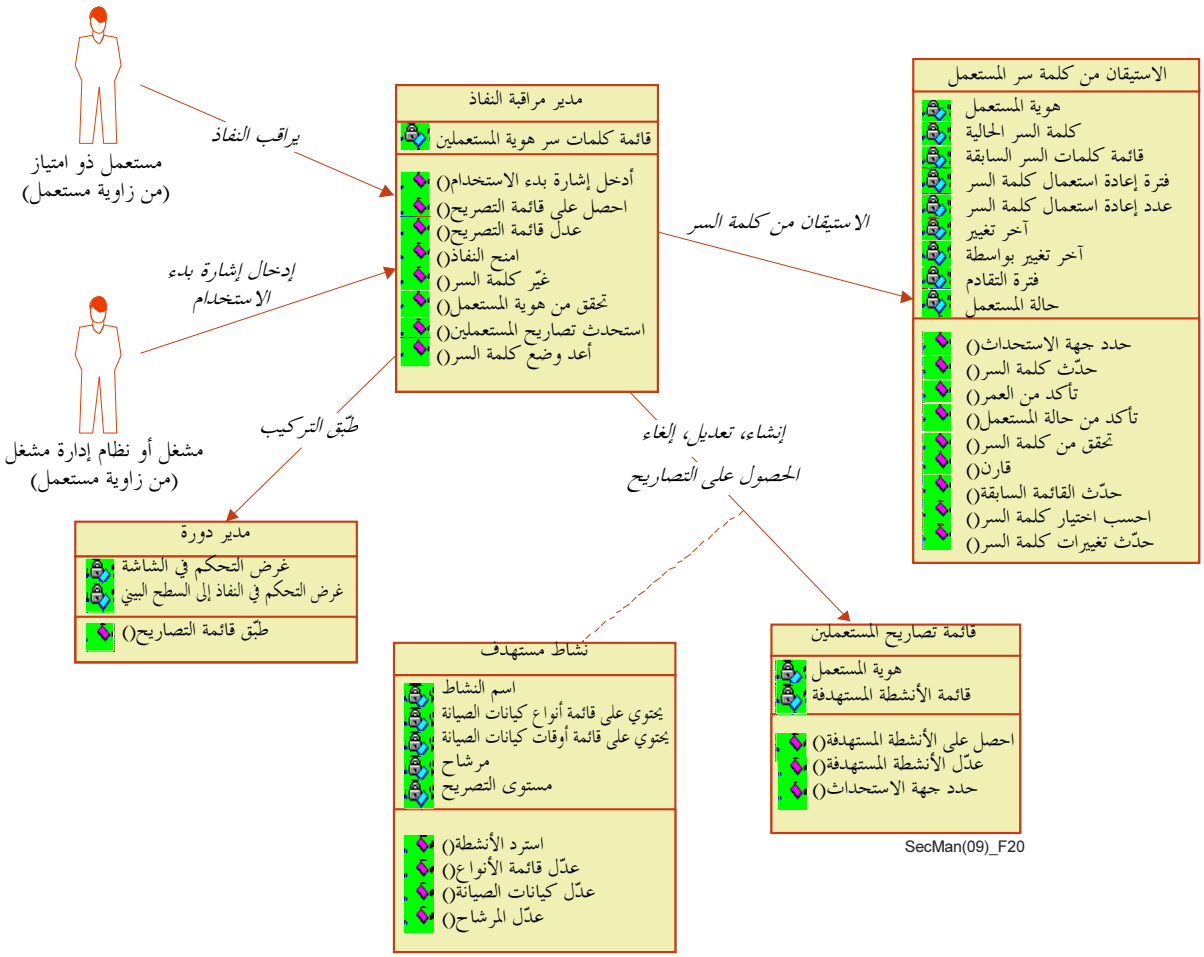
وتشتمل توصية قطاع تقييس الاتصالات M.3016.0 على لمحة عامة وهيكل يحدد محاذير الأمن التي تتهدد شبكة إدارة الاتصالات (TMN). وفي إطار سلسلة التوصيات M.3016 تحدد توصية قطاع تقييس الاتصالات M.3016.1 المتطلبات المفصلة وتوصية قطاع تقييس الاتصالات M.3016.2 خدمات الأمن وتوصية قطاع تقييس الاتصالات M.3016.3 الآليات التي يمكن بها مواجهة التهديدات ضمن سياق المعمارية الوظيفية لشبكة TMN، كما هي محددة في توصية قطاع تقييس الاتصالات M.3010. وبما أن مختلف المنظمات لا تحتاج إلى أن تضع جميع المتطلبات فإن توصية قطاع تقييس الاتصالات M.3016.4 توفر قالباً لاستحداث مواصفات على أساس متطلبات الأمن والخدمات والآليات. يمكن استخدام هذا من أجل الامتثال لسياسة الأمن التي تنفرد بها منظمة ما.

وهنالك وجهان يؤخذان في الاعتبار عند مناقشة إدارة أمن الشبكة. يتعلق أحدهما بمستوي الإدارة لنشاط مستعمل من طرف إلى طرف (مثل خدمات نقل الصوت بواسطة بروتوكول الإنترنت). ولا بد من القيام بإدارة المستعملين بطريقة آمنة. وهذا ما يشار إليه بعبارة تبادل *أمن معلومات الإدارة* عبر الشبكة لدعم تطبيق من طرف إلى طرف. والوجه الآخر هو إدارة معلومات الأمن التي تُطبق بغض النظر عن التطبيق. فمثلاً، يجب القيام بنشاط الإبلاغ عن عطل بين جهتين من مقدمي الخدمة بشكل آمن. وقد يستلزم ذلك تجفير التبادلات، وفي هذه الحالة يجب أن يُحسب حساب إدارة مفاتيح التجفير.

وتتوفر عدة توصيات تتناول وظائف إدارة الأمن لمعمارية التوصية X.805 بالنسبة إلى طبقات مستوي الإدارة الثلاث (انظر الشكل 1). وبالإضافة إلى ذلك، ووفق البحث الوارد في الأقسام الفرعية أدناه، هنالك توصيات أخرى تتضمن تعريف الخدمات النوعية أو المشتركة مثل إطلاق الإنذارات عند حدوث انتهاك للأمن، ووظائف التدقيق، ونماذج معلومات تعرّف سويات الحماية لأهداف مختلفة.

3.7 تأمين عناصر البنية التحتية لشبكة

يمكن النظر في توصيلية من طرف إلى طرف على أساس شبكة (أو شبكات) نفاذ وشبكة (أو شبكات) أساسية. ويمكن استخدام تكنولوجيات مختلفة في هذه الشبكات. وقد تم وضع توصيات تتناول كلاً من شبكات النفاذ والشبكات الأساسية. وتُستعمل الشبكة البصرية المنفعلة عريضة النطاق كمثال هنا. وتتضمن توصية قطاع تقييس الاتصالات Q.834.3 إدارة امتيازات مستعمل شبكة نفاذ باستخدام منهجية وضع النماذج الموحدة، بينما تتضمن توصية قطاع تقييس الاتصالات Q.834.4 تعريف تبادل الإدارة باستخدام معمارية وسيط مشترك لطلب غرض (CORBA). ويطبق السطح البيني الموصوف في هذه التوصيات بين نظام إدارة العناصر ونظام إدارة الشبكات. ويستخدم الأول لإدارة عناصر الشبكة الفردية، وبالتالي يدرك التفاصيل الداخلية لمعماريات عتاد وبرمجيات العناصر الواردة من طرف واحد أو أكثر، بينما يقوم الثاني بالأنشطة على مستوى الشبكة من طرف إلى طرف ويشمل أنظمة إدارة العديد من الموردين. ويبين الشكل 20 الأغراض المختلفة المستخدمة لإنشاء وإلغاء وتخصيص واستخدام معلومات التحكم في النفاذ لمستعملي نظام إدارة العناصر. وتحتوي قائمة تصاريح المستعملين على قائمة بأنشطة الإدارة المسموح بها لكل مستعمل مرخص له بذلك. ويتحقق مدير التحكم في النفاذ من هوية المستعمل ومن كلمة المرور الخاصة به لنشاط الإدارة ويمنحه حق النفاذ وفقاً للعناصر الوظيفية المسموح بها والمدرجة في قائمة التصاريح.



الشكل 20 – إدارة امتيازات المستعمل بموجب توصية قطاع تقييس الاتصالات Q.834.3

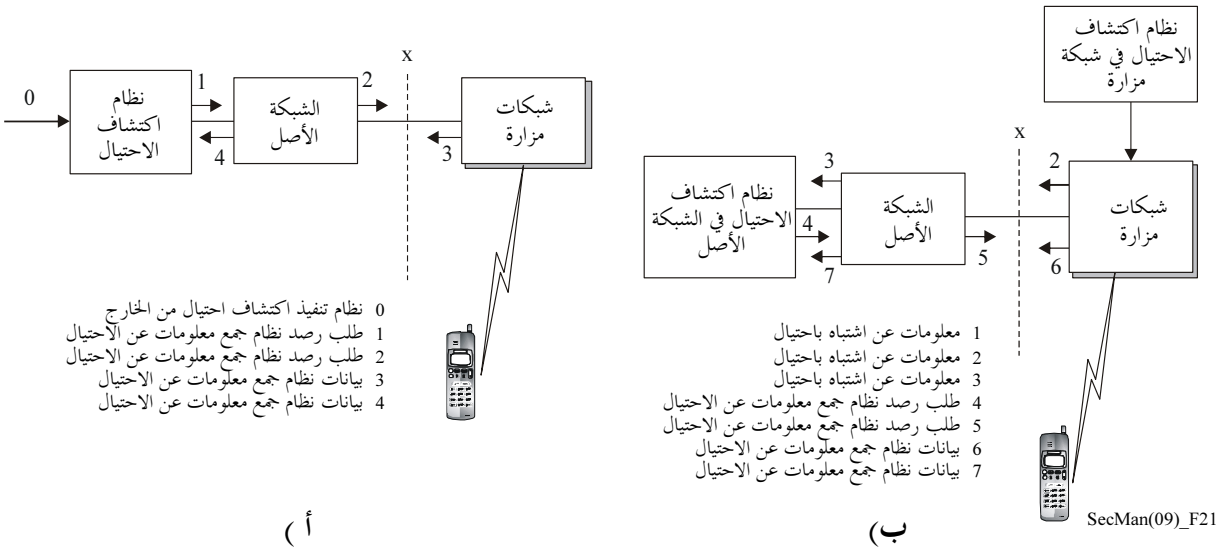
4.7 تأمين أنشطة المراقبة والتحكم

هناك جانبان للأمن على صلة بالتقاطع بين مستوي الإدارة وطبقة الخدمات. إذ يضمن أحدهما توفير تدابير الأمن الملائمة للخدمات المقدمة في الشبكة. ومن أمثلة ذلك، ضمان أن أداء العمليات المرتبطة بتوفير الخدمة يقتصر على المستعملين المخولين، بينما يتناول الجانب الثاني تعريف ما هي التبادلات الإدارية وتبادلات الإدارة الصحيحة، بغية المساعدة في اكتشاف انتهاكات الأمن.

فتوصية قطاع تقييس الاتصالات M.3208.2، بشأن *إدارة التوصيل لتوصيلات وصلة الخدمة الموفرة مسبقاً لإنشاء خدمة دارة مؤجرة*، تتناول الجانب الأول وهو نشاط إدارة خدمة ما. وتسمح خدمة إدارة التوصيل هذه للمشترك بإنشاء/تفعيل، أو تعديل أو إلغاء الدارات المؤجرة في نطاق حدود الموارد الموفرة مسبقاً. ولأن المستعمل هو الذي يوفر التوصيلية من طرف إلى طرف، فمن الضروري ضمان أن المستعملين المخولين فقط هم الذين يسمح لهم بأداء هذه العمليات. وأبعاد الأمن X.805 المرتبطة بهذه الخدمة هي الاستيقان من كيان نظير، والتحكم في سلامة البيانات (لمنع التعديل غير المرخص به للبيانات أثناء العبور)، والتحكم في النفاذ (لضمان عدم نفاذ مشترك ما إلى بيانات مشترك آخر قصد الإيذاء أو بشكل عرضي).

وتوصية قطاع تقييس الاتصالات M.3210.1 ، بشأن *خدمات إدارة شبكة إدارة الاتصالات (TMN) لإدارة أمن الاتصالات المتنقلة الدولية 2000*، تحدد الأنشطة الإدارية المرتبطة بمستوي الإدارة للخدمات اللاسلكية، وتقدم مثالاً عن معيار يتناول الجانب الثاني. وفي الشبكة اللاسلكية، عندما يتحول المستعملون من الشبكة

الأصل إلى الشبكة المزارة قد يعبرون ميادين إدارية مختلفة. وتصف الخدمات المعرّفة في توصية قطاع تقييس الاتصالات M.3210.1 كيف أن ميدان إدارة حالات الاحتيال في الموقع الأصل يقوم بجمع المعلومات الملائمة عن مشترك ما مسجل على الشبكة المزارة. ويوضح كل من السيناريو أ) والسيناريو ب) في الشكل 21 الشروع في نشاط رصد الإدارة سواء بواسطة الشبكة الأصل أو الشبكة المزارة. ويطلب نظام كشف الاحتيال في الشبكة الأصل معلومات عن الأنشطة عندما يُسجل مشترك ما لدى شبكة مزارة ويظل ناشطاً فيها إلى أن ينسحب من التسجيل فيها. وبعدئذ يمكن وضع مواصفات تتصل بالاستعمال على أساس تحليل سجلات النداءات إما في سوية الخدمة أو من أجل مشترك ما. ويستطيع نظام كشف الاحتيال القيام بعملية التحليل وتوليد الإنذارات الملائمة عند كشف السلوك الاحتيالي.

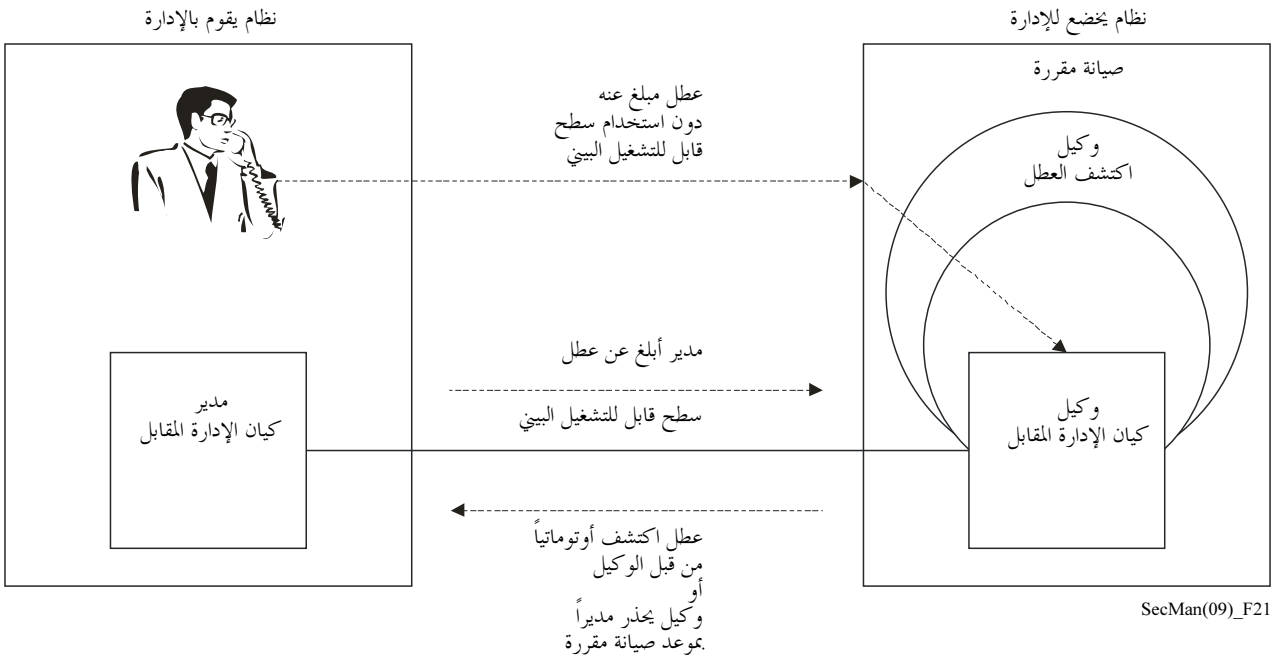


الشكل 21 – إدارة حالات الاحتيال في الخدمات اللاسلكية

5.7 تأمين التطبيقات القائمة على الشبكة

يقابل تقاطع مستوي الإدارة وطبقة التطبيق في توصية قطاع تقييس الاتصالات X.805، تأمين تطبيقات المستعمل النهائي القائمة على الشبكة. ويتضمن ذلك تطبيقات مثل إرسال الرسائل وتنظيم الدليل. والنوع الآخر من التطبيقات التي يجري فيها تأمين أنشطة الإدارة هو نوع تطبيقات الإدارة نفسها. ومن الأفضل شرح ذلك باستخدام الأمثلة. فالمستعملون النهائيون لهذه التطبيقات هم موظفو (عمليات) الإدارة لدى مقدم الخدمة. ولننظر في حالة مقدم خدمات يستخدم خدمات توصيل يوفرها مقدم خدمات آخر من أجل توفير خدمة التوصيل من طرف إلى طرف. وتبعاً للبيئة التنظيمية أو بيئة السوق، قد يوفر بعض مقدمي الخدمات خدمات نفاذ، بينما يوفر مقدمو خدمات آخرون، يشار إليهم باسم *الشركات الناقلة فيما بين البدالات*، توصيلية مسافات بعيدة. وتستأجر هذه الشركات خدمات نفاذ من مقدم خدمات محلي للحصول على توصيلية من طرف إلى طرف عبر مواقع موزعة جغرافياً. وعندما تتعطل خدمة ما، يستخدم تطبيق يسمى إدارة تقرير الأعطال للتبليغ عن المشكلة. ويتطلب مستعمل هذه الأنظمة وكذلك التطبيق نفسه تخويلاً للإبلاغ عن المشاكل. وينبغي للأنظمة المخول لها والمستعملين المخول لهم اتخاذ الإجراءات اللازمة لتدارك المشكلة أو المشاكل المبلغ عنها.

ويوضح الشكل 22 التفاعلات التي ينبغي تنفيذها بطريقة آمنة. وتُدار امتيازات النفاذ لمنع النفاذ غير المرخص به إلى تقارير الأعطال. ويسمح لمقدم الخدمة بالتبليغ فقط عن الأعطال في الخدمات التي يستأجرها وليس في الخدمات التي يستأجرها مقدم خدمة آخر.



الشكل 22 – وضع تقرير عن إدارة الأعطال

وتتضمن توصية قطاع تقييس الاتصالات X.790 ، بشأن *وظيفة إدارة الإشكالات في تطبيقات قطاع تقييس الاتصالات*، تعريف تطبيق الإدارة هذا وتستخدم آليات مثل قوائم التحكم في النفاذ والاستيقان المتبادل لتأمين الأنشطة.

6.7 الخدمات المشتركة في إدارة الأمن

تتعدد الخدمات المشتركة التي تُعتبر من أنشطة مستوي الإدارة X.805. وتطبق هذه الخدمات على وجه الخصوص لدى استخدام *بروتوكول معلومات الإدارة المشتركة (CMIP)* (توصية قطاع تقييس الاتصالات X.711). وفيما يلي أدناه وصف موجز للخدمات الواردة في هاتين التوصيتين.

1.6.7 وظيفة الإبلاغ عن إنذار أمن

الإبلاغ عن إنذار عموماً وظيفة أساسية في السطوح البينية للإدارة. وعندما يُكشف عطل ناتج من إشكالات تشغيلية (عطل في رزمة الدارة) أو من انتهاك لسياسة الأمن يبلّغ عن إنذار إلى النظام القائم بالإدارة. ويحتوي بلاغ الإنذار على عدد من المعلمات بحيث يتمكن النظام القائم بالإدارة من معرفة سبب العطل واتخاذ تدابير تصحيحية. وتشمل معلمات أي حدث حقلاً إلزامياً يدعى *نمط الحدث* ومجموعة من الحقول الأخرى تشمل *معلومات الحدث*. وتتألف هذه المجموعة من معلومات تتناول مثلاً حدة الإنذار والأسباب المحتملة للإنذار وكاشف انتهاك الأمن. وأسباب الإنذار مرتبطة بأنماط الأحداث كما هو مبين في الجدول 6.

الجدول 6 – أسباب إنذار الأمن

نمط الحدث	أسباب إنذار الأمن
انتهاك السلامة	معلومات مزدوجة معلومات ناقصة كشف عن تعديل معلومات معلومات في غير ترتيبها معلومات غير متوقعة
انتهاك التشغيل	رفض الخدمة تعطل الخدمة خطأ إجرائي سبب غير محدد
انتهاك مادي	تلاعب في الكبل كشف دخيل سبب غير محدد
انتهاك خدمة أمن أو آلية أمن	فشل الاستيقان انتهاك السرية فشل عدم التنصل محاولة نفاذ غير مرخص به سبب غير محدد
انتهاك ميدان زمني	معلومات متأخرة مفتاح انتهت صلاحيته نشاط خارج الساعات المحددة

وأسباب الإنذار هذه موضحة بشكل أوفى في توصية قطاع تقييس الاتصالات X.736 بشأن *وظيفة الإبلاغ عن إنذار أمن*.

2.6.7 وظيفة تعقب التدقيق الأمني

يُستعمل تعقب التدقيق الأمني لتسجيل الأحداث المتعلقة بالأمن، ولا سيما منها انتهاكات الأمن. ويمكن لهذه الأحداث أن تشمل عمليات الوصل والقطع واستعمالات آليات الأمن وعمليات الإدارة ومحاسبة الاستعمال. وتحدد توصية قطاع تقييس الاتصالات X.740 *وظيفة تعقب التدقيق الأمني*.

3.6.7 التحكم في النفاذ للكيانات الخاضعة للإدارة

تتضمن توصية قطاع تقييس الاتصالات X.741 بشأن *أشياء ونعوت التحكم في النفاذ* وصفاً مفصلاً للنموذج المرتبط بتخصيص التحكم في النفاذ لمختلف الكيانات التي تخضع للإدارة. ومن المتطلبات التي تلبيها هذه التوصية حماية معلومات الإدارة من استحداث أو حذف أو تعديل غير مرخص به، ضامنةً اتساق العمليات مع حقوق النفاذ التي يتمتع بها مستهلو العمليات، ومانعةً إرسال معلومات الإدارة إلى جهات غير مرخص لها بذلك. وثمة سويات مختلفة من التحكم في النفاذ معرّفة من أجل الوفاء بهذه المتطلبات. وبالنسبة إلى عمليات الإدارة، يمكن تطبيق قيود النفاذ في سويات متعددة. ويمكن أن تستند سياسة التحكم في النفاذ إلى واحد أو أكثر من المخططات المحددة (مثل قوائم التحكم في النفاذ؛ والتحكم في النفاذ على أساس

المقدرة أو الوسم أو السياق). وفي نموذج توصية قطاع تقييس الاتصالات X.741، يستند قرار السماح بالنفاذ أو منعه إلى السياسة ومعلومات التحكم في النفاذ (ACI) التي تشمل مثلاً القواعد وهوية الجهة التي تستهل العملية وهويات الجهات المقصودة المطلوب النفاذ إليها والمعلومات المتصلة بالاستيقان من الجهة مستهلة العملية.

4.6.7 خدمات الأمن القائمة على أساس معمارية وسيط مشترك لطلب غرض (CORBA)

لئن افترضت توصيات عديدة من السلسلة X.700 استخدام بروتوكول معلومات الإدارة المشتركة (CMIP) بوصفه بروتوكول السطح البيني للإدارة فإن هناك الآن اتجاهات أخرى تنعكس في هذه التوصيات. وهي تشمل استخدام بروتوكول يقوم على أساس معمارية وسيط مشترك لطلب غرض وما يتصل بها من خدمات ونماذج أغراض للسطوح البينية للإدارة. وجدير بالذكر من بين توصيات قطاع تقييس الاتصالات هذه، التوصية X.780 بعنوان: *المبادئ التوجيهية لشبكة إدارة الاتصالات في تعريف الأغراض التي تديرها معمارية CORBA*؛ والتوصية X.780.1 بعنوان: *المبادئ التوجيهية لشبكة إدارة الاتصالات في تعريف الأغراض ذات التفاصيل العامة التي تديرها معمارية CORBA*؛ والتوصية X.780.2 بعنوان: *المبادئ التوجيهية لشبكة إدارة الاتصالات في تعريف الأغراض ذات التوجه الخدمي التي تديرها معمارية CORBA* وفي تعريف أغراض الواجهة؛ والتوصية X.781 بعنوان: *المتطلبات والمبادئ التوجيهية لقوالب بيانات مطابقة التنفيذ المرتبطة بالأنظمة القائمة على معمارية CORBA*. وذلك إضافة إلى توصية قطاع تقييس الاتصالات Q.816 التي تحدد إطاراً لاستعمال هذه الخدمات في سياق السطوح البينية للإدارة. وللقيام بمتطلبات الأمن لهذه السطوح البينية فإن هذه التوصية تشير إلى المواصفة التي وضعها فريق إدارة الأغراض (OMG) للخدمات المشتركة من أجل الأمن.

8. بعض النُّهُج المحددة في أمن الشبكات

8 بعض النُّهُج المحددة في أمن الشبكات

تُستعرض في هذا القسم نُهُج لحماية أنماط مختلفة من الشبكات. ويُستهل القسم بنظرة على المتطلبات الأمنية لشبكات الجيل التالي. ويلي ذلك استعراض لشبكات الاتصالات المتنقلة التي تمر بمرحلة انتقالية من التنقل على أساس تكنولوجيا واحدة (مثل النفاذ المتعدد بتقسيم شفري (CDMA) أو النظام العالمي للاتصالات المتنقلة (GSM)) للتنقل عبر منصات غير متجانسة باستخدام بروتوكول الإنترنت. وبعد ذلك، تجري دراسة الشبكات المنـــزلية والتلفزيون الكبلي. وأخيراً، تعرض تحديات الأمن في شبكات الاستشعار الشمولي.

1.8 أمن شبكات الجيل التالي

شبكة الجيل التالي هي شبكة قائمة على الرزم تستطيع أن تقدم خدمات الاتصالات إلى المستعملين وبوسعها الاستفادة من نطاقات عريضة متعددة ومن تكنولوجيات النقل المفعلة بجودة الخدمة. وبالإضافة إلى ذلك، فإن وظائف الخدمة ذات الصلة مستقلة عن التكنولوجيات الأساسية المتصلة بالنقل. وتمكّن شبكات الجيل التالي المستعمل من النفاذ غير المقيد إلى الشبكات وإلى المنافسين من مقدمي الخدمة ومن الخدمات. وهي تدعم التنقلية المعممة التي تسمح بتقديم خدمات إلى المستعملين على نحو ثابت في كل مكان. وترد تفاصيل أوفى عن الخصائص العامة لشبكات الجيل التالي في توصية قطاع تقييس الاتصالات Y.2001 بعنوان نظرة عامة على شبكات الجيل التالي.

1.1.8 أهداف ومتطلبات أمن شبكات الجيل التالي

إذ يبرز الأمن كإحدى السمات المميزة لشبكات الجيل التالي، لا بد من وضع مجموعة من المعايير تضمن أمن شبكات الجيل التالي إلى أقصى درجة ممكنة. وإذ تتطور شبكات الجيل التالي، تظهر ثغرات أمنية جديدة لا يُعرف لها علاج فوري تلقائياً، لا مناص من توثيقها على الوجه الصحيح ليتمكن مديرو الشبكة والمستعملون النهائيون من الحد من آثارها.

وعلى دراسات الأمن في شبكة الجيل التالي أن تتناول معماريات الشبكة وتطورها بحيث تحقق ما يلي:

- توفر الحماية القصوى للشبكة وموارد المستعمل النهائي؛
- تتيح درجة عالية من الحوسبة اللامركزية الموزعة من طرف إلى طرف؛
- تتيح التعايش بين تقنيات متعددة للربط الشبكي؛
- توفر آليات الأمن من طرف إلى طرف؛
- توفر حلولاً أمنية تسري على ميادين إدارية متعددة؛
- توفر إدارة آمنة للهوية تشمل ما يلي، دون أن تقتصر على:
  - استيقان موثوق من الكيانات في شبكات الجيل التالي (مثل المستعملين وأجهزتهم ومقدمي الشبكة ومقدمي الخدمة ومقدمي الهوية وغيرهم)؛
  - منع النفاذ غير المصرح به إلى بيانات الهوية في شبكات الجيل التالي، والتبادل الآمن لمعلومات الهوية بين الكيانات؛
  - أمن تبادل معلومات الهويات بين الكيانات المتحدة في شبكات الجيل التالي؛
  - دعم الاحتفاظ بسجلات استعمال معلومات الهويات في شبكات الجيل التالي؛
  - ضمان الخصوصية للمستعملين وإغفال هويتهم في شبكات الجيل التالي؛

– توفير القدرة لمستعملي شبكات الجيل التالي على إدارة معلومات هوياتهم بصورة آمنة (مثل تعديل صفات المستعمل وتغيير كلمات المرور وباستعمال خدمات تحديد المواقع والاطلاع على سجلات الحسابات وغيرها).

- وتوفر حلولاً أمنية لخدمة التلفزيون القائم على بروتوكول الإنترنت (IPTV) بحيث تكون فعالة التكاليف ذات التأثير المقبول على الأداء ونوعية الخدمة وإمكانية الاستعمال والتوسيع. وتضم أنواع الحماية التي ينبغي أن تتوفر في أمن خدمة التلفزيون القائم على بروتوكول الإنترنت (IPTV) البنود التالية دون أن تقتصر عليها:

– حماية المحتوى؛

– حماية الخدمة؛

– حماية الشبكة؛

– حماية المطراف؛

– حماية المشترك.

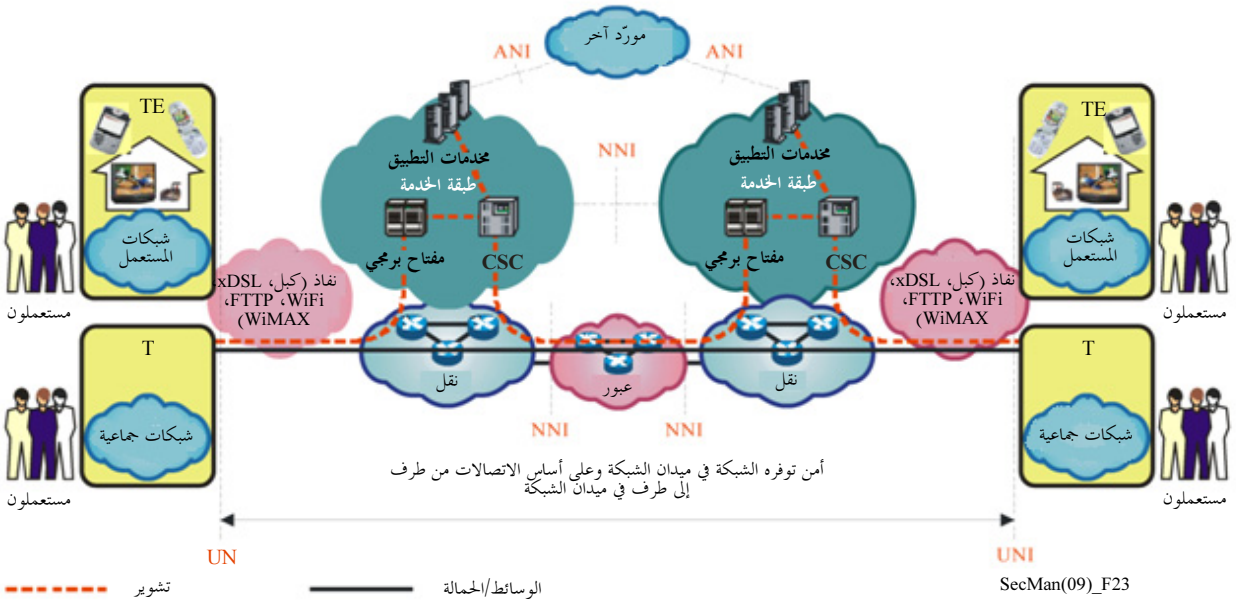
أما توصية قطاع تقييس الاتصالات Y.2701 بعنوان *متطلبات أمن شبكة الجيل التالي – الإصدار الأول*، فهي تستند إلى مبادئ توصية قطاع تقييس الاتصالات X.805، وتوصّف المتطلبات الأمنية لحماية شبكات الجيل التالي ضد التهديدات الأمنية، وتغطي بعض الجوانب التقنية لإدارة الهوية.

ويجب حماية العناصر التالية في بيئة متعددة الشبكات:

- البنية التحتية للشبكة ولمقدم الخدمة وما يخصهما من الأصول (مثل أصول وموارد شبكة الجيل التالي من قبيل عناصر الشبكة والأنظمة والمكونات والسطوح البينية والبيانات والمعلومات) والخدمات؛
- خدمات شبكات الجيل التالي وقدراتها (مثل خدمات الصوت والفيديو والبيانات)؛
- اتصالات المستعمل النهائي والمعلومات عنه (المعلومات الخاصة مثلاً).

ويجب أن توفر المتطلبات أمنَ اتصالات المستعمل النهائي المستند إلى الشبكة عبر الميادين الإدارية لشبكات متعددة على النحو المبيّن في الشكل 23.

وتعتبر المتطلبات المحددة في توصية قطاع تقييس الاتصالات Y.2701 مجموعة الحد الأدنى من المتطلبات. وقد يحتاج مقدم شبكة الجيل التالي إلى اتخاذ تدابير إضافية غير تلك المحددة.



الشكل 23 – أمن الاتصالات عبر شبكات متعددة

2.8 أمن الاتصالات المتنقلة

تتطور الاتصالات المتنقلة من التنقلية المحصورة بتكنولوجيا معينة (مثل النظام العالمي للاتصالات المتنقلة (GSM) أو النفاذ المتعدد بتقسيم شفري (CDMA)) إلى تنقلية عابرة لشبكات غير متجانسة (مثل شبكات النظام العالمي للاتصالات المتنقلة (GSM) والأمانة اللاسلكية (Wi-Fi) والشبكة الهاتفية العمومية التبديلية (PSTN)) مع استعمال بروتوكول الإنترنت. وبعبارة أخرى ، فإن شبكات المستقبل تنطوي على التكامل بين الشبكات اللاسلكية والسلكية التي تقدم مجموعة واسعة من الخدمات الجديدة التي لا يمكن أن توفرها شبكة قائمة واحدة.

وإذ يُنشر التقارب بين الاتصالات الثابتة والاتصالات المتنقلة (FMC)، يمكن لمستعمل الاتصالات المتنقلة أن يتجول عبر شبكات غير متجانسة مثل النظام العالمي للاتصالات المتنقلة (GSM) والشبكة المحلية (LAN) اللاسلكية والبلوتوث. وسيتعين تلبية المتطلبات الأمنية لكل نمط من أنماط النفاذ بسبل مختلفة، ولكن يجب أن تلبى جميع المتطلبات الأمنية لحماية المستعملين والشبكات والتطبيقات التي يجري النفاذ إليها.

ويمكن تصنيف قضايا الأمن عموماً على النحو التالي:

- القضايا الناشئة عن استعمال بروتوكول الإنترنت في الاتصالات اللاسلكية المتنقلة؛
- القضايا الناشئة عن استعمال عدة شبكات ذات تكنولوجيات متعددة.

ومن شأن هجمات ونقاط الضعف الإنترنت أن تهدد شبكات الاتصالات المتنقلة اللاسلكية التي تستعمل بروتوكول الإنترنت كبروتوكول النقل فيها. وبالإضافة إلى ذلك، ستظهر تهديدات جديد للأنظمة اللاسلكية القائمة على بروتوكول الإنترنت جراء طبيعة الشبكات اللاسلكية نفسها، أي طبيعتها التنقلية. وقد لا تلبي آليات الأمن التي سبق وضعها جميع الاحتياجات الأمنية للأنظمة اللاسلكية القائمة على بروتوكول الإنترنت. ومن ثم، قد يتعين إعداد إجراءات أمن جديدة أو معززة لبروتوكول الإنترنت. ولا بد أيضاً ألا يقتصر تناول الأمن على السطح البيني الراديوي، بل يشمل كامل الخدمة من طرف إلى طرف وأن يكون مرناً بما يكفي ليوفر مستويات متنوعة من الأمن الملائم للخدمات/التطبيقات المقدمة. وإذ تُنشر خدمات وتطبيقات بروتوكول الإنترنت المتنقلة، تزداد أهمية التدابير الأمنية للمستعمل والمشغّل ومقدم الخدمة.

وتستفحل فرص التهديدات بفعل مشاركة شبكات متعددة، ومن هذه الفرص الاعتراض غير القانوني للملامح العامة لمستعمل، وللمحتوى (مثل اتصالات الصوت أو البيانات) ولمعلومات الاستيقان.

الاتصالات المتنقلة الدولية-2000 (IMT - 2000) هي معيار عالمي للجيل الثالث (3G) للاتصالات اللاسلكية. ويرد تعريفها في مجموعة من التوصيات المترابطة لقطاع تقييس الاتصالات. وتوفر الاتصالات المتنقلة الدولية-2000 إطاراً للنفاذ اللاسلكي في جميع أنحاء العالم بتوصيل أنظمة متنوعة لشبكات قائمة على محطات أرضية و/أو ساتلية. وسوف تستفيد من التآزر المحتمل بين أنظمة وتكنولوجيات الاتصالات الرقمية وبين أنظمة النفاذ اللاسلكي للاتصالات الثابتة والمتنقلة.

وتشمل أنشطة الاتحاد الدولي للاتصالات بشأن الاتصالات المتنقلة الدولية-2000 (IMT - 2000) التقييس الدولي، بما في ذلك الطيف الترددي والمواصفات التقنية للمكونات الراديوية والشبكية، وللتعريفات والفوترة، والمساعدة التقنية والدراسات حول الجوانب التنظيمية والسياساتية.

وتغطى المتطلبات العامة لتحقيق الأمن في شبكات الاتصالات المتنقلة الدولية-2000 (IMT - 2000) في توصية قطاع تقييس الاتصالات Q.1701 بعنوان: *إطار شبكات الاتصالات المتنقلة الدولية-2000*، وتوصية قطاع تقييس الاتصالات Q.1702 بعنوان: *رؤية طويلة الأجل لجوانب الشبكة في أنظمة الاتصالات المتنقلة الدولية ما بعد عام 2000*، وتوصية

قطاع تقييس الاتصالات Q.1703 بعنوان: *إطار قدرات الخدمة والشبكة لجوانب الشبكة في أنظمة الاتصالات المتنقلة الدولية ما بعد عام 2000*.

أضف إلى ذلك، مواصفات الجيل الثالث (3G) الواردة في سلسلة توصيات قطاع تقييس الاتصالات Q.1741 (3GPP) وفي سلسلة توصيات قطاع تقييس الاتصالات Q.1742 (3GPP2)، وهي تحوي تقييماً للتهديدات المتصورة، وقائمة من المتطلبات الأمنية للتصدي لهذه التهديدات. كما تحتوي هذه التوصيات على أهداف ومبادئ أمن الاتصالات المتنقلة، ومعمارية أمن محددة، ومتطلبات خوارزمية التجفير، ومتطلبات الاعتراض القانوني، ومعمارية الاعتراض القانوني ووظائفه.

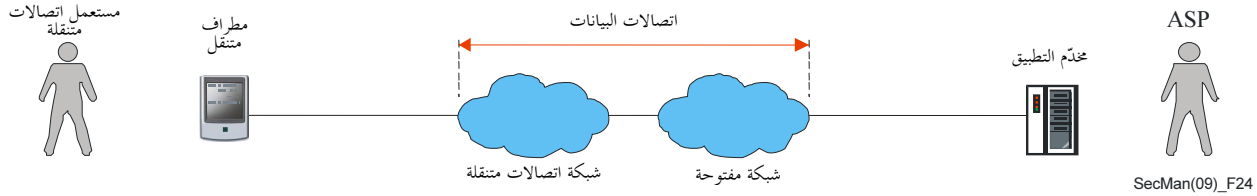
1.2.8 اتصالات بيانات متنقلة آمنة من طرف إلى طرف

تتوفر المطاريف المتنقلة التي تنطوي على مقدرات اتصالات البيانات (ومنها الهواتف المتنقلة في نظام IMT-2000 والحواسب الشخصية المحمولة والمساعدات الرقمية المحمولة المجهزة ببطاقة راديوية) على نطاق واسع وتستعمل خدمات مختلف التطبيقات (ومنها مثلاً التجارة الإلكترونية) المطاريف الموصولة بشبكة الاتصالات المتنقلة. وتُعتبر فعالية الأمن أمراً أساسياً لتطبيقات الأعمال، وكذلك لحماية المستعمل النهائي.

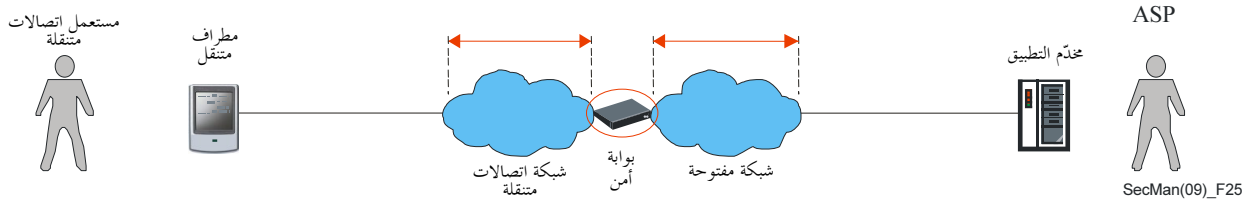
وتعود مواطن الضعف في شبكات الاتصالات المتنقلة بوجه خاص إلى طبيعة الشبكة اللاسلكية ونقاط الضعف الكامنة في تكنولوجيا الاتصالات اللاسلكية. ويجب النظر إلى الأمن من وجهة نظر مشغل شبكة الاتصالات المتنقلة ومقدم خدمات التطبيقات والمستعمل النهائي. ويحظى بأهمية خاصة. وقد وضع قطاع تقييس الاتصالات مجموعة كاملة من الحلول الأمنية لمعالجة الاتصالات المتنقلة من طرف إلى طرف، ويرد بحث بعضها أدناه.

1.1.2.8 إطار لاتصالات البيانات المتنقلة من طرف إلى طرف

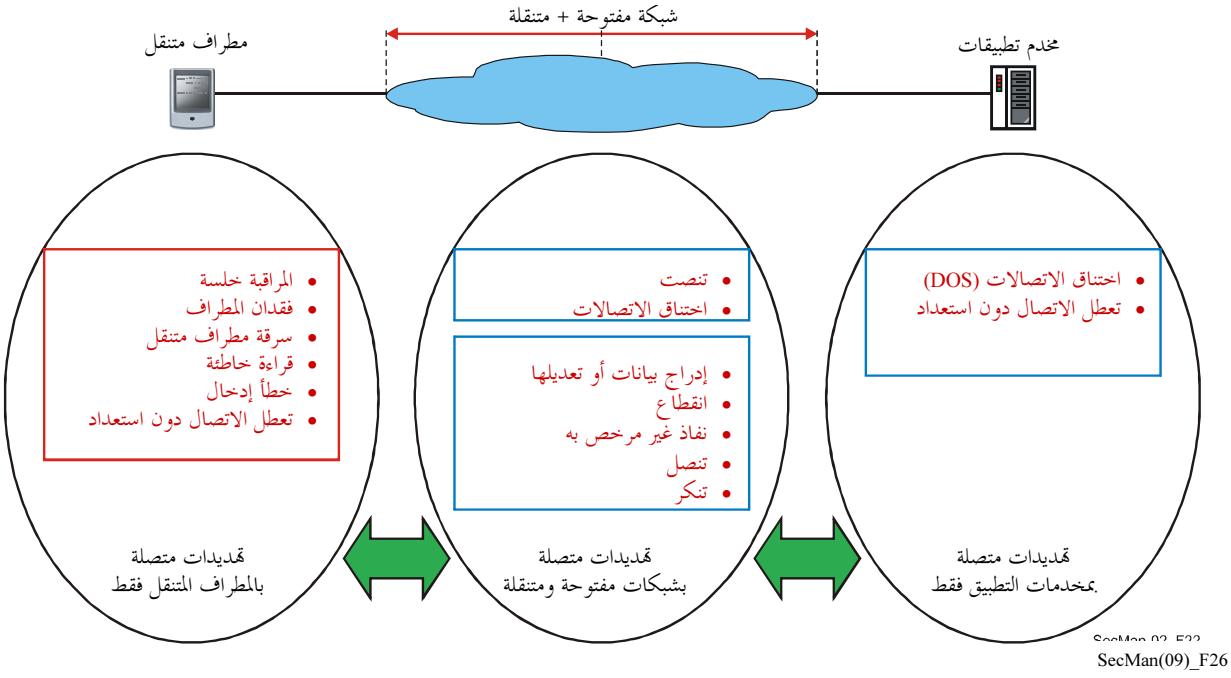
في توصية قطاع تقييس الاتصالات X.1121 بعنوان: إطار تكنولوجيات الأمن لاتصالات البيانات المتنقلة من طرف إلى طرف، يرد وصف لنموذجين لاتصالات البيانات المتنقلة من طرف إلى طرف بين مستعمل متنقل ومقدم خدمات تطبيقات (ASP) وهما: نموذج عام ونموذج بوابة، على النحو الموضح في الشكلين 24 و25. ويقوم مقدم خدمات تطبيقات بتوفير خدمة متنقلة إلى المستعملين المتنقلين من خلال مخدم التطبيقات. وفي نموذج البوابة، تقوم بوابة الأمن المتنقلة بترحيل الرزم من المطراف المتنقل إلى مخدم التطبيقات، وتقوم بتحويل بروتوكول اتصالات متنقلة قائم على شبكة إلى بروتوكول مفتوح قائم على شبكة، والعكس بالعكس. ويصور الشكل 26 التهديدات في شبكة لاتصالات البيانات المتنقلة من طرف إلى طرف، أما الشكل 27 فيبين الأماكن التي تتطلب ميزات الأمن لكل كيان والعلاقة بين الكيانات.



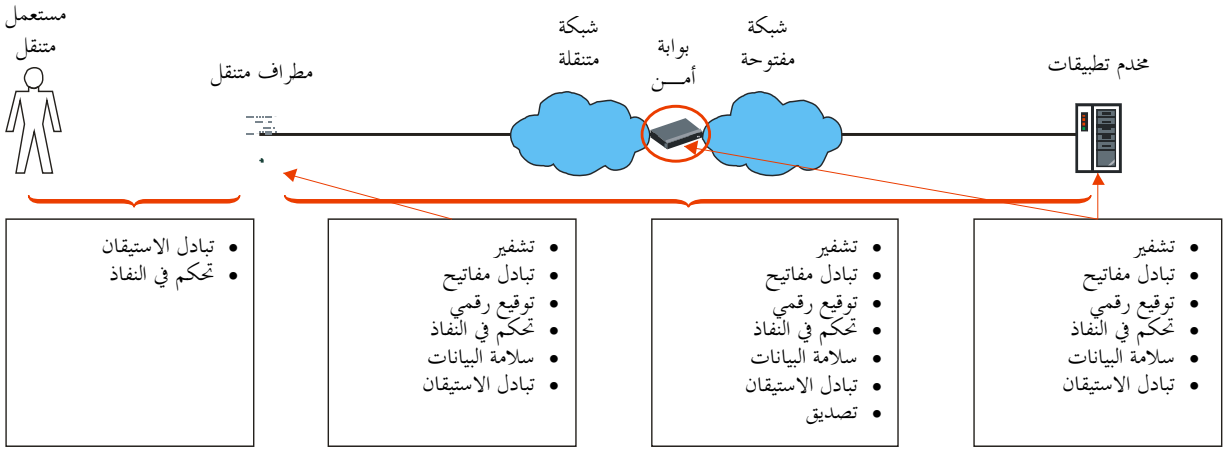
الشكل 24 – نموذج عام لاتصالات البيانات المتنقلة من طرف إلى طرف بين مستعمل ومقدم خدمات تطبيقات (ASP)



الشكل 25 – نموذج بوابة لاتصالات البيانات المتنقلة من طرف إلى طرف بين مستعمل متنقل ومقدم خدمات تطبيقات (ASP)



الشكل 26 – التهديدات في الاتصالات المتنقلة من طرف إلى طرف



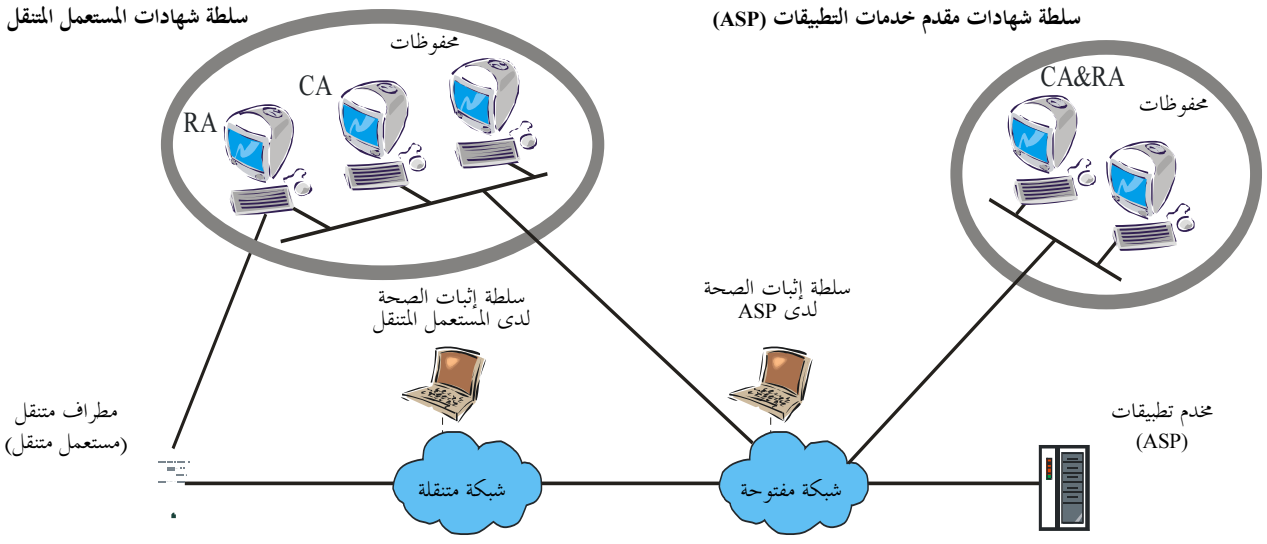
SecMan(09)_F27

الشكل 27 – وظيفة الأمن المطلوبة لكل كيان والعلاقة بين الكيانات

2.1.2.8 البنية التحتية للمفاتيح العمومية (PKI) من أجل اتصالات بيانات متنقلة آمنة من طرف إلى طرف

يستفاد من البنية التحتية للمفاتيح العمومية (PKI) كثيراً لتوفير بعض الوظائف الأمنية (مثل السرية والتوقيع الرقمي وسلامة البيانات) اللازمة لاتصالات بيانات متنقلة من طرف إلى طرف. ولكن خصائص اتصالات البيانات المتنقلة تتطلب بعض التكييف. وترد بعض التوجيهات بشأن تنفيذ البنية التحتية للمفاتيح العمومية في بيئة متنقلة في توصية قطاع تقييس الاتصالات X.1122 بعنوان: *المبدأ التوجيهي لتنفيذ الأنظمة المتنقلة الآمنة على أساس البنية التحتية للمفاتيح العمومية*. وتقدم التوصية كل من النموذج العام للبنية التحتية للمفاتيح العمومية ونموذج البوابة للبنية التحتية للمفاتيح العمومية.

وفي النموذج العام (الموضح في الشكل 28) تصدر سلطة الشهادات (CA) لدى المستعمل المتنقل شهادة لذلك المستعمل وتقوم بإدارة مكان المحفوظات وقائمة إبطال الشهادات (CRL). وتوفر سلطة إثبات الصحة لدى المستعمل المتنقل خدمة إثبات صحة شهادات على الخط لذلك المستعمل. وتصدر سلطة الشهادات (CA) لدى مقدم خدمات التطبيقات (ASP) شهادة وتقوم بإدارة ما يخص ذلك المقدم من مكان المحفوظات وقائمة إبطال الشهادات.وتوفر سلطة إثبات الصحة لدى المقدم (ASP) خدمة إثبات صحة شهادات على الخط.

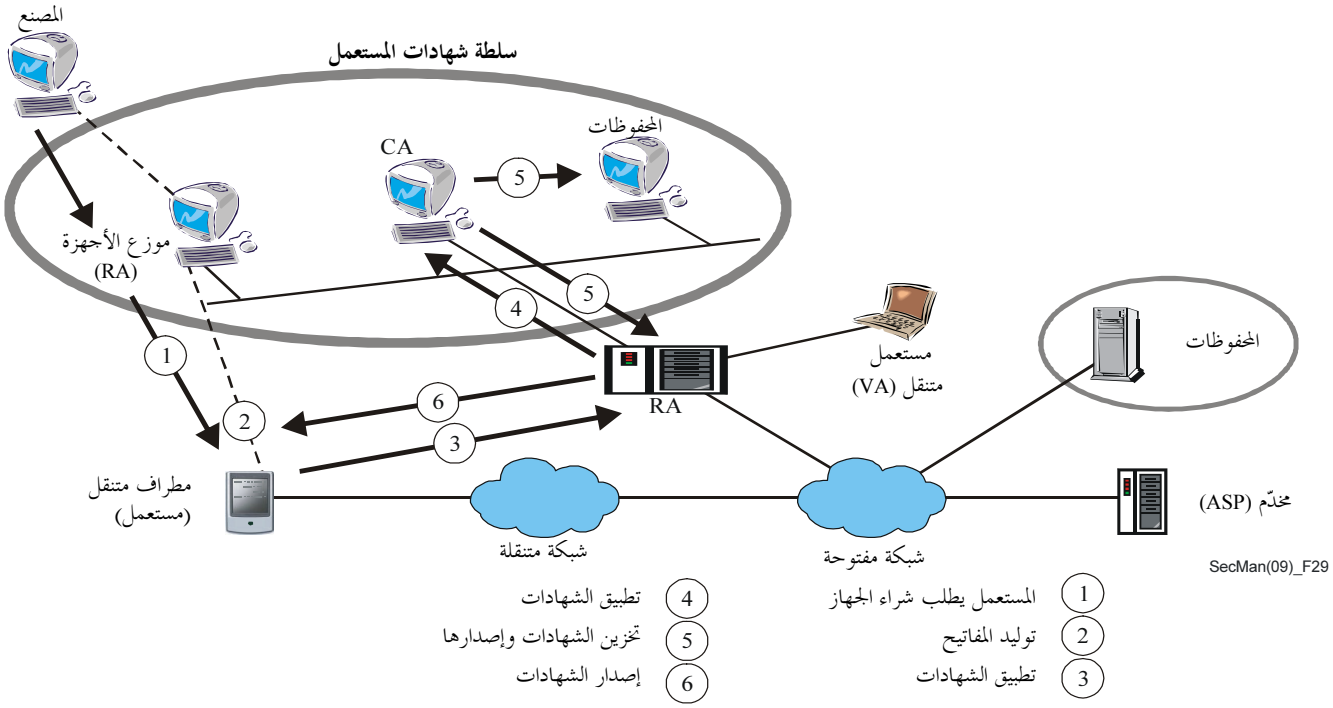


SecMan(09)_F28

الشكل 28 – نموذج PKI عام لاتصالات بيانات متنقلة من طرف إلى طرف

هنالك طريقتان لإصدار الشهادات تبعاً للموقع الذي يتولد فيه المفتاح العمومي/الخاص. في الطريقة الأولى يتولد زوج المفاتيح المجفرة ويستحدث في مصنع المطراف المتنقل، أما في الطريقة الثانية فيتولد زوج المفاتيح المجفرة في المطراف المتنقل أو في العلامة المصونة من التلاعب المتصلة بالمطراف المتنقل.

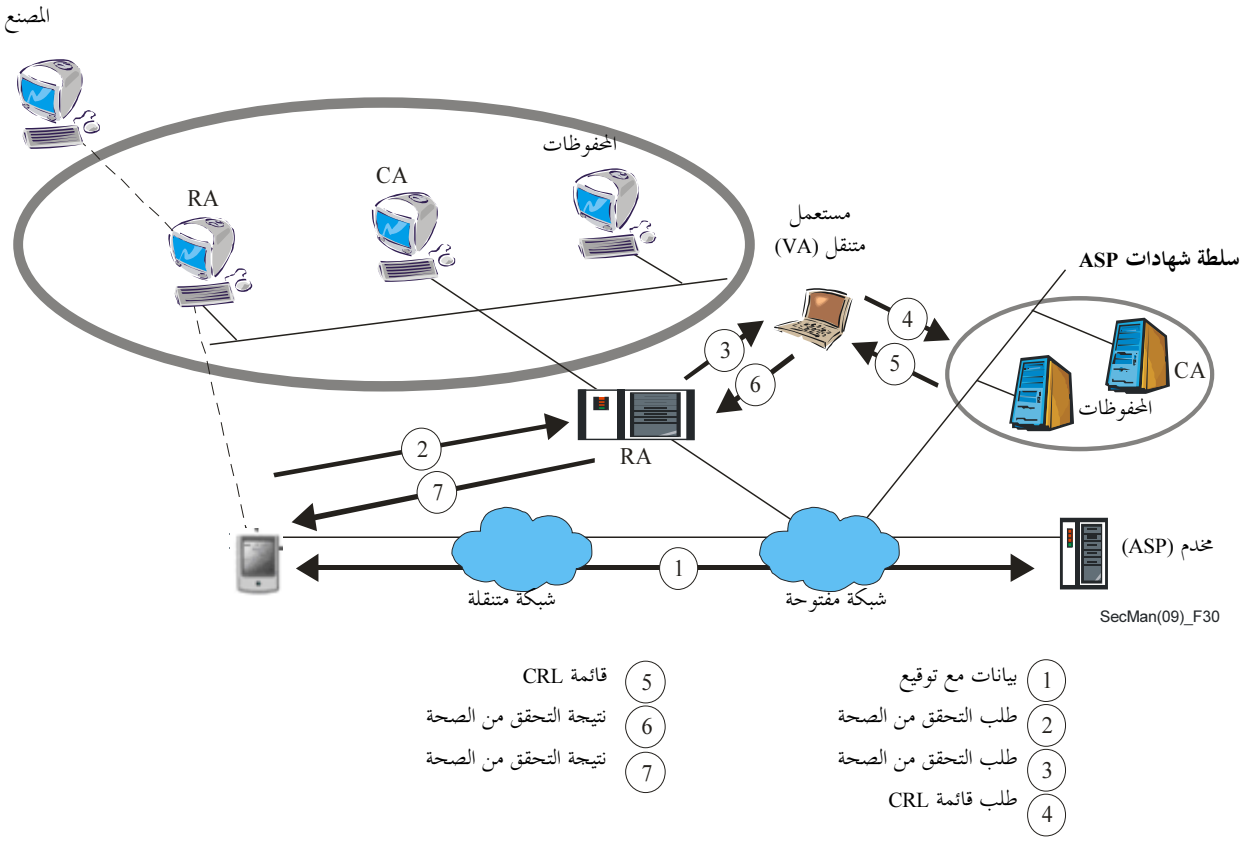
ويبين الشكل 29 الإجراءات التي يتّبعها المطراف المتنقل للحصول على شهادة، حيث يتولد زوج المفاتيح المجفرة في المطراف المتنقل.



الشكل 29 – إجراءات إصدار الشهادات للمطراف المتنقل

يتمتع المطراف المتنقل بقدرة حوسبة محدودة وذاكرة محدودة. ونتيجة لذلك يُفضل إثبات صحة الشهادات على الخط على إثبات صحة الشهادات خارج الخط الذي يقوم على أساس قائمة إبطال الشهادات (CRL).

ويصور الشكل 30 إجراء إثبات صحة الشهادات على الخط لمطراف متنقل.



الشكل 30 – إثبات صحة الشهادات من أجل اتصالات البيانات المتنقلة من طرف إلى طرف

ويمكن استعمال البنية التحتية للمفاتيح العمومية للاتصالات المتنقلة من طرف إلى طرف إما في طبقة الدورة، حيث يمكنها دعم خدمات أمن من قبيل الاستيقان من الزبون، والاستيقان من المخدم، وخدمة السرية والسلامة؛ أو في التطبيق حيث يمكن أن توفر خدمات عدم التنصل والسرية.

3.1.2.8 نظام ترابطي تفاعلي لاتصالات البيانات المتنقلة

ابتُكر النظام الترابطي التفاعلي لتمكين التعاون المشترك ما بين المطاريف أو الأجهزة المتنقلة والشبكة ضد التهديدات الأمنية. وتصف توصية قطاع تقييس الاتصالات X.1125 معمارية تنوعية لنظام ترابطي تفاعلي يمكن فيها التعاون التفاعلي ما بين شبكة اتصالات متنقلة ومطاريف مستعمليها لمكافحة التهديدات الأمنية المختلفة وتأمين اتصالات البيانات من طرف إلى طرف. وتشمل تلك التهديدات، على سبيل المثال، الفيروسات أو الديدان أو أحصنة طروادة أو التهديدات الشبكية الأخرى ضد شبكة الاتصالات المتنقلة ومستعمليها على السواء.

وتزوّد هذه المعمارية شبكات المشغلين بقدرة أمن معززة من خلال التحديثات الأمنية للمحطات المتنقلة والتحكم في النفاذ إلى الشبكة والقيود على خدمة التطبيق. وينتج عن ذلك آلية تحول دول التفشي السريع للفيروسات أو الديدان عبر شبكة المشغّل.

3.8 الأمن للشبكات المنـــزلية

بما أن الشبكة المنـــزلية تستعمل مختلف تقنيات الإرسال السلكية واللاسلكية، فهي تتعرض لتهديدات مماثلة لتلك التي تتعرض لها أية شبكة أخرى سلكية أو لا سلكية. ولحماية الشبكة المنـــزلية من هذه التهديدات، وضع قطاع تقييس الاتصالات مجموعة شاملة من الحلول لخدمات الشبكة المنـــزلية، ويرد بحث بعضها أدناه.

1.3.8 إطار الأمن للشبكة المنـــزلية

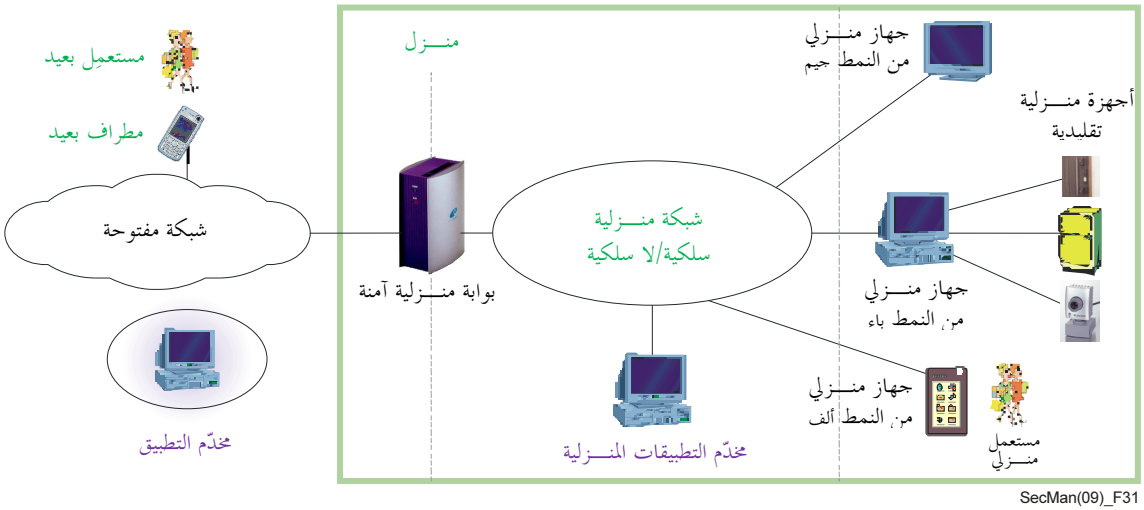
توصية قطاع تقييس الاتصالات X.1111 بعنوان: *إطار تكنولوجيات الأمن للشبكة المنـــزلية، تبني على نموذج التهديد* الوارد في توصية قطاع تقييس الاتصالات X.1121 لتؤسس إطار أمن للربط الشبكي المنـــزلي. ويمكن تلخيص خصائص الشبكة المنـــزلية على النحو التالي:

- يمكن استعمال مختلف وسائط الإرسال في الشبكة؛
- قد تشمل الشبكة تكنولوجيات سلكية و/أو لاسلكية؛
- تتعدد البيئات المحتملة التي يجب أخذها في الاعتبار من وجهة النظر الأمنية؛
- يمكن لمستعملين في مواقع نائية أن يحملوا في حلهم وترحالهم مطاريف بعيدة؛
- تتطلب الأنماط المتنوعة من أجهزة الشبكة المنـــزلية مستويات مختلفة من الأمن.

ويمكن للنموذج العام لأمن الشبكة المنـــزلية الظاهر في الشكل 31 أن يشمل العديد من الأجهزة مثل أجهزة المساعد الرقمي الشخصي وأجهزة الحاسوب وأجهزة التلفزيون/الفيديو. وفي هذا النموذج، تصنَّف الأجهزة المنـــزلية كأحد ثلاثة أنماط:

- أجهزة النمط ألف، مثل وحدات تحكم عن بعد أو أجهزة الحاسوب أو أجهزة المساعد الرقمي الشخصي، القادرة على التحكم في جهاز من النمط باء أو جيم؛
- وأجهزة النمط باء هي جسور توصل أجهزة النمط جيم (التي ليس لها سطح بيني للاتصالات) مع الشبكة، أي أن جهاز النمط باء يتصل بالأجهزة الأخرى في الشبكة بواسطة لغة خاضعة لملكية خاصة أو بواسطة آلية تحكم؛
- أجهزة النمط جيم، مثل كاميرات الأمن وأجهزة الصوت/الفيديو التي توفر الخدمة لباقي الأجهزة.

ومن الأجهزة ما يجمع وظائف النمط ألف والنمط جيم.



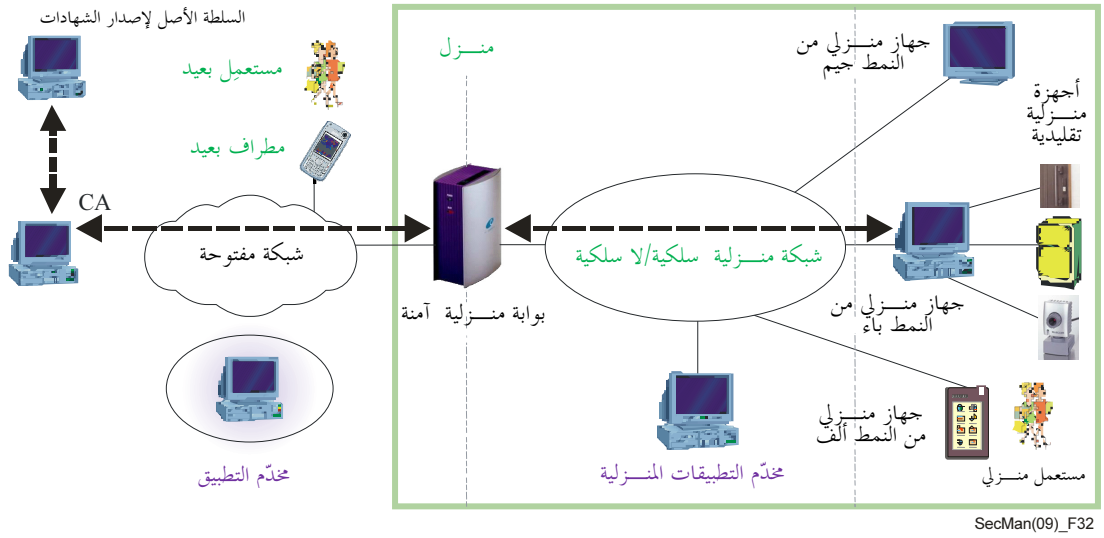
الشكل 31 – النموذج العام لأمن الشبكة المنـــزلية

وتصف توصية قطاع تقييس الاتصالات X.1111 التهديدات الأمنية ومتطلبات الأمن من وجهة نظر المستعملين المنـــزليين والمستعملين عن بُعد. وبالإضافة إلى ذلك، فإنها تصنف تكنولوجيات الأمن من حيث الوظائف التي تلبي متطلبات الأمن والموقع الذي يجب أن تطبق فيه التكنولوجيات الأمنية.

2.3.8 إصدار الشهادة للجهاز والاستيقان منه في الشبكات المنـــزلية

هناك خياران لإصدار شهادة لجهاز في الشبكة المنـــزلية: نموذج الإصدار الخارجي حيث تصدر سلطة شهادات (CA) خارجية جميع شهادات الأجهزة المنـــزلية؛ ونموذج الإصدار الداخلي حيث تصدر سلطة شهادات (CA) داخلية شهادات الأجهزة (بما في ذلك شهادات موقعة ذاتياً وشهادات كيان طرفي) في الشبكة المنـــزلية. وعادة ما تكون سلطة الشهادات الداخلية بوابة منـــزلية قادرة على توليد زوج مفاتيح وإصدار شهادة، أي يمكن للبوابة المنـــزلية أن تصدر شهادة السلطة (CA) وشهادات الأجهزة المنـــزلية على السواء. ويمكن لسلطة شهادات (CA) خارجية أن تصدر شهادة جهاز للبوابة المنـــزلية الآمنة نفسها لاستخدامها في الخدمات المنـــزلية الخارجية. ويمكن استخدام هذه الشهادة الصادرة من الخارج لجهاز البوابة المنـــزلية للاستيقان بين البوابة المنـــزلية ومقدم خدمة الشبكة.

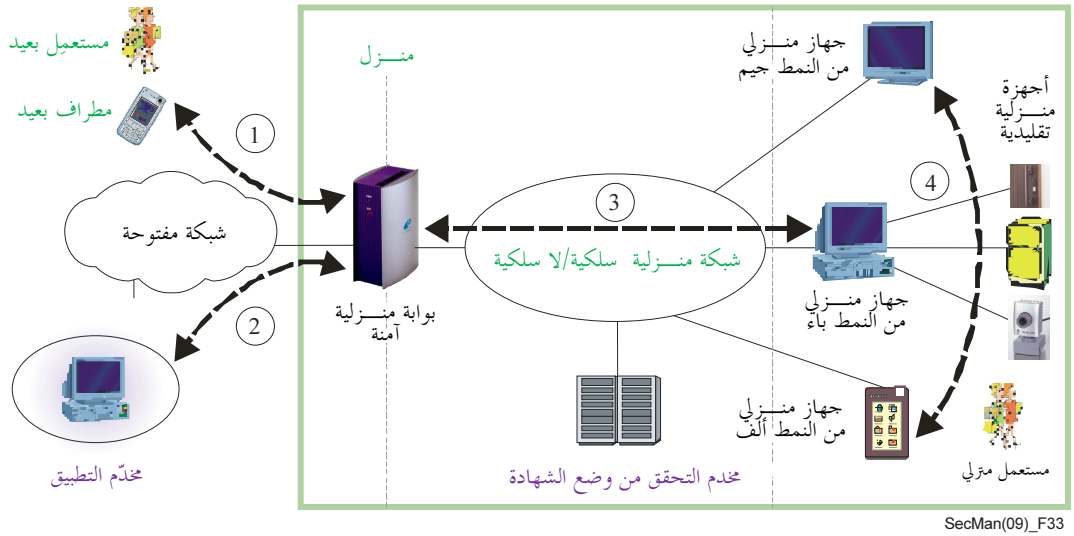
وتصف توصية قطاع تقييس الاتصالات X.1112 إطاراً لنموذج داخلي لإصدار شهادة لجهاز ولإدارة الشبكات المنـــزلية واستعمالها. ويُبيَّن هذا النموذج في الشكل 32.



الشكل 32 – نموذج الاستيقان من الجهاز للشبكة المنـــزلية الآمنة

للاستيقان من جهاز، يلزم معرّف ينفرد به كل جهاز في الشبكة المنـــزلية. وعلى وجه التحديد، ستلزم شهادة جهاز منـــزلي كعنصر ثقة ينفرد به ذلك الجهاز عند استعماله في الشبكة المنـــزلية.

ويبين الشكل 33 أربع حالات استعمال نمطية لشهادة جهاز: 1) بين المطراف البعيد والبوابة المنـــزلية الآمنة؛ 2) بين مخدّم التطبيق والبوابة المنـــزلية الآمنة؛ 3) بين الأجهزة المنـــزلية والبوابة المنـــزلية الآمنة؛ 4) بين الأجهزة المنـــزلية.



الشكل 33 – حالة استعمال الاستيقان من الجهاز استناداً إلى النموذج العام لأمن الشبكة المنـــزلية

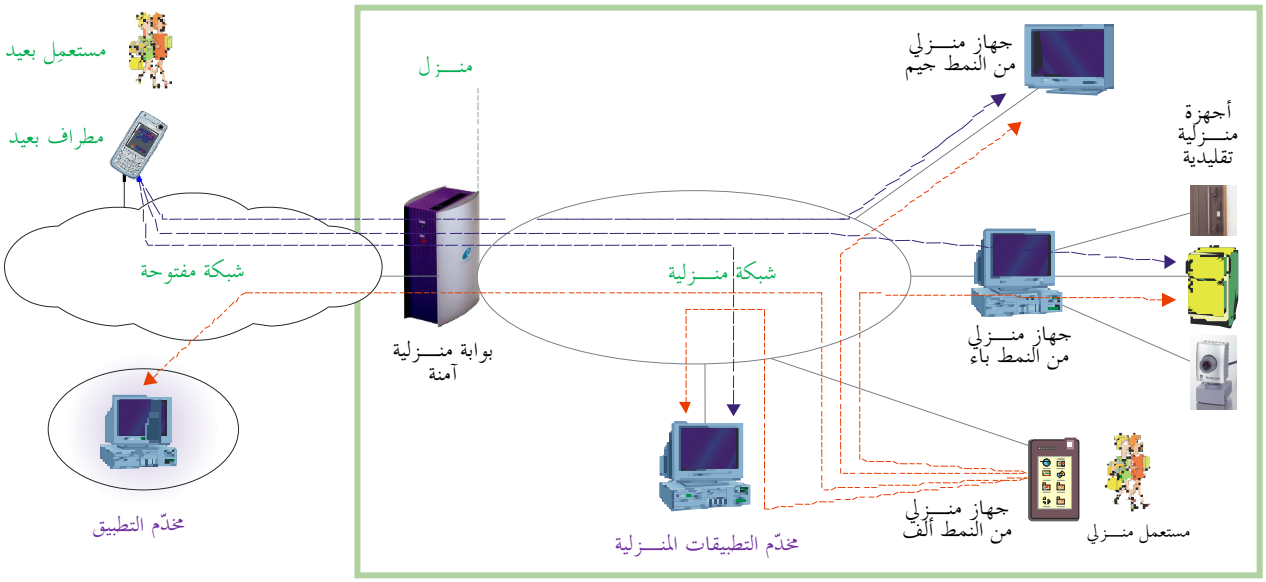
في خدمة الانترنت الخارجية من الجهاز المنـــزلي إلى مخدّم تطبيق خارجي، ينبغي الاستيقان من الجهاز المنـــزلي أولاً بواسطة البوابة المنـــزلية الآمنة باستعمال شهادة الجهاز نفسه. ثم ينبغي الاستيقان من البوابة المنـــزلية الآمنة بواسطة مخدّم التطبيق الخارجي باستعمال شهادة البوابة المنـــزلية الصادرة عن سلطة شهادات (CA) خارجية. ويمكن تطبيق حالات الاستعمال هذه على مختلف بروتوكولات التطبيق دعماً لخدمات آمنة في الشبكة المنـــزلية.

3.3.8 الاستيقان من مستعمل بشري لخدمات الشبكة المنـــزلية

تتطلب بعض البيئات الاستيقان من مستعمل بشري بدلاً من عملية أو جهاز. وفي هذه الحالات، يتطلب نظام الاستيقان من المستعملين البشريين إثبات ما يميزهم عن غيرهم. وتستند مثل هذه الفرادة عموماً إلى خصائص المستعمل مثل شيء يُعرف به أو شيء يملكه أو خاصية ما لا تتغير.

وتقدم توصية قطاع تقييس الاتصالات X.1113 توجيهات بشأن الاستيقان من مستعمل في الشبكة المنـــزلية لتمكّن من استعمال مختلف تقنيات الاستيقان مثل كلمات المرور والشهادات والاستدلال الأحيائي. كما تحدد مستوى ضمان الأمن ونموذج الاستيقان وفق سيناريوهات خدمة الاستيقان.

ويبين الشكل 34 انسيابات خدمة الاستيقان استناداً إلى النموذج العام لأمن الشبكة المنـــزلية المحدد في توصية قطاع تقييس الاتصالات X.1111. وفي هذا المثال، يحاول مستعمل بعيد النفاذ إلى كيانات داخل المنـــزل، فيما يحاول المستعمل المنـــزلي النفاذ إلى كيانات داخل وخارج المنـــزل.



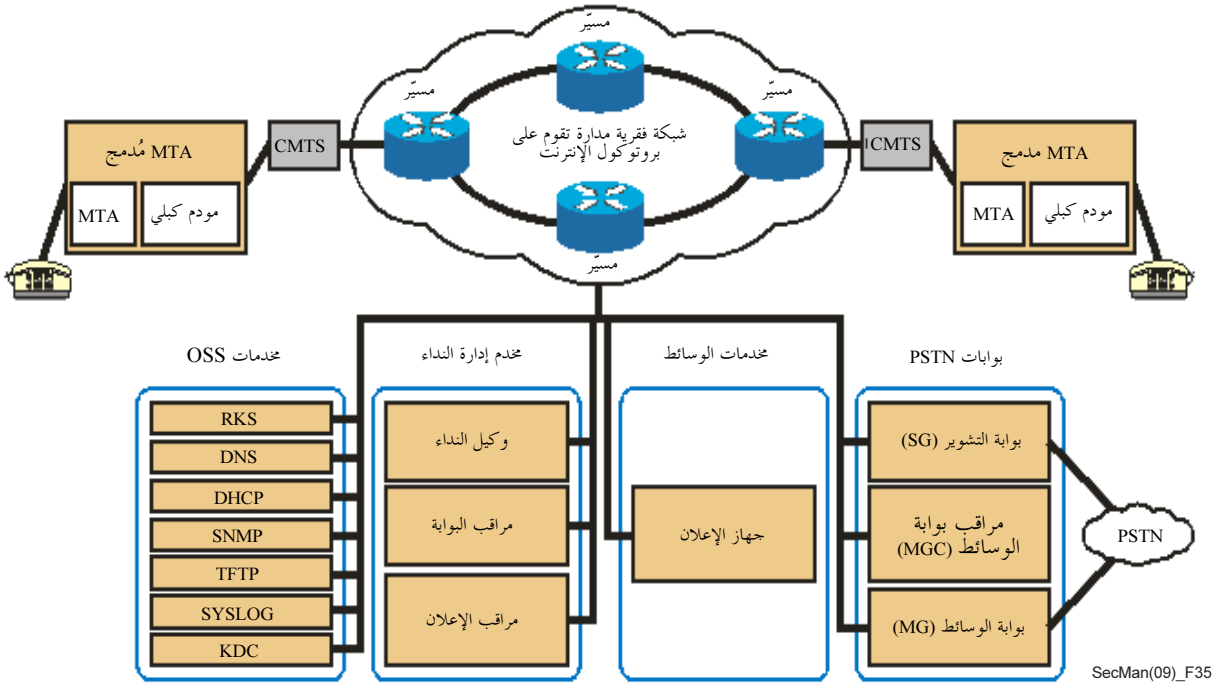
الشكل 34 – انسيابات خدمة الاستيقان للشبكة المنـــزلية

4.8 الاتصالات الكبلية بواسطة بروتوكول الإنترنت (IPCablecom)

يُمكّن نظام الاتصالات الكبلية بواسطة بروتوكول الإنترنت (IPCablecom) مشغلي التلفزيون الكبلي من توفير خدمات في الوقت الفعلي تقوم على أساس بروتوكول الإنترنت (IP) (مثل الاتصالات الصوتية) عبر شبكاتهم المعزَّزة لدعم المودمات الكبلية.

1.4.8 معمارية الاتصالات الكبلية بواسطة بروتوكول الإنترنت (IPCablecom)

تُحدَد معمارية الاتصالات الكبلية بواسطة بروتوكول الإنترنت في توصية قطاع تقييس الاتصالات J.160. ويبين الشكل 35 مكونات الاتصالات الكبلية بواسطة بروتوكول الإنترنت. وتحوي معمارية الاتصالات الكبلية بواسطة بروتوكول الإنترنت عناصر شبكية موثوقة وغير موثوقة على السواء. وتقع عناصر الشبكة الموثوقة عادةً ضمن الشبكة الفقرية التي يديرها مشغّل الكبل. أما عناصر الشبكة غير الموثوقة مثل المودم الكبلي ومكيف مطراف الوسائط (MTA) فهي تقع عادةً خارج مرفق مشغّل الكبل ضمن منـــزل المشترك.



الشكل 35 – النموذج المرجعي لمكونات الاتصالات الكبلية بواسطة بروتوكول الإنترنت (IPCablecom)

2.4.8 متطلبات أمن الاتصالات الكبلية بواسطة بروتوكول الإنترنت (IPCablecom)

يتعرض كل سطح بيني لبروتوكول شبكة الاتصالات الكبلية بواسطة بروتوكول الإنترنت لتهديدات قد تطال المشترك ومقدم الخدمة على السواء. فقد يعبر مسير تدفق الوسائط مثلاً عدداً كبيراً غير معروف أصلاً من أسلاك مقدمي خدمات الإنترنت وخدمات الشبكات الفقرية. ونتيجة لذلك، قد يكون تدفق الوسائط معرضاً لتنصت مؤذ مما يؤدي إلى فقدان خصوصية الاتصالات. أما أهداف تصميم الأمن المحددة في معمارية الاتصالات الكبلية بواسطة بروتوكول الإنترنت فهي كما يلي:

- تمكين قدرات الصوت المنـــزلية على نفس مستوى الخصوصية المتصورة في الشبكة الهاتفية العمومية التبديلية (PSTN)، أو أعلى؛
- توفير الحماية ضد الهجمات على مكيف مطراف الوسائط (MTA)؛
- حماية مشغّل الكبل من تعطل الشبكة والحرمان من الخدمة والهجمات الرامية لسرقة الخدمة.

ويجب أن تتضمن اعتبارات التصميم السرية والاستيقان والسلامة والتحكم في النفاذ.

وتوصّف متطلبات الأمن في توصية قطاع تقييس الاتصالات J.170 بعنوان مواصفة أمن الاتصالات الكبلية بواسطة بروتوكول الإنترنت (IPCablecom). وتلخَّص التهديدات التي ينبغي معالجتها على النحو التالي:

- سرقة الخدمة، التي تشمل الاحتيال في الاشتراك وعدم الدفع مقابل الخدمات ومستنسخات مكيف مطراف الوسائط (MTA) (مثلاً، حيث يُستنسخ مكيف مطراف وسائط مسجل في حساب احتيالي) وانتحال هوية مخدّم شبكة والتلاعب بالبروتوكول؛

- الإفصاح عن معلومات القناة الحمالة التي تشمل: التجسس البسيط ومستنسخات مكيف مطراف الوسائط (MTA) (مثل مكيف مطراف الوسائط الذي يمكن للعموم النفاذ إليه) والتلاعب بالبروتوكول وتحليل التجفير خارج الخط وتعطل الخدمة؛
- الإفصاح عن معلومات التشوير؛
- سرقة خدمات قائمة على مكيف مطراف الوسائط (MTA)؛
- تسجيل مكيف مطراف وسائط (MTA) مستأجر لدى مقدم خدمة آخر بصورة غير قانونية.

3.4.8 خدمات الأمن وآلياته في الاتصالات الكبلية بواسطة بروتوكول الإنترنت (IPCablecom)

تتخذ تدابير الأمن في شبكة الاتصالات الكبلية بواسطة بروتوكول الإنترنت في عناصر الطبقة الأدنى وهي تستخدم غالباً الآليات التي عرّفها فريق مهام هندسة الإنترنت (IETF). وتتناول معمارية الاتصالات الكبلية بواسطة بروتوكول الإنترنت هذه التهديدات بأن تحدد، لكل سطح بيني لبروتوكول معيّن، آليات الأمن التي يقوم عليها (مثل أمن بروتوكول الإنترنت IPSec) التي تزود السطح البيني للبروتوكول بخدمات الأمن التي يتطلبها. وفي سياق معمارية التوصية X.805، يتناول مجمل خدمات الأمن بالنسبة إلى الاتصالات الكبلية بواسطة بروتوكول الإنترنت جميع الخلايا التسع الناتجة عن ثلاثة مستويات وطبقات مبينة في الشكل 1.

وتتكون خدمات الأمن المتاحة من خلال طبقة الخدمة الأساسية في الاتصالات الكبلية بواسطة بروتوكول الإنترنت (IPCablecom) هي الاستيقان والتحكم في النفاذ والسلامة والسرية وعدم التنصل. وتشمل آليات الأمن كلاً من بروتوكول الأمن (مثل أمن بروتوكول الإنترنت (IPSec)، وأمن طبقة بروتوكول الوقت الفعلي (RTP)، وأمن بروتوكول إدارة الشبكة البسيطة v3 (SNMP) ودعم بروتوكول إدارة المفاتيح (مثل بدالة مفتاح الإنترنت (IKE) والاستيقان الأولي من تجفير المفاتيح العمومية /Kerberos) وكذلك تشمل خدمات الأمن الأساسية في الاتصالات IPCablecom آلية تجفير تدفقات الوسائط في بروتوكول الوقت الفعلي من طرف إلى طرف، ومن ثم تحول دون قدر كبير من تهديد الخصوصية.

5.8 الاتصالات الكبلية بواسطة بروتوكول الإنترنت 2 (IPCablecom2)

الاتصالات الكبلية بواسطة بروتوكول الإنترنت 2 هي مبادرة من دوائر صناعة الاتصالات الكبلية صُممت لدعم تقارب تكنولوجيات الصوت والفيديو والبيانات والتنقلية.

1.5.8 معمارية الاتصالات الكبلية بواسطة بروتوكول الإنترنت 2 (IPCablecom2)

تستند الاتصالات الكبلية بواسطة بروتوكول الإنترنت 2 إلى الإصدار 6 من النظام الفرعي متعدد الوسائط بواسطة بروتوكول الإنترنت (IMS) كما حدده مشروع شراكة الجيل الثالث (3GPP). ويندرج في مجال تطبيق مشروع شراكة الجيل الثالث إنتاج المواصفات التقنية للنظام العالمي للاتصالات المتنقلة (GSM) وللجيل الثالث (3G) من شبكات النظام المتنقل، ووضع معمارية لاتصالات بروتوكول الإنترنت القائمة على بروتوكول استهلال الجلسة (SIP) لشبكات الخدمة المتنقلة. وتشكل المعمارية الناتجة، وهي *النظام الفرعي متعدد الوسائط بواسطة بروتوكول الإنترنت*، الأساس لمعمارية الاتصالات الكبلية بواسطة بروتوكول الإنترنت 2 المعرّفة في توصية قطاع تقييس الاتصالات J.360.

2.5.8 متطلبات أمن الاتصالات الكبلية بواسطة بروتوكول الإنترنت 2 (IPCablecom2)

تشمل أهداف التصميم لمعمارية أمن الاتصالات الكبلية بواسطة بروتوكول الإنترنت 2 (IPCablecom2) ما يلي:

- دعم آليات السرية والاستيقان والسلامة والتحكم في النفاذ؛

- حماية الشبكة من الحرمان من الخدمة ومن تعطلها ومن الهجمات الرامية لسرقة الخدمة؛
- حماية معدات المستعملين (UE) (أي الزبائن) من هجمات الحرمان من الخدمة والثغرات الأمنية والنفاذ غير المصرح به إلى الشبكة؛
- دعم خصوصية المستعمل النهائي عبر التجفير وآليات التحكم في النفاذ إلى بيانات المشترك مثل معلومات التواجد؛
- آليات من أجل الجهاز ومعدات المستعملين والاستيقان من المستعمل والتقديم الآمن للخدمات والتشوير الآمن والتحميل الآمن للبرمجيات؛
- الاستفادة من معمارية أمن النظام الفرعي متعدد الوسائط بواسطة بروتوكول الإنترنت (IMS) تعزيزاً للأهداف التي سلف ذكرها.

أما التهديدات العامة التي تنطبق على الاتصالات الكبلية بواسطة بروتوكول الإنترنت 2 (IPCablecom2) فهي كما يلي:

التهديدات التي يتعرض لها ميدان الثقة

ميدان الثقة هو تجمع منطقي لعناصر الشبكة المؤتمنة على القيام باتصالات. ويمكن ترسيم حدود ميادين الثقة بتخوم مادية أو منطقية. ويجب أن تكون الاتصالات عبر ميادين الثقة محمية دوماً بالاستيقان والتخويل. وبالإضافة إلى ذلك، فإن السطوح البينية التي توصل عناصر شبكة ضمن ميدان والسطوح البينية ما بين الميادين والسطوح البينية ما بين معدات المستعمل ومقدم الخدمة يجب تأمينها ضد مجموعة متنوعة من التهديدات.

سرقة الخدمة

تتعدد سبل سرقة الخدمة، ومنها على سبيل الذكر لا الحصر، التلاعب في معدات المستعمل؛ واستغلال ضعف البروتوكول؛ وانتحال الهوية؛ واستنساخ معدات المستعمل (الإقدام على انتحال صفة معدات مشروعة لمستعمل)؛ والاحتيال في الاشتراكات وعدم الدفع لقاء الخدمات.

تعطل الخدمة والحرمان منها

ويشمل ذلك هجمات تهدف لحرمان المستعمل من الخدمة بصفة عامة؛ والهجمات العارمة (أي منع توفر عنصر معين في الشبكة، عادةً، بتوجيه كمية مفرطة من حركة شبكة الوسائط إلى سطوحه البينية)؛ وهجمات بواسطة حواسيب مأمورة (أي العديد من أنظمة النقطة الطرفية المخترقة).

التهديدات ضد قناة التشوير

في بيئة وسائط متعددة، تشمل رسائل التشوير البيانات المتعلقة بالهوية والخدمات والتسيير وغيرها من البيانات الحساسة والحرجة. وتوجد في ميدان النفاذ مكونات الوسائط المتعددة مثل الوكلاء، مما يعرضها لعدد أكبر من التهديدات. وتشمل التهديدات ضد قناة التشوير ما يلي: النيل من سرية معلومات التشوير؛ وهجمات طرف متوسط بين طرفي اتصالات جراء اعتراض الحركة العابرة بينهما أو ربما تعديلها؛ وهجمات الحرمان من الخدمة في مدى قناة التشوير.

التهديدات ضد القناة الحمالة

تتصل التهديدات ضد القناة الحمالة بحركة الوسائط المنقولة بين أطراف الاتصال.

التهديدات الأمنية الخاصة ببروتوكول معين

تتنوع التهديدات الماثلة ضد فرادى بروتوكولات الوسائط المتعددة.

3.5.8 خدمات الأمن وآلياته في الاتصالات الكبلية بواسطة بروتوكول الإنترنت 2 (IPCablecom2)

في الاتصالات الكبلية بواسطة بروتوكول الإنترنت 2، هناك استعمال مكثف لأمن طبقة النقل وللآليات الأخرى المشار إليها في النظام الفرعي متعدد الوسائط بواسطة بروتوكول الإنترنت كما حدده مشروع شراكة الجيل الثالث (3GPP) (3GPP 23.002 v6.10.0، *معمارية الشبكة*، ديسمبر 2005). وتلخص الفقرات التالية التحسينات التي تدخلها الاتصالات الكبلية بواسطة بروتوكول الإنترنت 2 (IPCablecom2) على معمارية أمن النظام الفرعي متعدد الوسائط بواسطة بروتوكول الإنترنت (IMS).

1.3.5.8 الاستيقان من المستعمل ومعداته

تدعم معمارية الاتصالات الكبلية بواسطة بروتوكول الإنترنت 2 (IPCablecom2) آليات الاستيقان التالية:

- الاستيقان من النظام الفرعي متعدد الوسائط بواسطة بروتوكول الإنترنت واتفاق مفتاح؛
- الاستيقان من خلاصة بروتوكول استهلال الدورة (SIP)؛
- تفعيل الشهادة.

وتستوعب المعمارية معدات المستعمل ذات المستندات الإثباتية المتعددة للاستيقان. فعلى سبيل المثال، قد تكون إحدى معدات المستعمل مزودة بشهادة للنفاذ إلى خدمات لدى دخولها على شبكة الكابل، وببطاقة دارة متكاملة عامة (UICC) للنفاذ إلى خدمات لدى دخولها على شبكة خلوية.

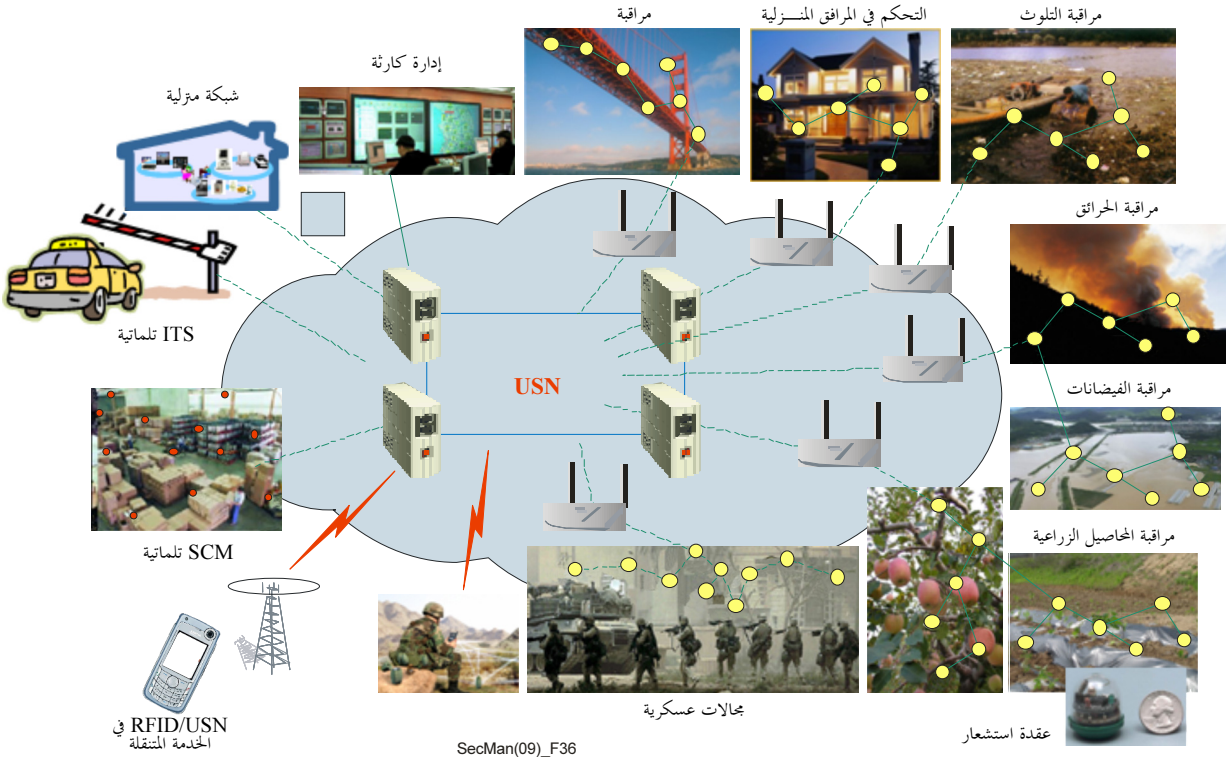
ويجوز تعدد المستندات الإثباتية لدى مشترك. فقد تتعدد معدات المستعمل لدى مشترك مع اختلاف القدرات المتصلة بتلك المستندات الإثباتية. فقد يكون لدى مشترك، مثلاً، مكيف مطراف وسائط (MTA) مزود بشهادة للاستعمال المنـــزلي، وجهاز مستعمل قائم على بطاقة دارة متكاملة عامة (UICC) للسفر.

2.3.5.8 أمن التشوير

تضيف الاتصالات الكبلية بواسطة بروتوكول الإنترنت 2 (IPCablecom2) أمن طبقة النقل (TLS) كخيار لأمن التشوير ما بين معدات المستعمل ووظيفة التحكم في دورة نداء الوكيل. ويُعتبر استعمال أمن طبقة النقل (على النحو المحدد في النظام الفرعي متعدد الوسائط بواسطة بروتوكول الإنترنت (IMS)) أمراً اختيارياً لأمن التشوير.

6.8 أمن شبكات الاستشعار في كل مكان

جهاز الاستشعار هو مجرد جهاز يولد إشارة كهربائية تمثل خاصية فيزيائية قابلة للقياس. أما شبكة الاستشعار في كل مكان (USN) فهي شبكة تستعمل أجهزة استشعار زهيدة الكلفة قليلة الاستهلاك القدرة لتنمية وعي بسياق ما من أجل تقديم خدمات المعلومات والمعرفة لأي شخص في أي مكان وفي أي وقت. ويمكن لشبكة الاستشعار في كل مكان أن تغطي منطقة جغرافية واسعة ويمكن أن تدعم مجموعة متنوعة من التطبيقات. ويوضح الشكل 36 التطبيقات المحتملة لشبكة الاستشعار في كل مكان (USN).



الشكل 36 – التطبيقات المحتملة لشبكة الاستشعار في كل مكان (USN)

جرت العادة على توصيل شبكات الاستشعار مع شبكات المستعمل النهائي. وفيما يرجح أن تستعمل شبكات الإرسال الأساسية الإنترنت وتكنولوجيات شبكة الجيل التالي، ستُستعمل مجموعة متنوعة من التكنولوجيات التي ترتكز إليها (مثل عروة المشترك الرقمية (DSL) والساتل والنظام العام للاتصالات الراديوية بأسلوب الرزم (GPRS) والنفاذ المتعدد بتقسيم شفري (CDMA) أو النظام العالمي للاتصالات المتنقلة (GSM) وغيرها).

وبما أن نقل المعلومات في شبكة الاستشعار في كل مكان (USN) يواجه العديد من التهديدات المحتملة، فإن الحاجة تدعو إلى تقنيات أمنية فعالة لمواجهة تلك التهديدات.

وبالإضافة إلى التهديدات العادية التي يتعرض لها الربط الشبكي (كتلك التي نوقشت في القسم 3)، ثمة تهديدات تستهدف شبكات الاستشعار في كل مكان على وجه التحديد، وهي تشمل ما يلي:

- **اختراق عقدة جهاز الاستشعار** جراء تعرض فرادى أجهزة الاستشعار لهجوم أو اختراق من مهاجم يُدخل أجهزة استشعار غير مشروعة؛
- **التنصت** من خلال مراقبة الإرسالات بين العقد؛
- **اختراق البيانات المستشعَرة أو انكشافها؛**
- **الهجمات المؤدية إلى الحرمان من الخدمة** على أجهزة استشعار أو الاتصالات؛
- **الاستعمال المؤذي لأجهزة الاستشعار أو إساءة استعمالها**، مثلاً، باستخدام أجهزة الاستشعار لأغراض غير قانونية.

زد على ذلك أن شبكات الاستشعار في كل مكان (USN) تتعرض لعدد من التهديدات المتعلقة بالتسيير بين عقد الاستشعار.

وتعقّد خصائص شبكة الاستشعار كثيراً من عملية تصميم شبكة آمنة. إذ يتعذر مثلاً استعمال تجفير المفاتيح العمومية أو تخزين مفاتيح فريدة في عقد الاستشعار، نظراً لمحدودية قدرتها الحاسوبية وذاكرتها ومحدودية التغذية الكهربائية وعرض النطاق فيها. وبالإضافة إلى ذلك، قد تقع أجهزة الاستشعار في بيئات معادية ويُجهل موقعها الدقيق بعد نشرها. وأخيراً، تعتمد شبكة الاستشعار بدرجة عالية على محطة القاعدة فيها التي تشكل النقطة الوحيدة لاحتمال وقوع عطل فيها وهدفاً مغرياً للراغبين في الهجوم عليها.

وتقدم البرمجيات الوسيطة لشبكات الاستشعار في كل مكان (USN) منصة مشتركة للتطبيقات لدعم مختلف الوظائف بالنيابة عن تطبيقات شبكة الاستشعار في كل مكان وخدماتها وللتحكم في شبكات الاستشعار. وتقوم البرمجيات الوسيطة لشبكات الاستشعار في كل مكان بتخزين الكمية الكبيرة من البيانات التي جمعها جهاز استشعار الشبكة وبإدارتها وتحليلها. وعلى هذه البرمجيات أيضاً أن توصل البيانات على نحو آمن إلى التطبيقات المناسبة. ويتعين أن تتناول تدابير الأمن في البرمجيات الوسيطة أمن البيانات أثناء تخزينها وإرسالها، فضلاً عن توفر البرمجيات الوسيطة.

ورغم عدم اكتمال توصيات بشأن شبكات الاستشعار في كل مكان (USN) فقد قطع العمل شوطاً طويلاً نحو معالجة الاحتياجات الأمنية لهذه الشبكات ولبرمجياتها الوسيطة.

9. أمن التطبيقات

9 أمن التطبيقات

مع ازدياد الوعي بأهمية الأمن، صار مطورو التطبيقات اليوم يولون المزيد من الاهتمام إلى الحاجة لبناء الأمن في منتجاتهم بدلاً من محاولة استدراك الجانب الأمني بعد انتقال التطبيق إلى مرحلة الإنتاج. ورغم ذلك، تُصادَف نقاط ضعف كامنة في معظم التطبيقات في مرحلة ما من دورة حياتها. وفوق ذلك، فإن التهديدات المستفحلة كثيراً ما تكشف النقاب عن مواطن ضعف لا سابق معرفة بها، وتستغلها.

وتُدرس في هذا القسم الميزات الأمنية لعدد من تطبيقات تكنولوجيا المعلومات والاتصالات مع التركيز بوجه خاص على ميزات الأمن التي تناولتها توصيات قطاع تقييس الاتصالات.

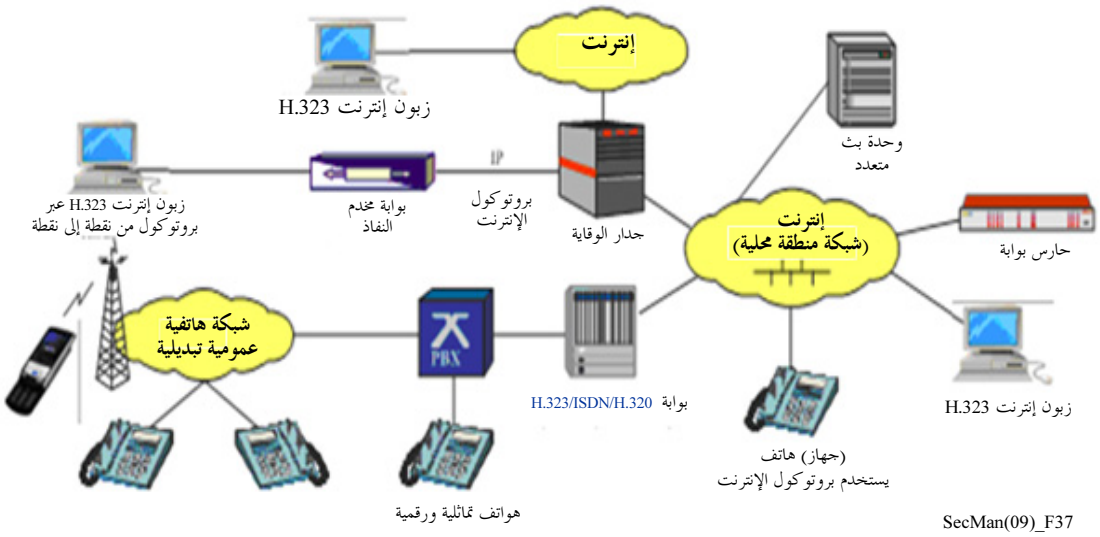
1.9 نقل الصوت بواسطة بروتوكول الإنترنت (VoIP) والوسائط المتعددة

إن نقل الصوت بواسطة بروتوكول الإنترنت (VoIP)، المعروف أيضاً باسم المهاتفة بواسطة بروتوكول الإنترنت، هو توفير الخدمات التي كانت تقدم تقليدياً عبر الشبكة الهاتفية العمومية التبديلية (PSTN) عن طريق شبكة تستخدم بروتوكول الإنترنت. وتشمل هذه الخدمات الصوت في المقام الأول ولكنها قد تشمل أيضاً أشكالاً أخرى من الوسائط، بما في ذلك الفيديو والبيانات. ويشمل نقل الصوت بواسطة بروتوكول الإنترنت أيضاً خدمات تكميلية مصاحبة مثل المؤتمرات الشبكية (مد الجسور) وإمكانية إحالة النداء والنداء قيد الانتظار والنداء المحوّل وتعدد الخطوط واستبقاء النداء للرد على نداء آخر والاطلاع على النداءات الواردة وإمكانية "تتبّع الجهة المطلوبة" وغير ذلك من الخدمات الكثيرة الأخرى التي توفرها الشبكات الذكية. ونقل الصوت بواسطة الإنترنت حالة خاصة لنقل الصوت بواسطة بروتوكول الإنترنت، وفيها تُرحَّل حركة الصوت عبر الشبكة الفقرية العمومية للإنترنت.

وتوصية قطاع تقييس الاتصالات H.323 بعنوان *أنظمة الاتصالات بوسائط متعددة قائمة على الرزم*، هي توصية شاملة توفر أساساً لنقل الصوت والفيديو والبيانات عبر شبكات تبديلية بالرزم، بما في ذلك الإنترنت وشبكات المناطق المحلية (LAN) وشبكات المناطق العريضة (WAN)، والتي لا توفر نوعية خدمة مضمونة. وتسود هذه الشبكات الحواسيب المكتبية للمؤسسات وتشمل تكنولوجيات بروتوكول التحكم في الإرسال بتبديل الرزم/بروتوكول الإنترنت (TCP/IP) وتبادل بروتوكول الإنترنت عبر إثرنت، والإثرنت السريعة والعلامة الجوالة في شبكة حلقية. ومن شأن الامتثال لتوصية قطاع تقييس الاتصالات H.323 أن يمكّن تحقيق التشغيل البيني لمنتجات وتطبيقات متعددة الوسائط من بائعين متعددين بما يسمح للمستعملين بالاتصال دون قلق بشأن التوافق. وكانت توصية قطاع تقييس الاتصالات H.323 أول بروتوكول لنقل الصوت بواسطة بروتوكول الإنترنت (VoIP) وتعتبر حجر الأساس للمنتجات القائمة على هذا البروتوكول للمستهلكين والمعاملات وتقديم الخدمات والتسلية والتطبيقات المهنية. وترد مواصفات أمن سلسلة توصيات قطاع تقييس الاتصالات H.323 في توصيات قطاع تقييس الاتصالات H.Imp235 بعنوان دليل المنفذين إلى *توصية قطاع تقييس الاتصالات H.235 V3: "الأمن والتجفير لمطاريف الوسائط المتعددة في السلسلة H (القائمة على توصيات قطاع تقييس الاتصالات H.323 وغيرها من توصيات قطاع تقييس الاتصالات H.245)"* وفي توصية قطاع تقييس الاتصالات H.235.x التي تضم سلسلة من تسعة أطر ومعايير للأمن، وتوصية قطاع تقييس الاتصالات H.530 بشأن *إجراءات الأمن التناظرية لتنقلية H.323 في توصية قطاع تقييس الاتصالات H.510* التي تتناول تنقلية الأنظمة والخدمات متعددة الوسائط وفق توصية قطاع تقييس الاتصالات H.323.

ويتسع نطاق توصية قطاع تقييس الاتصالات H.323 ليشمل كلاً من الأجهزة التي تعمل بمفردها والتكنولوجيا المدمجة في الحاسوب الشخصي، وكذلك الاتصالات من نقطة إلى نقطة والاتصالات متعددة النقاط.

وتتضمن التوصية H.323 تعريف أربعة مكونات رئيسية لنظام الاتصالات القائم على الشبكات، وهي: المطاريف، والبوابات، وحراس البوابات، ووحدات التحكم متعددة النقاط. ويمكن أن تتناول أيضاً عناصر ترادف أو تماس. وتبدو هذه العناصر في الشكل 37.

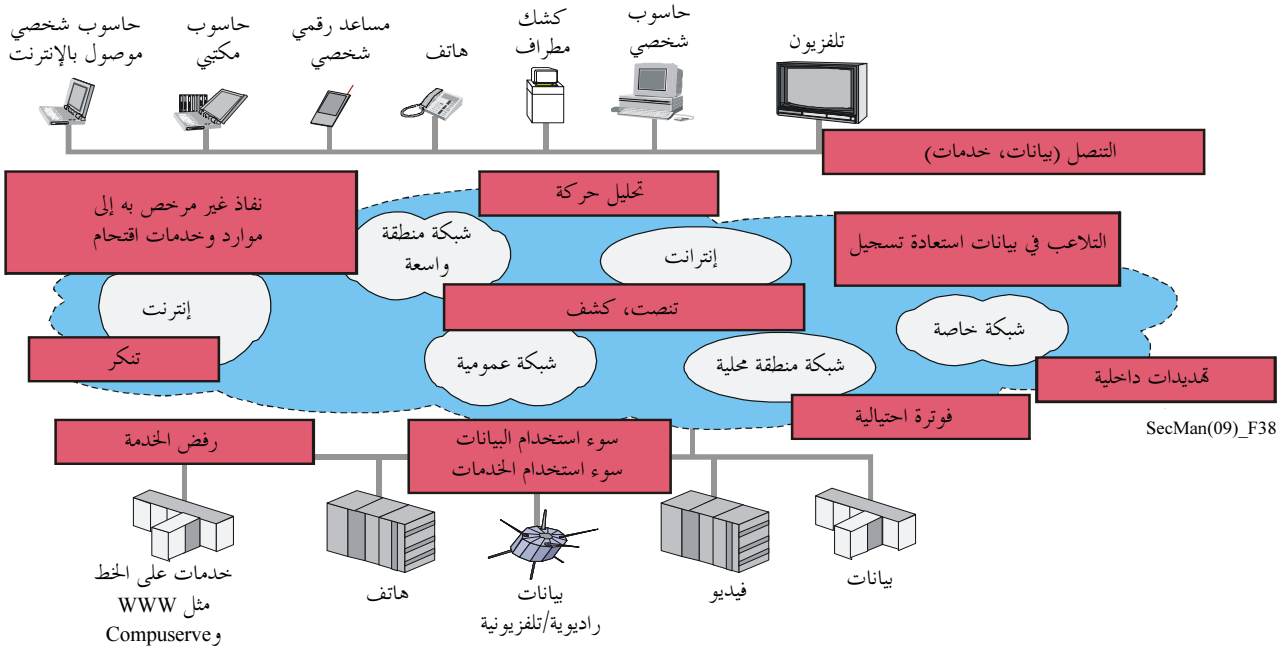


الشكل 37 – نظام التوصية H.323: مكونات وسيناريوهات النشر

ومن أمثلة استخدام التوصية ITU-T H.323 عبور بالجملة لوكالات التشغيل، ولا سيما عبر الشبكات الفقرية للمهاتفة بواسطة بروتوكول الإنترنت وخدمات بطاقات النداء. وفي اتصالات المؤسسات، تستخدم التوصية H.323 للبدالات الفرعية الخاصة بواسطة بروتوكول الإنترنت (IP-PBX) ونظام IP-Centrex – والشبكات الخاصة التقديرية (VPN) الصوتية والأنظمة المتكاملة للصوت والبيانات، وهواتف WiFi، وتنفيذ مراكز النداءات وخدمات التنقلية. وبالنسبة للاتصالات المهنية، تستخدم التوصية بشكل واسع في مجال المؤتمرات الصوتية (أو السمعية) والمؤتمرات الفيديوية، والتطبيقات التي تجمع بين الصوت/البيانات/الفيديو، وفي التعلم عن بُعد. وتشمل الاستعمالات في بيئة سكنية النفاذ السمعي البصري عريض النطاق، ومن حاسوب شخصي إلى هاتف، ومن هاتف إلى حاسوب، ومن حاسوب إلى حاسوب، ويمكن أن تستخدم أيضاً في تقديم الأخبار والمعلومات حسب الطلب.

1.1.9 قضايا الأمن في الوسائط المتعددة ونقل الصوت بواسطة بروتوكول الإنترنت

بما أن جميع عناصر النظام في التوصية ITU-T H.323 يمكن أن تتوزع جغرافياً، وبحكم الطابع المفتوح لشبكات بروتوكول الإنترنت، ينشأ العديد من التهديدات للأمن، كما هو مبين في الشكل 38.



الشكل 38 – تهديدات الأمن في حالة الاتصالات متعددة الوسائط

والقضايا الرئيسية للأمن في الاتصالات متعددة الوسائط والمهاتفة بواسطة بروتوكول الإنترنت هي على النحو التالي:

- الاستيقان من المستعمل والمطراف: يحتاج مقدمو خدمات نقل الصوت بواسطة بروتوكول الإنترنت إلى معرفة من يستخدم خدماتهم وذلك لأغراض المحاسبة وفوترة استخدام الخدمة. وكشرط مسبق للاستيقان ينبغي معرفة هوية المستعمل و/أو المطراف. ثم يتعين على المستعمل/المطراف أن يثبت صحة الهوية التي يدّعيها. ويحدث هذا عموماً من خلال إجراءات استيقان مجفرة (مثل كلمة مرور محمية أو توقيعات رقمية طبقاً للتوصية ITU-T X.509).

- الاستيقان من المخدم: بما أن مستعملي نقل الصوت بواسطة بروتوكول الإنترنت يتصلون فيما بينهم من خلال بنية تحتية ما لنقل الصوت بواسطة بروتوكول الإنترنت تنطوي على مخدمات (حراس البوابات، ووحدات تعدد الإرسال، والبوابات)، يحتاج المستعملون لمعرفة ما إذا كانوا يتحدثون مع المخدم الصحيح و/أو مقدم الخدمة المقصود. ويشمل هذا الجانب مستعملي الخدمات الثابتة والمتنقلة.

- الاستيقان من المستعمل/المطراف والمخدم: وهذا يلزم للتصدي للتهديدات ضد الأمن مثل التنكر وتدخل طرف متوسط بين طرفين وتقليد عناوين بروتوكول الإنترنت واختطاف التوصيل.

- التخويل بالنداء: هو عملية اتخاذ قرار لتقرير ما إذا كان المستعمل/المطراف مسموحاً له حقاً باستخدام موارد الخدمة (مثل النداء على الشبكات الهاتفية العمومية التبديلية) أو مصدر شبكة (نوعية الخدمة، وعرض النطاق، وأجهزة كودك، وما إلى ذلك). وغالباً ما تأتي وظائف الاستيقان والتخويل معاً لاتخاذ قرار التحكم في النفاذ. ويساعد الاستيقان والتخويل في إحباط الهجمات مثل التنكر وإساءة الاستخدام والغش والتلاعب والحرمان من الخدمة.

- حماية أمن التشوير: وهي تتناول حماية بروتوكولات التشوير من التلاعب وإساءة الاستخدام كما تتناول السرية والخصوصية. وتكون حماية بروتوكولات التشوير عموماً باستخدام التجفير فضلاً عن ضمان سلامة البيانات ومنع تكرار استعراضها. وينبغي إيلاء عناية خاصة لتلبية متطلبات الأداء الحرج لإجراء الاتصالات في الوقت الفعلي لتجنب أي تدهور في الخدمة نتيجة لتطبيق إجراءات الأمن.

- سرية الصوت: وهي تتحقق من خلال تجفير رزم الصوت والحيلولة دون التنصت. وبصورة عامة، يجري كذلك تجفير رزم الوسائط (مثل الفيديو) لتطبيقات الوسائط المتعددة. كذلك تشمل الحماية المتطورة لرزم الوسائط حماية الاستيقان وضمان سلامة بيانات الحمولة النافعة.
- إدارة المفاتيح: وهي لا تقتصر على جميع المهام الضرورية لتوزيع مواد المفاتيح بشكل آمن بين الأطراف على المستعملين والمخدمات فحسب، بل تشمل أيضاً مهام مثل تحديث المفاتيح التي انتهت صلاحيتها أو المفاتيح المفقودة. وقد تكون إدارة المفاتيح مهمة منفصلة عن تطبيق نقل الصوت بواسطة بروتوكول الإنترنت (توفير كلمة مرور) أو قد تكون متكاملة مع التشوير عندما يتم التفاوض الدينامي بشأن أشكال الأمن التي تتوافر لها المقدرات اللازمة، ويتعين توزيع المفاتيح على أساس الدورة.
- الأمن فيما بين الميادين: وهو يتعامل مع مشكلة أن الأنظمة في بيئات غير متجانسة تنفذ خصائص مختلفة للأمن بحكم اختلاف الاحتياجات وسياسات الأمن ومقدراته. وعليه تدعو الحاجة إلى التفاوض دينامياً بشأن مواصفات الأمن ومقدراته مثل الخوارزميات المجفرة ومعلماتها. ويتسم الأمر بأهمية خاصة عند عبور حدود بين الميادين واختلاف مقدمي الخدمات والشبكات. ومن المتطلبات الهامة لأمن الاتصالات بين الميادين إمكانية عبور الجدران الواقية بسهولة والتغلب على القيود التي تفرضها أجهزة ترجمة العناوين في الشبكة (NAT).

وهذه القائمة ليست شاملة ولكنها أساسية لمتطلبات الأمن بموجب التوصية ITU-T H.323. ولكن قد يواجه المرء في مجال التطبيق قضايا أخرى متعلقة بالأمن تعتبر خارج نطاق التوصية ITU-T H.323، ومنها مثلاً سياسة الأمن أو أمن إدارة الشبكات أو توفير الأمن أو أمن التنفيذ أو أمن التشغيل أو التعامل مع حادث في مجال الأمن.

2.1.9 لمحة عامة عن توصيات السلسلة الفرعية H.235.x

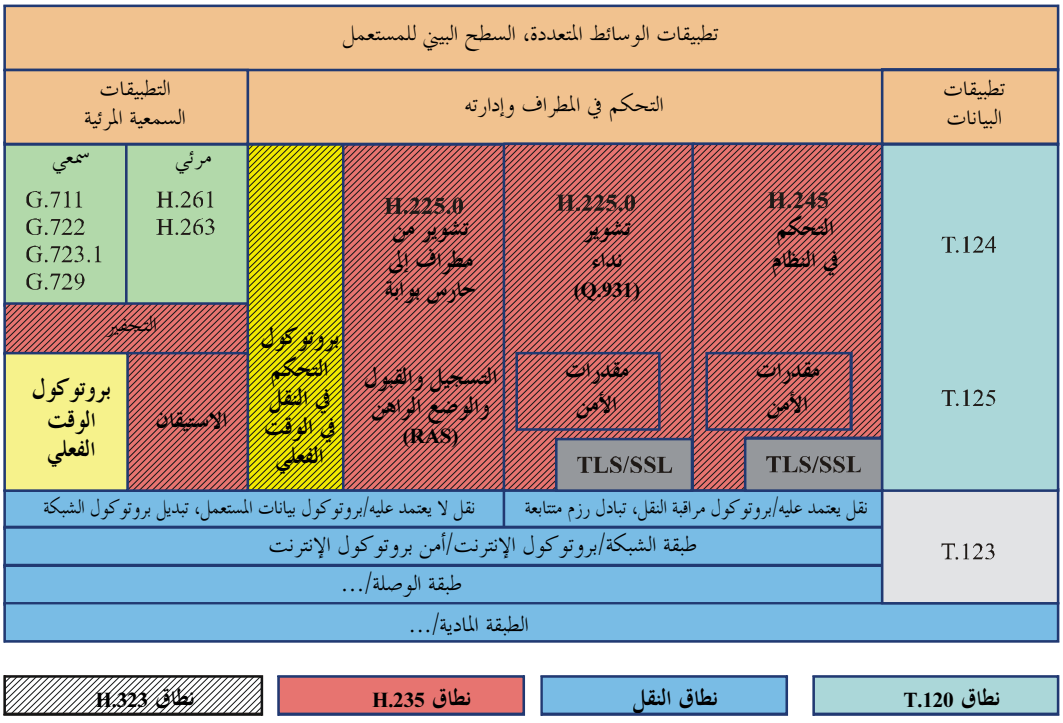
تتألف توصيات السلسلة الفرعية H.235.x من أحد عشر معياراً علاوة على دليل للمنفذين. وهي توفر بمجملها مواصفة آليات الأمن وبروتوكولاته بالإضافة إلى إرشادات مفصلة بشأن تنفيذ الأمن في سلسلة توصيات قطاع تقييس الاتصالات ITU-T H.323. كما توفر حلولاً أمنية يمكن تنويع مقاييسها للمجموعات الصغيرة والمؤسسات والشركات الناقلة التي تعمل على نطاق واسع، وتقدم حماية تجفيرية لبروتوكولات التحكم فضلاً عن بيانات تدفق الوسائط السمعية/الفيديوية.

وتوفر التوصية ITU-T H.235 وسائل للتفاوض بشأن خدمات مجفرة مطلوبة وخوارزميات تجفير ومقدرات أمن. ووظائف إدارة المفاتيح لاستحداث مفاتيح جلسات دينامية مدمجة تماماً ضمن إجراءات التشوير مما يساعد على خفض فترة الانتظار في إقامة النداء. وتضم التشكيلات المدعومة، الاتصالات "الكلاسيكية" من نقطة إلى نقطة، فضلاً عن التشكيلات متعددة النقاط مع وحدات الإرسال المتعدد عندما تتواصل عدة مطاريف متعددة الوسائط داخل مجموعة.

وتستخدم التوصية ITU-T H.235 تقنيات أمن خاصة مثلى كتجفير منحني إهليلجي ومعيار التجفير المتطور (AES) لتلبية قيود الأداء الصارمة. ويكون التجفير الصوتي في طبقة التطبيقات حيث يتم تجفير أحمال نافعة لبروتوكول الوقت الفعلي (RTP). وهذا يسمح بتنفيذ مفيد باستخدام حيز صغير في النقاط الطرفية من خلال التفاعل المحكم مع معالج الإشارة الرقمية (DSP) وجهاز تفكيك انضغاط الصوت دون ضرورة الاعتماد على منصة نظام تشغيل محدد.

ويبين الشكل 39 نطاق التوصية H.235 التي تحتوي على أحكام لإقامة نداءات (فدرات H.225.0 وH.245) واتصالات في اتجاهين (تجفير أحمال نافعة لبروتوكول الوقت الفعلي (RTP) الذي يحتوي على صوت و/أو فيديو منضغط). وتشمل العناصر الوظيفية آليات الاستيقان وسلامة البيانات والخصوصية وعدم التنصل. وحراس البوابات مسؤولون عن الاستيقان عن طريق التحكم في القبول في النقاط الطرفية وعن توفير آليات عدم التنصل. أما الأمن على طبقة النقل والطبقات السفلية، على أساس بروتوكول الإنترنت، فيعدّ خارج نطاق أي من التوصيتين H.323 وH.235 ولكنه ينفذ عادة باستخدام أمن بروتوكول الإنترنت (IPSec) لفريق مهام هندسة الإنترنت (IETF) وبروتوكولات أمن طبقة النقل (TLS). وحيثما تقتضي سياسة الأمن عند كل طرف، يمكن استخدام أمن بروتوكول الإنترنت (IPSec) أو أمن طبقة

النقل (TLS) لتوفير الاستيقان أو، اختيارياً، لتوفير السرية عند طبقة بروتوكول الإنترنت الشفافة لأي (تطبيق) بروتوكول يجري فوقها.



SecMan 02_F39

الشكل 39 – الأمن في التوصية H.323 كما يرد في التوصية H.235

وتشمل سلسلة التوصيات ITU-T H.235.x طائفة واسعة من تدابير الأمن التي تتناول بيئات مستهدفة مختلفة (كما في داخل المؤسسات/وفيما بينها وفي الشركات الناقلة) والتي يمكن تكييفها حسب الطلب ووفق سيناريو محدد تبعاً لعوامل محلية من قبيل ما هو متوفر من بنية تحتية للأمن ومن مقدرات للمطراف (ومثال ذلك نقاط طرفية بسيطة مقابل نقاط طرفية ذكية).

وتوفر مواصفات الأمن المتاحة تقنيات للأمن تتراوح من التقنيات البسيطة السرية المشتركة التي تنطوي على كلمة مرور محمية إلى مواصفات متطورة تعمل بتوقيعات رقمية وشهادات البنى التحتية للمفاتيح العمومية بموجب X.509 (H.235.2). وهذه التقنيات تسمح إما بالحماية قفزة قفزة باستخدام تقنيات بسيطة ولكنها أقل قابلية لتنويع المقاييس أو بالحماية من طرف إلى طرف باستخدام التقنيات القابلة لتنويع مقاييس البنى التحتية للمفاتيح العمومية. وتدعى ITU-T H.235.3 مواصفة الأمن الهجينة إذ إن هذه التوصية التي تجمع ما بين إجراءات الأمن التناظرية من H.235.1 وباستعمال الشهادات والتواقيع القائمة على البنى التحتية للمفاتيح العمومية من ITU-T H.235.2 تحقق أداء أمثل وزمن إقامة نداء أقصر. وتخفف التوصية ITU-T H.323 الاعتماد الصارم على معمارية مركزها مخدم يسيّرها حارس بوابة وهي توفر تدابير أمن ترمي إلى تأمين نموذج الند إلى الند. وتعرّف هذه التوصية إجراءات لإدارة المفاتيح في بيئة مؤسسة أو في بيئة ما بين الميادين.

وسعياً إلى تعزيز أمن الأنظمة التي تستعمل أرقام تعرّف الهوية الشخصية (PINs) أو كلمات المرور للاستيقان من المستعملين فإن التوصية ITU-T H.235.5 توفر إطاراً آخر هو "*إطار لتأمين الاستيقان في عملية التسجيل والقبول والوضع الراهن RAS باستخدام أسرار متقاسمة ضعيفة*" وذلك باستخدام طرائق المفاتيح العمومية لتأمين استعمال الأرقام PIN أو كلمات المرور. وتضم التوصية ITU-T H.235.6 "*مواصفة تجفير الصوت على أساس إدارة المفتاح الأصلي*

H.245/H.235" كل الإجراءات اللازمة لتجفير تدفق وسائط في بروتوكول الوقت الفعلي (RTP) بما في ذلك إدارة المفاتيح المحيطة المعبّر عنها كلياً ضمن حقول تشوير ITU-T H.245.

وإذ تغطي التوصية ITU-T H.530 *تنقلية آمنة للمستعملين والمطاريف في بيئات H.323 الموزعة، تغطي التوصية H.510 إجراءات الأمن التناظرية لتنقلية H.323* وتتناول جوانب أمنية من قبيل ما يلي:

- الاستيقان من مطراف/مستعمل متنقل والتصريح له في الميادين الأجنبية التي يزورها؛
- الاستيقان من الميدان موضع الزيارة؛
- تأمين إدارة المفتاح؛
- حماية بيانات التشوير بين مطراف متنقل وميدان موضع الزيارة.

وتوفر توصية قطاع تقييس الاتصالات ITU-T H.235.0 الإطار الأمني العام لأنظمة الوسائط المتعددة من السلسلة H. أما التوصيات H.235.0 وH.350 فهي تمكّن الإدارة متنوعة المقاييس للمفاتيح باستخدام بروتوكول النفاذ السريع إلى الدليل (LDAP) وطبقة المقبس الآمن (SSL/TLS). وعلى وجه الخصوص، فإن سلسلة التوصيات ITU-T H.350 توفر مقدرات تمكّن المؤسسات وشركات الاتصالات من إدارة آمنة لأعداد كبيرة من مستعملي الخدمات الفيديوية وخدمات نقل الصوت بواسطة بروتوكول الإنترنت. كما توفر وسيلة لتوصيل H.323 وبروتوكول استهلال الدورة (SIP) وH.320 وخدمات المراسلة المعتادة بخدمة دليل بحيث يمكن تطبيق الممارسات الحديثة لإدارة الهوية على الاتصالات متعددة الوسائط.

3.1.9 أجهزة ترجمة عناوين الشبكة وجدران الوقاية

صممت شبكة الإنترنت بحيث تراعي مبدأ "من طرف إلى طرف". أي أن بإمكان أي جهاز على الشبكة الاتصال مباشرة بأي جهاز آخر على الشبكة. ومع ذلك، وبحكم اعتبارات الأمن ونظراً إلى النقص في عناوين الشبكات في الإصدار الرابع من بروتوكول الإنترنت (IPv4)، فإن أجهزة جدران الوقاية (FW) وترجمة عنوان الشبكة (NAT) كثيراً ما تُستخدم عند حدود الشبكات. وتشمل هذه الحدود ميدان الإقامة وميدان مقدم الخدمة وميدان المؤسسة، وأحياناً ميدان البلد. ويُستخدم أحياناً أكثر من جهاز جدار وقاية أو ترجمة عناوين شبكة ضمن ميدان واحد. وأجهزة جدران الوقاية مصممة بحيث تتحكم بشكل صارم في كيفية انتقال المعلومات عبر حدود الشبكات وهي مشكّلة عادة بحيث تمنع مرور معظم اتصالات بروتوكول الإنترنت. ولذلك، وما لم يشكّل جدار الوقاية صراحة لتمرير حركة ITU-T H.323 الآتية من الأجهزة الخارجية وتمكينها من العبور لكي تصل إلى أجهزة ITU-T H.323 الداخلية فإن الاتصال غير ممكن إطلاقاً. وهذا يطرح مشكلة لكل من يستعمل تجهيزات ITU-T H.323.

وتقوم أجهزة NAT بترجمة العناوين المستخدمة في الميدان الداخلي إلى عناوين مستخدمة في الميدان الخارجي والعكس بالعكس. وتكون العناوين المستخدمة ضمن ميدان سكني أو ميدان مؤسسة مخصصة عموماً وليس دوماً، من مساحات عناوين شبكات خاصة محددة في المعيار IETF RFC 1597. وهي كما يلي:

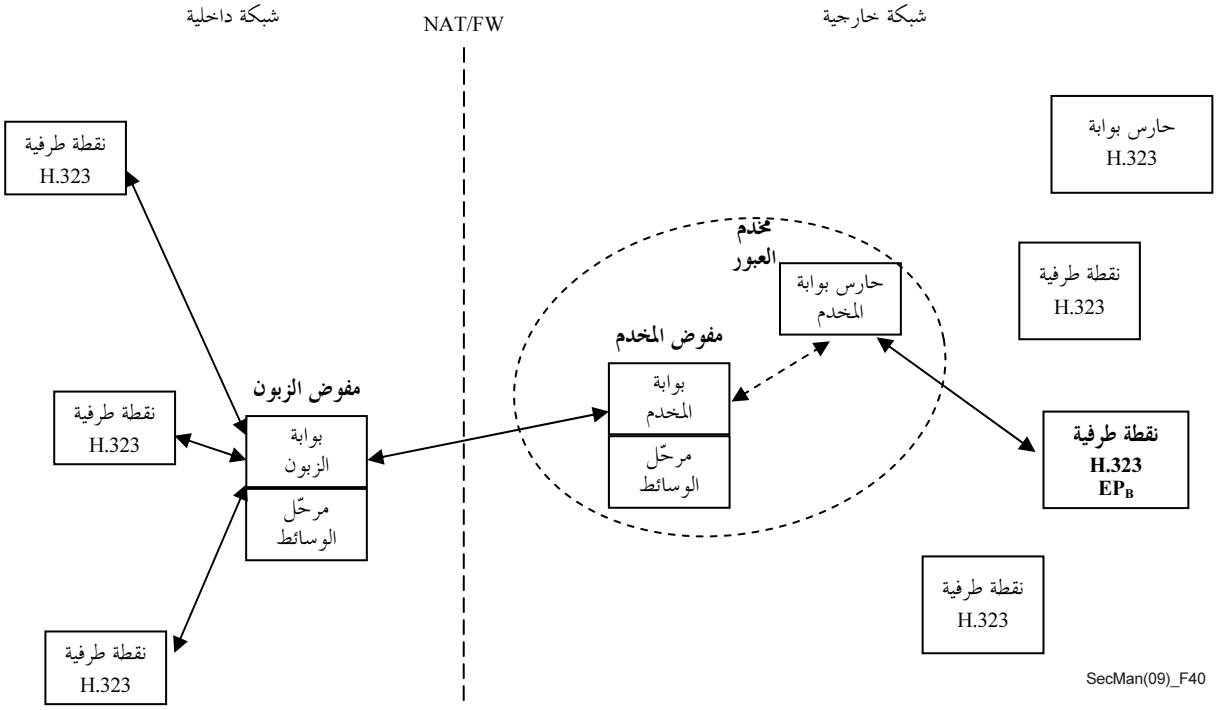
الصنف	مدى العنوان	عدد عناوين بروتوكول الإنترنت
A	10.0.0.0 – 10.255.255.255	16 777 215
B	172.16.0.0 – 172.31.255.255	1 048 575
C	192.168.0.0 – 192.168.255.255	65 535

وتنطوي أجهزة NAT على مشكلة عويصة لمعظم بروتوكولات الإنترنت، لا سيما تلك التي تحمل عناوين بروتوكول الإنترنت داخل البروتوكول. ولا بد لبروتوكولات ITU-T H.323 وSIP وغيرها من بروتوكولات الاتصال في الوقت

الفعلي التي تعمل عبر شبكات التبديل بالرزم من أن تقدم عنوان بروتوكول الإنترنت ومعلومات المنفذ لكي تعرف الأطراف الأخرى في الاتصال إلى أين ترسل تدفقات الوسائط (مثال ذلك التدفقات السمعية والمرئية).

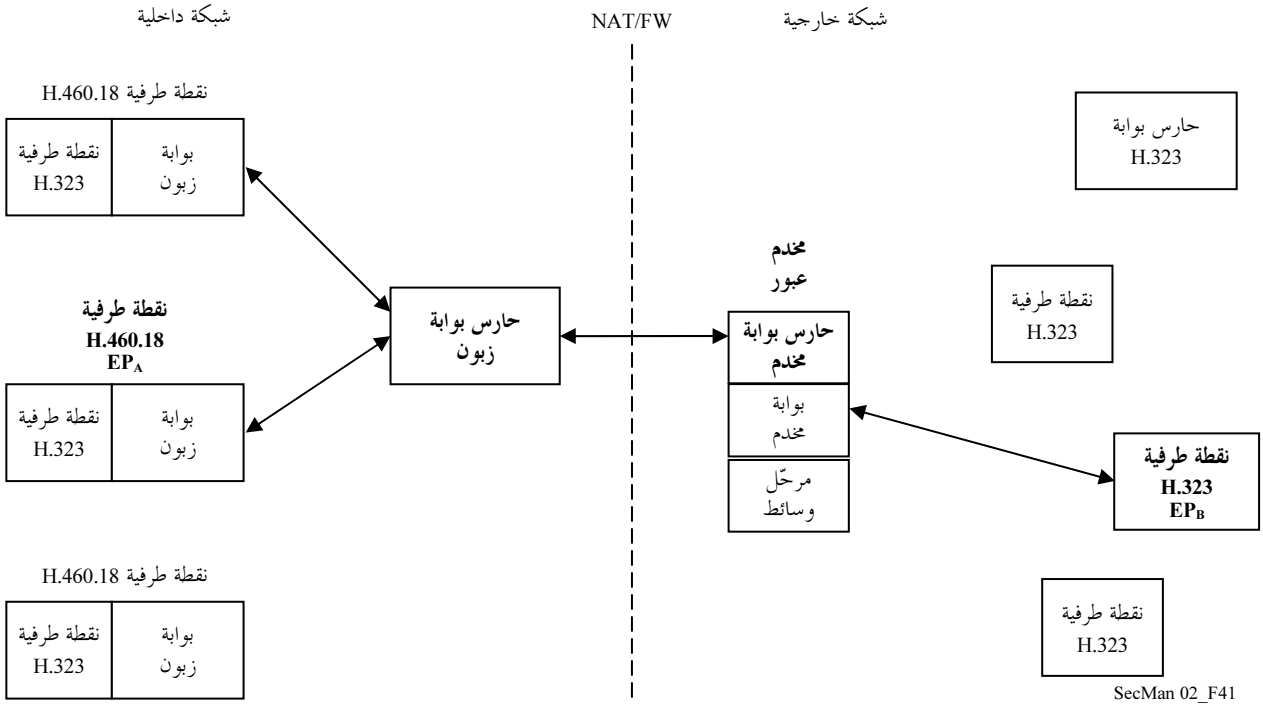
وقد درس قطاع تقييس الاتصالات مسائل عبور أجهزة NAT/FW ووضع ثلاث توصيات من سلسلة H.460 لأنظمة H.323 لتمكين هذه الأنظمة من عبور واحد أو أكثر من أجهزة NAT/FW بشكل انسيابي. وهذه التوصيات هي: H.460.17 ("*استعمال توصيل تشوير النداء H.225.0 كوسيلة نقل لرسائل التسجيل والقبول والوضع الراهن RAS في إطار H.323*") وH.460.18 ("*عبور تشوير H.323 من خلال أجهزة ترجمة عناوين الشبكة وجدران الوقاية*") وH.460.19 ("*عبور وسائط H.323 من خلال ترجمة عناوين الشبكة وجدران الوقاية*").

ويصور الشكل 40 كيف يمكن استعمال جهاز "مفوض" خاص لمساعدة الأجهزة "الغافلة" عن NAT/FW على عبور حدود NAT/FW على نحو ملائم.



الشكل 40 – عبور حدود NAT/FW في معمارية H.460.18

وقد تُستعمل الطوبولوجيا المصورة أعلاه عندما ترغب مؤسسة مثلاً في التحكم في الطريق التي يمر فيها تشوير النداء وتدفقات الوسائط H.323 عبر الشبكة. غير أن H.460.17 وH.460.18 تمكنان النقاط الطرفية أيضاً من عبور حدود NAT/FW دون المساعدة من أي أجهزة داخلية خاصة "مفوضة". ويصور الشكل 41 مثل هذه الطوبولوجيا:



الشكل 41 – معمارية الاتصال بين حراس البوابة

في الشكل 41، تتصل النقاط الطرفية على الشبكة الداخلية مع حارس البوابة الذي يقيم أيضاً في الشبكة الداخلية لاستخلاص عنوان كيانات خارجية (رقم هاتف مثلاً أو معرف موارد موحّد H.323 URL لعنوان IP). ثم يتصل حارس البوابة في الشبكة الداخلية بحارس البوابة في الشبكة الخارجية لتبادل معلومات العنونة تلك وينقل تلك المعلومات إلى النقطة الطرفية صاحبة النداء. وعندما يباشر جهاز ضمن الشبكة الداخلية نداءً إلى جهاز في الشبكة الخارجية فإنه يستخدم الإجراءات المحددة في H.460.18 لكي يفتح ما يلزم من "ثقوب دبوس" عبر أجهزة NAT/FW للحصول على التشوير من الشبكة الداخلية إلى الشبكة الخارجية. وكذلك يستخدم الإجراءات المحددة في H.460.19 لكي يفتح ما يلزم من "ثقوب دبوس" لتمكين تدفقات الوسائط من العبور الملائم من الشبكة الداخلية إلى الشبكة الخارجية والعكس بالعكس.

وعندما تكون الأجهزة طالبة النداء والأجهزة المطلوبة واقعة في شبكتين خاصتين مختلفتين تفصل بينهما أجهزة NAT/FW وشبكة الإنترنت العمومية عندئذ يحتاج الأمر إلى ما لا يقل عن "بوابة مخدم" واحدة و"مرحل وسائط" واحد (محددين في التوصية H.460.18) وذلك لتسيير التشوير والوسائط على نحو ملائم بين الشبكتين الخاصتين. وكثيراً ما يشار إلى هذه التوليفة من الأجهزة باسم "مراقب حدود الدورة". والسبب بكل بساطة أن لا سبيل، بحكم التصميم، لأي رزمة IP ضمن شبكة خاصة كي تدخل شبكة خاصة أخرى دون مساعدة من كيان ما في الشبكة العمومية يضطلع بدور "المفوض" لتلك الرزمة.

2.9 التلفزيون القائم على بروتوكول الإنترنت (IPTV)

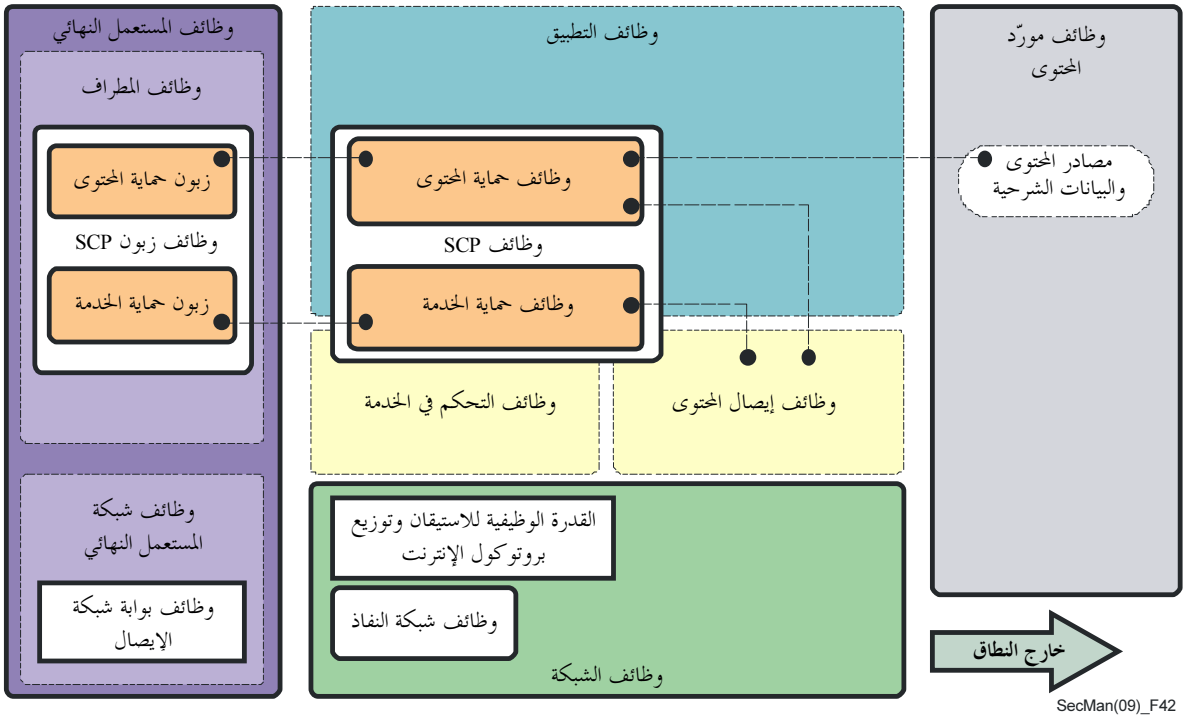
يجب أن تشمل أحكام الأمن للتلفزيون القائم على بروتوكول الإنترنت (IPTV) حماية المحتوى المقدَّم من خلال خدمات التلفزيون القائم على بروتوكول الإنترنت، وحماية أجهزة المطراف المستعملة وعملية تقديم مثل هذه الخدمات.

وفي التلفزيون القائم على بروتوكول الإنترنت، تتمثل حماية المحتوى في ضمان عدم تمكن المستعمل النهائي من استعمال المحتوى إلا وفقاً للحقوق التي يمنحها صاحب الحقوق. ويشمل ذلك حماية المحتويات من الأعمال غير القانونية من نسخ وتوزيع واعتراض وعبث واستعمال غير مصرح به.

وتشمل حماية أجهزة مطراف التلفزيون القائم على بروتوكول الإنترنت (IPTV) ضمان تمكّن الجهاز الذي يستخدمه مستعمل نهائي لاستقبال الخدمة من استعمال المحتوى على نحو موثوق آمن، وضمان إنفاذ حقوق استخدام المحتوى وحماية سلامة وسرية محتوى فضلاً عن المعايير الأمنية الحرجة مثل مفاتيح التشفير.

وتشمل حماية خدمة التلفزيون القائم على بروتوكول الإنترنت (IPTV) ضمان عدم تمكن المستعملين النهائيين من الحصول على خدمات ومحتويات إلا ما كان من حقهم استقباله. كما تشمل حماية الخدمة من النفاذ غير المصرح به.

وهناك عدد من توصيات الأمن الخاصة بالتلفزيون القائم على بروتوكول الإنترنت (IPTV) قيد الإعداد، وقد تمت الموافقة على إحداها وهي توصية قطاع تقييس الاتصالات X.1191 بعنوان: *المتطلبات الوظيفية لجوانب أمن التلفزيون القائم على بروتوكول الإنترنت (IPTV) ومعماريته*. وتظهر معمارية الأمن العامة للتلفزيون القائم على بروتوكول الإنترنت في الشكل 42؛ علماً بأن نطاق تطبيق التوصية لا يأخذ في الاعتبار إلا الوظائف التي تشمل المستعمل النهائي ومزود الشبكة ومقدم الخدمة. أما الوظائف المتصلة بمقدم المحتوى فهي تخضع لاتفاقات خاصة بين أصحاب المصلحة وتُعتبر خارج نطاق هذه التوصية.



الشكل 42 – معمارية الأمن العامة للتلفزيون القائم على بروتوكول الإنترنت (IPTV)

1.2.9 آليات حماية محتوى التلفزيون القائم على بروتوكول الإنترنت (IPTV)

تشمل آليات الأمن التي يمكن استخدامها لحماية المحتوى ما يلي:

- تجفير المحتوى؛
- العلامة المائية (أي اللجوء إلى تقنيات إخفاء المعلومات لتغيير سمات محتوى معين دون أن يُكتشف هذا التغيير بسهولة)؛
- تحديد تتبع المحتوى ومعلومات هذا التتبع لتسهيل التحقيق في النفاذ غير المصرح به إلى المحتوى واستعماله؛

- وسم المحتوى (من قبيل معلومات التصنيف للسماح بدرجة ما من تحكم المستعمل النهائي في النفاذ إلى المحتوى غير اللائق)؛
- تحويل الشفرة الآمن (الذي يسمح للعقد الوسيطة في الشبكة بتحويل محتوى الوسائط المتعددة إلى نسق أو نوع آخر دون فك التشفير، مما يحافظ على الأمن من طرف إلى طرف).

2.2.9 آليات حماية خدمة التلفزيون القائم على بروتوكول الإنترنت (IPTV)

تشمل آليات حماية الخدمة ما يلي:

- الاستيقان من المستعمل (المشترك) و/أو جهاز المطراف من طرف إلى طرف؛
- التخويل (التأكد من المستعمل النهائي أو المطراف مصرح له بالنفاذ إلى الخدمات و/أو المحتوى)؛
- التحكم في النفاذ (وخاصة لضمان أن المحتوى الذي يحمَّل من زبون إلى مخدِّم لا يمكن إلا لمقدم خدمة مخوّل النفاذ إليه).

3.2.9 حماية معلومات المشترك

من دواعي الانشغال الخاصة عند تنفيذ التلفزيون القائم على بروتوكول الإنترنت (IPTV)، الحاجة إلى حماية المعلومات المشترك التي قد تتضمن تتبع البيانات والمعلومات مثل رقم القناة قبل وبعد تغيير القناة، ووقت التغيير، ومعلومات المستعمل لخدمة دليل البرنامج الالكترونية، وتحديد الرزمة، ووقت التشغيل، وما إلى ذلك. فلا بد من أن تُعتبر هذه البيانات حساسة، ولا بد من اتخاذ تدابير لمنع الإفصاح عنها دون تصريح عبر المطراف أو الشبكة أو مقدم الخدمة. وترد مقترحات لحماية معلومات المشترك في ملحق توصية قطاع تقييس الاتصالات X.1191.

3.9 الفاكس الآمن

يظل الفاكس تطبيقاً شائعاً جداً، إلا أن الثقة في خدمات الفاكس تعمد إلى حد بعيد على فعالية تدابير الأمن المدمجة فيه. وقد وُضعت معايير الفاكس في البداية للإرسال عبر الشبكات PSTN (توصية قطاع تقييس الاتصالات T.4) ثم للشبكات الرقمية متكاملة الخدمات (ISDN) (توصية قطاع تقييس الاتصالات T.6). وقد توسعت مؤخراً لتشمل النقل عبر شبكات بروتوكول الإنترنت (بما في ذلك الإنترنت) للإرسال في الوقت الفعلي (توصية قطاع تقييس الاتصالات T.38) أو عبر أنظمة التخزين والإرسال (توصية قطاع تقييس الاتصالات T.37).

بغض النظر عن أسلوب الإرسال، فإن القضايا أمنية التي تواجهها خدمات الفاكس تشمل سرية البيانات المرسلة والاستيقان وعدم التنصل. وقد ازدادت أهمية هذه القضايا بانتقال الحركة إلى الإنترنت نتيجة للطابع المفتوح والموزع للوسط الناقل.

أما توصية قطاع تقييس الاتصالات T.36 بعنوان: المقدرات الأمنية المعدة للاستعمال في مطاريف فاكس من الزمرة 3، فهي تتناول أمن الفاكس وتعرّف حلين تقنيين مستقلين يمكن استخدامهما في سياق إرسال آمن للفاكس لتجفير الوثائق التي يتم تبادلها. ويتمثل أحد الخيارين المحددين في استعمال خوارزمية *ريفست وشامير وأدلمان RSA التجفيرية*؛ فيما تلجأ الطريقة الأخرى إلى الجمع بين خوارزمية *هوثورن لإدارة المفاتيح* (HKM) وخوارزمية *هوثورن لشفرة فاكس* (HFX). ويرد تعريف خدمات الأمن التالية:

- الاستيقان المتبادل (إلزامي)؛
- خدمة أمن (اختيارية) تشمل الاستيقان المتبادل وسلامة الرسالة وتأكيد استلام الرسالة؛
- خدمة أمن (اختيارية) تشمل الاستيقان المتبادل وسرية الرسالة (تجفير) وإقامة مفتاح الدورة؛

- خدمة أمن (اختيارية) تشمل الاستيقان المتبادل وسلامة الرسالة وتأكيد استلام الرسالة وسرية الرسالة (تجفير) وإقامة مفتاح الدورة.

ويوفر الجمع بين خوارزمية *هوثورن لإدارة المفاتيح* وخوارزمية *هوثورن لشفرة فاكس* المقدرات التالية لتوفير اتصالات الوثائق الآمنة بين كيانات:

- الاستيقان المتبادل من الكيانات؛
- إقامة مفتاح سري للدورة؛
- سرية الوثائق؛
- تأكيد الاستلام؛
- تأكيد أو نفي سلامة الوثائق.

4.9 خدمات الويب

يجري تطبيق تكنولوجيات الويب، بما في ذلك المعماريات ذات التوجه الخدمي، على نطاق واسع لأنها تسمح للمطورين بوضع خدمات جديدة ونشرها بكفاءة وفعالية من حيث التكلفة، وبدمج المحتوى من مصادر مختلفة لتشكيل مركّب خدمات بيسر وسرعة. وتكثر الجوانب الأمنية للخدمات على شبكة الإنترنت. وإذ تُعتبر آليات الاستيقان والدخول الواحد (SSO) مهمةً نظراً لتطبيق خدمات الويب على شبكات الاتصالات المتنقلة، فمن المهم أيضاً النظر في آليات الأمن اللازمة لخدمات الويب المتنقلة.

وقد حدت وفورات الحجم بباعة منصات الحوسبة إلى تطوير منتجات ذات عناصر وظيفية على قدر عال من العمومية بحيث يمكن استخدامها في أوسع نطاق ممكن من الحالات. وتسلَّم هذه المنتجات مزودةً بأقصى امتياز ممكن للنفاذ إلى البيانات ولتنفيذ البرامج، بحيث يمكن استعمالها في أكبر عدد ممكن من بيئات التطبيقات بما فيها تلك الأكثر تهاوناً في سياساتها الأمنية. وأينما دعت الحاجة لسياسة أمن أكثر تشدداً، يتعين تقييد الامتيازات المتاحة ضمن المنصة بتشكيلة محلية.

وتكثر عناصر سياسة الأمن في مؤسسة كبيرة وتتعدد نقاط إنفاذها. ويمكن أن تُسنَد إدارة عناصر هذه السياسة إلى دائرة أنظمة المعلومات ودائرة الموارد البشرية والدائرة القانونية ودائرة الشؤون المالية. ويمكن إنفاذ هذه السياسة من خلال الشبكة الخارجية والبريد وشبكة المنطقة الواسعة (WAN) وأنظمة النفاذ عن بعد – وهي منصات تنفذ أصلاً سياسة أمن متساهلة. والدارج حالياً هو إدارة تشكيلة كل نقطة إنفاذ على نحو مستقل من أجل تنفيذ سياسة الأمن بأكبر قدر ممكن من الدقة. وبالتالي، فإن تعديل سياسة الأمن أمر مكلف وغير موثوق. كما يصعب (بل وربما يستحيل) الحصول على وجهة نظر موحدة بشأن الضمانات المرعية في جميع أنحاء المؤسسة لإنفاذ هذه السياسة. وفي الوقت نفسه، يتزايد ضغط المستهلكين والمساهمين والمنظمين على المدراء التنفيذيين في الشركات ودوائر الحكومة كي يبينوا "الممارسات الفضلى" في حماية أصول معلومات المؤسسة وزبائنها.

لهذه الأسباب، تقتضي الحاجة لغة مشتركة للتعبير عن سياسة الأمن. فإذا ما نُفذت في عموم المؤسسة، فهي تتيح للمؤسسة إدارة إنفاذ جميع عناصر سياستها الأمنية في جميع مكونات أنظمة معلوماتها. وقد تشمل إدارة سياسة الأمن بعضاً من الخطوات التالية أو كلها: تدوين هذه السياسة ومراجعتها والموافقة عليها وإصدارها ودمج أجزاء فيها وتحليلها وتعديلها وسحبها واستخراجها وإنفاذها.

وبالإضافة إلى ذلك، تدعو الحاجة لإطار لتبادل المعلومات الأمنية. وتسهيلاً لهذه التبادلات، أُعدت لغات ترميز، ومنها: لغة ترميز تأكيد الأمن ولغة ترميز التحكم في النفاذ القابلة للتوسيع (XACML). وهي لغات أعدتها في الأصل منظمة

النهوض بالمعايير الإعلامية المهيكلة (OASIS)، وقد اعتمدها الآن قطاع تقييس الاتصالات ونشرها بمساعدة من المنظمة.

1.4.9 لغة ترميز تأكيد الأمن

تعرّف توصية قطاع تقييس الاتصالات X.1141 لغة ترميز تأكيد الأمن (SAML 2.0). وهذه اللغة هي إطار قائم على لغة الترميز القابلة للتوسيع (XML) من أجل تبادل معلومات أمنية. ويُعبر عن معلومات الأمن هذه في شكل تأكيدات حول مواضيع، حيث الموضوع هو كيان ذو هوية في ميدان أمني ما. ويمكن لتأكيد واحد أن يحتوي على العديد من البيانات الداخلية المختلفة عن الاستيقان والتخويل والنعوت.

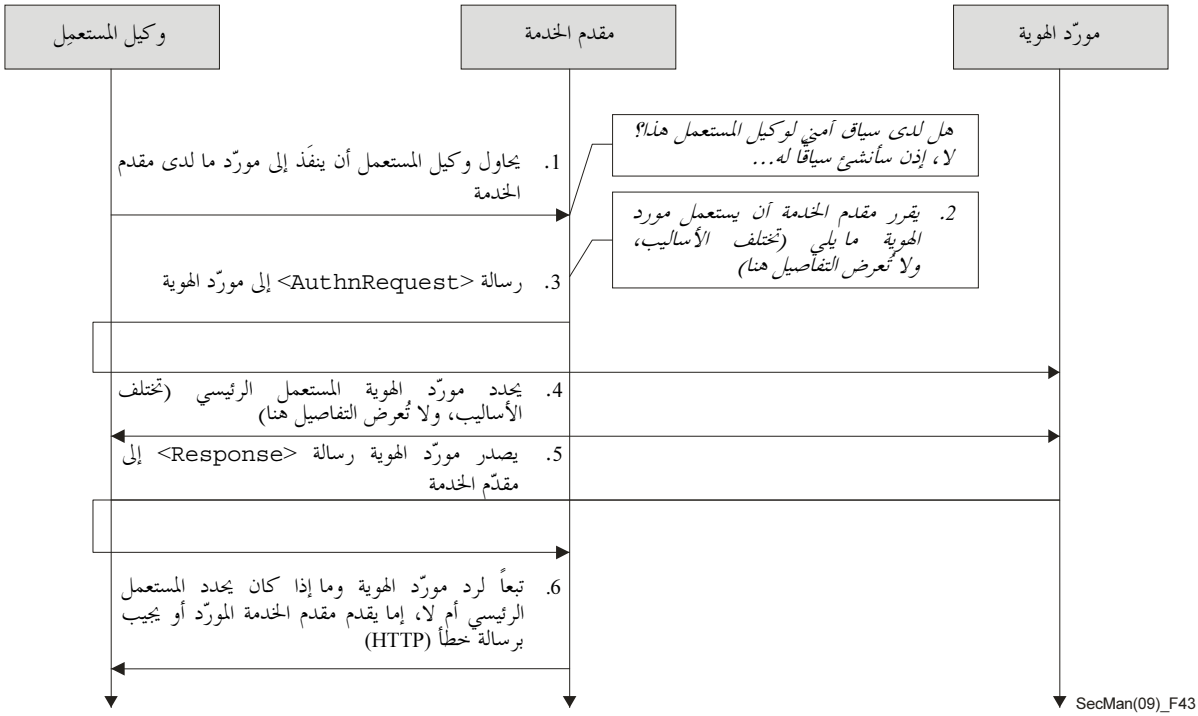
وعادة ما تقدم تأكيدات بلغة ترميز تأكيد الأمن (SAML) حول *موضوع ما*. وهناك عدد من مقدمي الخدمة نمطياً ممن يمكنهم الاستفادة من التأكيدات بشان موضوع معين للتحكم في النفاذ وتقديم طلبات حسب الطلب. وعليه، فهم يصبحون أطرافاً معتمِدة على الطرف المؤكد المدعو *مقدم الهوية*.

وتعرّف توصية قطاع تقييس الاتصالات X.1141 يحدد ثلاثة أنواع مختلفة من بيانات التأكيد التي يمكن أن تصدر عن سلطة لغة ترميز تأكيد الأمن (SAML)، وترتبط جميعها بموضوع ما. أما الأنواع الثلاثة من البيانات المحددة في توصية قطاع تقييس الاتصالات X.1141، فهي كالتالي:

- الاستيقان: هو الاستيقان من موضوع التأكيد بوسيلة معينة في وقت معين؛
- والنعت: هو ارتباط موضوع التأكيد بالنعوت المورَّدة؛
- وقرار التخويل: هو طلب بالسماح لموضوع التأكيد بالنفاذ إلى مورد محدد تم منحه أو حجبه.

وتعرّف توصية قطاع تقييس الاتصالات X.1141 أيضاً بروتوكولَ يمكن لزبون بواسطته أن يطلب تأكيدات من سلطات لغة ترميز تأكيد الأمن (SAML)، وأن يحصل على رد منها. ويمكن لهذا البروتوكول، المؤلف من أنساق طلب قائم على لغة الترميز القابلة للتوسيع (XML) ورسالة الرد عليه، أن يُسند إلى العديد من الاتصالات المختلفة الكامنة وبروتوكولات النقل. وإذ تصيغ سلطات لغة ترميز تأكيد الأمن ردودها، يمكنها أن تستعمل مختلف مصادر المعلومات مثل مخازن سياسات خارجية وتأكيدات وردت كمساهمة ضمن الطلبات.

وتُعرَّف مجموعة مواصفات دعماً للدخول الواحد (SSO) للمتصفحين وأجهزة الزبائن الأخرى. ويبين الشكل 43 النموذج الأساسي لتحقيق الدخول الواحد (SSO).



الشكل 43 – الأنموذج الأساسي لتحقيق الدخول الواحد (SSO)

2.4.9 لغة ترميز التحكم في النفاذ القابلة للتوسيع

تندرج لغة ترميز التحكم في النفاذ القابلة للتوسيع (XACML) في مفردات لغة الترميز القابلة للتوسيع (XML) للتعبير عن سياسات تحكم في النفاذ مآلها اتخاذ قرار بشأن ما إذا كان ينبغي الموافقة على طلب بالنفاذ إلى مورد، وإنفاذ ذلك القرار. وتعرِّف توصية قطاع تقييس الاتصالات X.1142 لغة ترميز التحكم في النفاذ القابلة للتوسيع الأساسية، بما في ذلك نماذج تركيب اللغة ونموذج لغة السياق المحتكم إلى سياسة معينة وقواعد التركيب والمعالجة. وتعزيزاً لأمن تبادل السياسات القائمة على لغة ترميز التحكم في النفاذ القابلة للتوسيع، توصِّف التوصيةُ X.1142 أيضاً مواصفة التوقيع الرقمي بلغة الترميز القابلة للتوسيع في لغة ترميز التحكم في النفاذ القابلة للتوسيع من أجل تأمين البيانات. وتوصَّف مواصفة الخصوصية لتوفير مبادئ توجيهية للمنفذين. وتُعد لغة ترميز التحكم في النفاذ القابلة للتوسيع مناسبة لمجموعة متنوعة من بيئات التطبيقات.

5.9 الخدمات القائمة على الوسم

يجري نشر وسوم التعرّف (بما فيها وسوم التعرف بواسطة الترددات الراديوية (RFID)) على نطاق واسع، غير أن القلق يتزايد بشأن مخاطر انتهاك الخصوصية. ويرجع ذلك جزئياً إلى قدرة تكنولوجيا التعرف بواسطة الترددات الراديوية على جمع البيانات ومعالجتها تلقائياً وما يرافق ذلك من مخاطر الكشف المتعمد أو العرضي عن معلومات حساسة و/أو شخصية.

والتطبيقات التي تستخدم التعرف القائم على الوسم أو تعتمد عليه في مجالات تتضمن معلومات شخصية، مثل الرعاية الصحية وجوازات السفر ورخص القيادة، صارت قضية الخصوصية فيها مشكلة تتفاقم باستمرار.

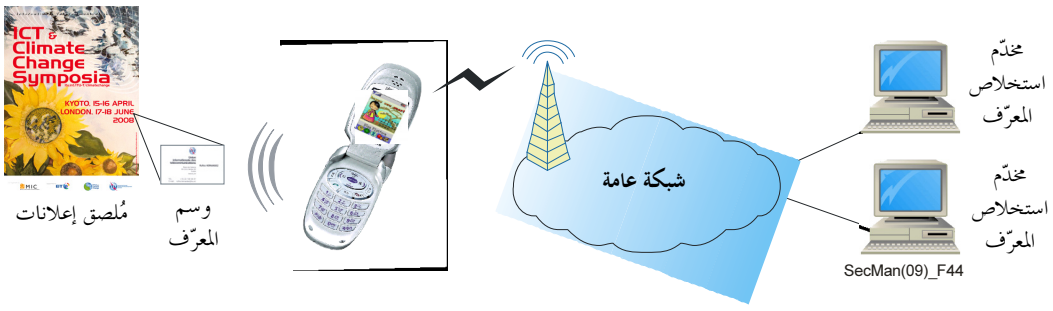
وفي الأوساط الأكاديمية والصناعية، انصبت معظم الجهود الرامية إلى إيجاد آلية لحماية المعلومات التي يمكن تعرّف هوية أصحابها شخصياً (PII) باتجاه بروتوكولات الاستيقان ما بين وسم الهوية ومطراف الهوية. ومع ذلك، فإن هذه الجهود

لا تعالج المشكلة تماماً، إذ تبقى في المخدم في ميدان الشبكة معلومات مفيدة عن المعرّف. ويتمثل أحد حلول هذه المشكلة في استعمال آلية تقوم على مواصفة لحماية المعلومات التي يمكن تعرّف هوية أصحابها شخصياً.

أما توصية قطاع تقييس الاتصالات X.1171 بعنوان: *التهديدات ومتطلبات حماية المعلومات التي يمكن تعرّف هوية أصحابها شخصياً في التطبيقات التي تستعمل تعرّف الهوية على أساس الوسم*، فهي تدرس التهديدات التي تتعرض لها المعلومات التي يمكن تعرّف هوية أصحابها شخصياً في بيئة اتجاهها من مصلحة الأعمال إلى الزبون، وتستعمل فيها التطبيقات التعرّف القائم على الوسم. وتحدد متطلبات حماية هذه المعلومات في مثل تلك البيئات، وتحدد الهيكل الأساسي لحماية هذه المعلومات استناداً إلى مواصفة لسياسة يحددها المستعمل بشأن المعلومات التي يمكن تعرّف هوية أصحابها شخصياً (PII).

ويمكن تصنيف التطبيقات التي تتوجه من مصلحة الأعمال إلى الزبون وتستعمل التعرّف القائم على الوسم ضمن ثلاثة أنماط:

أ) *مستعمل الجهاز بوصفه زبوناً*: في خدمة إيصال محتوى المعلومات، يستخرج الزبون المعلومات بواسطة جهاز القارئ بحوزته. وفي هذا النمط من الخدمة، يمكن أن يفترض معظم مقدمي خدمة التطبيق أن لدى الزبون مطراف متنقل مجهز بجهاز قارئ. ويبين الشكل 44 يظهر النموذج الأساسي لهذا النمط من التطبيقات. وهو يتألف من عمليتين أساسيتين في الشبكة: استخلاص المعرّف واستخراج المحتوى. وأما استخلاص المعرّف فهو إجراء ينطوي على ترجمة المعرّف إلى عنوان. فالمطراف المتنقل المجهز بقارئ يستخلص المعرّف أولا من وسمه عبر خدمة الدليل، ثم يقوم باستخراج المحتوى.



الشكل 44 – النموذج الأساسي لتطبيق متجه من مصلحة أعمال إلى الزبون باستعمال التعرّف القائم على الوسم

ب) *مستعمل وسم الهوية بوصفه زبوناً*: إن المثال النمطي لهذا التطبيق المتجه من مصلحة الأعمال إلى الزبون باستعمال التعرّف القائم على الوسم يتناول التحكم في النفاذ و/أو الاستيقان، ومثال ذلك، التحقق من مدخل أو جواز السفر أو الترخيص أو خدمة الإدارة ما بعد البيع. وفي هذا النمط من التطبيقات تكون أجهزة القارئ من نمط المطراف الثابت و/أو نمط المطراف المتحرك. وقد لا يحتاج الزبون إلى جهاز قارئ خاص به.

ج) *الزبون بوصفه مستعمل وسم الهوية مستعمل الجهاز على السواء*: في خدمة استخراج معلومات المنتَج، يصبح الزبون مستعمل وسم كذلك لدى شراء المنتج الموسوم وبعد تصفح محتويات معلومات المنتج من مطرافه الجوال. وفي مثال آخر، يمكن النظر في خدمة على صلة بالرعاية الصحية تحركها بطاقة مريض مفعّلة بوسم الهوية. وفي هذا التطبيق، تتعدد أنواع الزبائن ممن يمكن أن يستعملوا وسم الهوية (ومثالهم، المريض والطبيب والممرضة). ويمكن لمستعمل وسم الهوية أن يتصفح ما يخصه في سجلات المرضى من خلال مطراف متنقل مزود بجهاز قارئ فيقرأ بطاقة المريض الخاصة به المفعّلة بوسم الهوية.

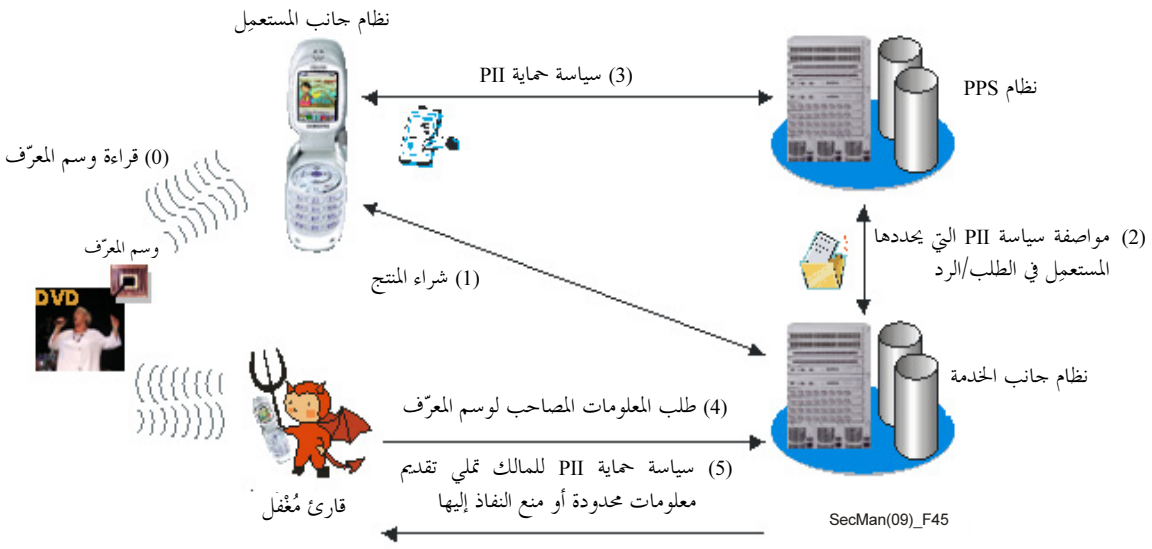
وفي التطبيقات المتجهة من مصلحة الأعمال إلى الزبون باستعمال التعرّف القائم على الوسم، يبرز خطران رئيسيان بشأن انتهاك المعلومات التي يمكن تعرّف هوية أصحابها شخصياً (PII):

- تسرب المعلومات المرتبطة بالمعرف: وفي هذه الحالة، يمكن للمهاجم قراءة المعلومات من وسم الهوية دون علم مستعمل المنتج الموسوم. فأولاً، يقرأ المهاجمُ المعرفَ من وسم الهوية الذي يحمله المستعمل. ثم يستخلص المعرّف ويستعلم عن موقع المعلومات من خدمة الدليل. وأخيراً، يطلب المهاجم معلومات مرتبطة بوسم الهوية.
- تسرب بيانات السياق التاريخي: يمكن للمهاجم أن يستخرج بيانات المستعمل (مثل أموره المفضلة وعاداته ومجالات اهتمامه، وما إلى ذلك) من بيانات السياق التاريخي المرتبطة بسمة الهوية.وقد يستعمل المهاجم هذه البيانات لأغراض غير قانونية أو تجارية دون موافقة المستعمل.

وتصف توصية قطاع تقييس الاتصالات X.1171 المتطلبات التقنية التالية للوقاية من انتهاكات المعلومات التي يمكن تعرّف هوية أصحابها شخصياً (PII) في التطبيقات المتجهة من مصلحة الأعمال إلى الزبون:

- *تحكم مستعمل وسم الهوية في المعلومات التي يمكن تعرّف هوية أصحابها شخصياً (PII)*: يتعين على مستعمل وسم الهوية أن يكون قادراً على إدارة أو تحديث المعلومات التي يمكن تعرّف هوية أصحابها شخصياً المرتبطة بوسم هويته على الشبكة. وبهذه الطريقة، يمكن لمستعمل وسم الهوية أن يحدد أي من هذه المعلومات ينبغي حذفها أو الاحتفاظ بها في التطبيق.
- *الاستيقان من مستعمل وسم هوية و/أو مستعمل جهاز*: يتعين على مخدّم التطبيق أن يوفر إجراءات استيقان لمستعمل وسم هوية، ويمكن لمخدّم التطبيق أن يوفر إجراءات استيقان لمستعمل الجهاز إذا لزم الأمر (بعض التطبيقات التي تستعمل التعرف القائم على الوسم ليست ملزمة بالاستيقان من المستعمل).
- التحكم *في النفاذ إلى المعلومات التي يمكن تعرّف هوية أصحابها شخصياً (PII) لمستعمل وسم الهوية في مخدم تطبيق*: يتعين على مخدم التطبيق أن يتحكم في النفاذ إلى المعلومات الهامة المتصلة بتلك التي يمكن تعرّف هوية أصحابها شخصياً والخاصة بمستعمل وسم الهوية.
- *سرية البيانات للمعلومات المرتبطة بوسم هوية*: يتعين على مخدم التطبيق أن يوفر بيانات السرية لضمان عدم تمكن مستعملين غير مخولين من قراءة المعلومات المرتبطة بوسم هوية.
- *الموافقة على جمع بيانات السجل المتصلة بمستعمل جهاز*: يمكن لمخدم التطبيق أن يوفر إجراءات الموافقة على جمع بيانات السجل المتصلة بمستعمل جهاز، إذا ما دعت ضرورات التطبيق إلى هذا النمط من جمع بيانات السجل.

ويوضح المثال التالي خدمة حماية المعلومات التي يمكن تعرّف هوية أصحابها شخصياً (PPS) بناءً على مواصفة السياسة الناظمة لهذه المعلومات لدى المستعمل. ويتأتى سيناريو هذه الخدمة من إجراء تخصيص الوسم كما في شراء منتج موسوم. ويبين الشكل 45 الانسياب العام لخدمة حماية المعلومات التي يمكن تعرّف هوية أصحابها شخصياً (PPS) في تطبيق يستعمل التعرف القائم على الوسم.



الشكل 45 – الانسياب العام لخدمة حماية المعلومات التي يمكن تعرّف هوية أصحابها شخصياً (PPS)

1) يقرأ المستهلك المعرفَ من المنتج الموسوم بواسطة مطرافه المتنقل المجهز بجهاز قارئ.

2) يستعرض المستهلك المعلومات ذات الصلة بالمنتج من شبكة خدمة التطبيق، ويشتري المنتج لاحقاً باستعمال إحدى طرائق الدفع المختلفة. وآنئذ، يصبح المستهلك مستعمل وسم الهوية.

3) ثم يطلب التطبيق الذي يستعمل تعرّف قائم على الوسم مواصفةَ السياسة الناظمة للمعلومات التي يمكن تعرّف هوية أصحابها شخصياً (PII) من النظام الحامي لهذه المعلومات، ويرد هذا النظام على التطبيق مقدماً المواصفة التي حددها المستعمل.

4) يتلقى نظام خدمة حماية المعلومات التي يمكن تعرّف هوية أصحابها شخصياً (PPS) سياسة المستعمل الناظمة لحماية هذه المعلومات في هذا التطبيق.

5) يمكن لأي كان أن يطلب المعلومات المرتبطة بوسم الهوية هذا من نظام الجانب الخدمي.

6) يمكن لصاحب الطلب، إذا كان هو مستعمل وسم الهوية، أن يستعرض جميع المعلومات التي يوفرها نظام الجانب الخدمي. وفيما عدا ذلك، إما أن يتعذر على صاحب الطلب النفاذ إلى أية معلومة، أو إنه لا يحصل إلا على قدر محدود من المعلومات.

10. التصدي للتهديدات الشائعة في الشبكة

10 التصدي للتهديدات الشائعة في الشبكة

تتعدد وتتنوع التهديدات التي تحدق بأنظمة الحاسوب وبالشبكات التي توصل فيما بينها. ورغم إمكانية إطلاق العديد من الهجمات محلياً، فإن الغالبية العظمى من هجمات اليوم تُشن عبر شبكات الاتصالات. وتزداد كثيراً سهولة واحتمالات الهجمات التي تُشن عن بعد والعشوائية في كثير من الأحيان، جراء الجموع الغفيرة والمتزايدة من الحواسيب وأجهزة الشبكة الموصولة بالإنترنت التي يشغلها من المنازل وأماكن العمل أشخاص قليلو التدريب أو الوعي أو المعرفة بأمن تكنولوجيا المعلومات. وتُنشر الرسائل الاقتحامية والبرمجيات التجسسية ونواقل الهجمات الأخرى بأعداد ما برحت تتعاظم. وغالباً ما يعتمد المهاجمون على أنظمة ضعيفة تعوزها الحماية الكافية كمعابر لبرمجياتهم الخبيثة.

وتُعرض في هذا القسم لمحة عامة عن العمل الجاري في قطاع تقييس الاتصالات للرد على هذه التهديدات.

1.10 التصدي للرسائل الاقتحامية

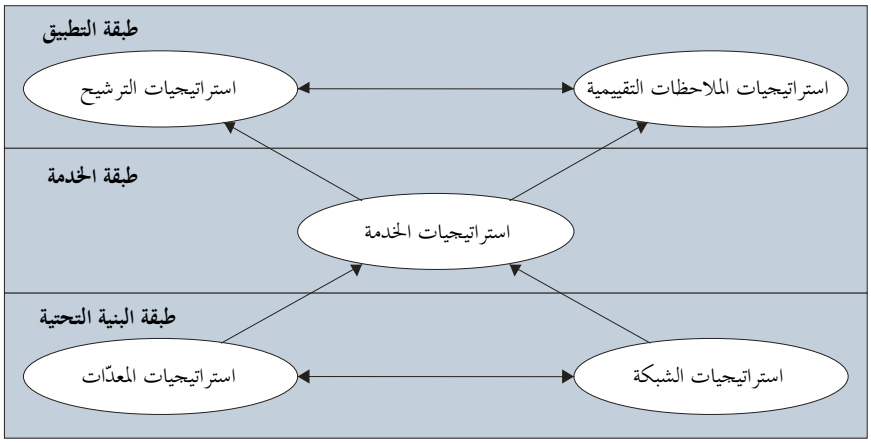
تُعرف الرسائل الاقتحامية (أي البريد الإلكتروني الطفيلي غير المرغوب فيه) على نطاق واسع باعتبارها مشكلة رئيسية لمستعملي الشبكة والشبكة ومقدمي الخدمات. فالرسائل الاقتحامية تتداخل مع عمليات مشروعة وتستهلك من عرض النطاق ودورات المعالجة، وفي الحالات القصوى، يمكنها أن تفضي إلى هجمات تحرم المستعمل من الخدمة بإغراق الشبكات. ويجري استخدام تدابير قانونية وتقنية على السواء في التصدي للرسائل الاقتحامية بدرجات متفاوتة من الفعالية. ولا يوجد تدبير معين ضد الرسائل الاقتحامية يحقق الفعالية بمفرده، نظراً لسرعة تحرك مرسلي الرسائل الاقتحامية وسعة حيلتهم؛ فحتى اعتماد مجموعة من التدابير لا يفلح غالباً إلا في التخفيف من كمية الرسائل الاقتحامية. ومن أمثلة التدابير التي يُلجأ إليها: التنظيم؛ والتدابير التقنية بما فيها ترشيح الرسائل الاقتحامية؛ والتعاون الدولي؛ وتثقيف المستعملين ومقدمي خدمات الإنترنت.

ويركز عمل قطاع تقييس الاتصالات في مجال التصدي للرسائل الاقتحامية بالدرجة الأولى على الجوانب التقنية لهذه المشكلة. لذا، ينصرف التركيز في هذا القسم إلى الوسائل التقنية لمكافحة الرسائل الاقتحامية وإلى تطوير وتطبيق تكنولوجيات مضادة للرسائل الاقتحامية.

1.1.10 الاستراتيجيات التقنية في التصدي للرسائل الاقتحامية

تحدد توصية قطاع تقييس الاتصالات X.1231، بشأن الاستراتيجيات التقنية في التصدي للرسائل الاقتحامية، متطلبات مكافحة الرسائل الاقتحامية كمنطلق العمل. وتصف هذه التوصية الأنماط المختلفة للرسائل الاقتحامية وخصائصها المشتركة وتقدم لمحة عامة عن النهج التقنية في التصدي للرسائل الاقتحامية. كما تقترح نموذجاً عاماً يمكن استعماله لوضع استراتيجية فعالة لمكافحة الرسائل الاقتحامية.

وهذا النموذج تراتبي وله خمس استراتيجيات موزعة على ثلاث طبقات. ويبين الشكل 46 العلاقات بين الاستراتيجيات. ويبين النموذج وجود درجة عالية من الترابط بين الاستراتيجيات، إلا أن اعتبارات التكلفة قد تحول دون استخدام جميع الاستراتيجيات في الحالات الفردية. ولا بد أيضاً من تكييف الاستراتيجيات وفقاً لسيناريو تطبيق معين.



SecMan(09)_F46

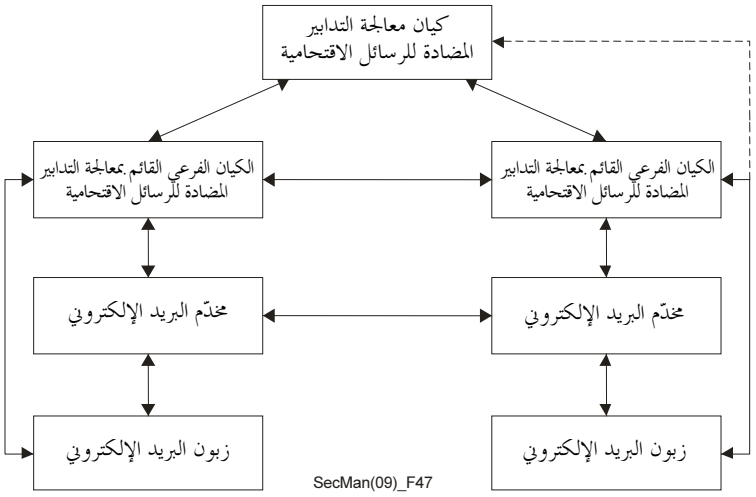
الشكل 46 – النموذج العام للتصدي للرسائل الاقتحامية

2.1.10 الرسائل الاقتحامية في البريد الإلكتروني

تُعرف الرسائل الاقتحامية، أكثر ما تُعرف، في البريد الإلكتروني. وهي تشكل تحديات تقنية معقدة تحتاج حلول التخلص منها لأن تُدعم بالتدابير التقنية المناسبة. وفيما تعد الإجراءات والتشريعات الحكومية عاملاً مساعداً، فهي لا تكفي لمواجهة التحديات التي تطرحها الرسائل الاقتحامية في البريد الإلكتروني. ومما يعقد المشكلة صعوبة تحديد مرسلي الرسائل الاقتحامية عند استعمال بروتوكول نقل البريد البسيط (SMTP).

وقد أُعدت توصيتان للمساعدة في التصدي للرسائل الاقتحامية. فتوصية قطاع تقييس الاتصالات X.1240 بشأن *التكنولوجيات التي ينطوي عليها التصدي للرسائل الاقتحامية*، تتوجه إلى المستعملين الراغبين بوضع الحلول التقنية لمكافحة الرسائل الاقتحامية. وهي تحدد المفاهيم الأساسية والخصائص والآثار والقضايا التقنية المرتبطة بالتصدي للرسائل الاقتحامية. كما أنها تحدد الحلول التقنية الحالية والأنشطة المتصلة بها من منظمات وضع المعايير وغيرها من الجماعات التي تعمل على التصدي للرسائل الاقتحامية.

أما توصية قطاع تقييس الاتصالات X.1241 بعنوان: *الإطار التقني للتصدي للرسائل الاقتحامية في البريد الإلكتروني*، فهي تصف هياكل توصي بها لميدان معالجة مكافحة الرسائل الاقتحامية، وتعرّف العناصر الوظيفية للوحدات الرئيسية في الميدان. ويؤسس الإطار آلية لتبادل المعلومات بشأن الرسائل الاقتحامية في البريد الإلكتروني بين مختلف مخدّمات البريد الإلكتروني. وتهدف التوصية لتشجيع المزيد من التعاون بين مقدمي الخدمات في التعامل مع الرسائل الاقتحامية. وعلى وجه الخصوص، فهي توفر إطاراً لتمكين منهجية اتصالات تحذر من رسائل اقتحامية تم التعرّف عليها. وهناك وثيقة أخرى، وهي إضافة إلى السلسلة X.1240 من *توصيات قطاع تقييس الاتصالات بشأن التصدي للرسائل الاقتحامية وما يرتبط بها من تهديدات*، وتستعرض هذه الوثيقة المحافل الدولية التي تعالج الرسائل الاقتحامية، كما تتضمن دراسة حالة.



الشكل 47 – الهيكل العام لميدان معالجة التصدي للرسائل الاقتحامية في البريد الإلكتروني

يوضح الشكل 47 عمليات الإطار الوارد في توصية قطاع تقييس الاتصالات X.1241. ويقع الكيان الذي يعالج مكافحة الرسائل الاقتحامية في نظام مستقل، فيما توجد الكيانات الفرعية التي تعالج مكافحة الرسائل الاقتحامية لدى واحد أو أكثر من مقدمي خدمة البريد الإلكتروني. ويسلم الكيان المعالج قواعد جديدة إلى الكيانات الفرعية التي يتعين عليها التحقق من هذه القواعد وتحسينها. كما توجد وظيفة لتسوية أي تضاربات في القواعد.

3.1.10 الرسائل الاقتحامية في الوسائط المتعددة القائمة على بروتوكول الإنترنت

إن توصية قطاع تقييس الاتصالات X.1244، بعنوان *الجوانب العامة لمكافحة الرسائل الاقتحامية في تطبيقات الوسائط المتعددة القائمة على بروتوكول الإنترنت*، تحدد المفاهيم الأساسية والخصائص والقضايا التقنية ذات الصلة بالتصدي للرسائل الاقتحامية في الوسائط المتعددة القائمة على بروتوكول الإنترنت مثل المهاتفة القائمة على بروتوكول الإنترنت والرسائل الفورية. وتُصنَّف الأنماط المتنوعة من الرسائل الاقتحامية في تطبيقات الوسائط المتعددة القائمة على بروتوكول الإنترنت، وتوصف، وفقاً لخصائصها. ويصف المعيار مختلف التهديدات الأمنية التي يمكن أن تتسبب برسائل اقتحامية في تطبيقات الوسائط المتعددة القائمة على بروتوكول الإنترنت، ويحدد الجوانب التي ينبغي أخذها في الاعتبار في التصدي لمثل هذه الرسائل الاقتحامية. كما يمكن استعمال بعض التقنيات المعدة لضبط الرسائل الاقتحامية في البريد الإلكتروني للتصدي للرسائل الاقتحامية في الوسائط المتعددة القائمة على بروتوكول الإنترنت. وتحلل توصية قطاع تقييس الاتصالات X.1244 الآليات التقليدية للتصدي للرسائل الاقتحامية، وتبحث إمكانية تطبيقها لمكافحة الرسائل الاقتحامية في الوسائط المتعددة القائمة على بروتوكول الإنترنت.

ويمكن تطبيق تقنيات مكافحة الرسائل الاقتحامية في الوسائط المتعددة القائمة على بروتوكول الإنترنت وفقاً للخصائص المحددة للرسائل الاقتحامية. ويبين الجدول 7 التصنيف المستعمل في توصية قطاع تقييس الاتصالات X.1244.

الجدول 7 – تصنيف الرسائل الاقتحامية في تطبيقات الوسائط المتعددة القائمة على بروتوكول الإنترنت

	نصوص	صوت	فيديو
في الوقت الفعلي	• الرسائل الاقتحامية في الرسائل الفورية • الرسائل الاقتحامية في الدردشة	• الرسائل الاقتحامية في VoIP • الرسائل الاقتحامية في الرسائل الفورية	• الرسائل الاقتحامية في الرسائل الفورية
في غير الوقت الفعلي	• الرسائل الاقتحامية في الرسائل النصية/متعددة الوسائط • رسائل اقتحامية نصية عبر خدمة تشارك بالملفات بين ندين • رسائل اقتحامية نصية في موقع الويب	• الرسائل الاقتحامية في الرسائل الصوتية/متعددة الوسائط • رسائل اقتحامية صوتية عبر خدمة تشارك بالملفات بين ندين • رسائل اقتحامية صوتية في موقع الويب	• الرسائل الاقتحامية في الرسائل الفيديوية/متعددة الوسائط • رسائل اقتحامية فيديوية عبر خدمة تشارك بالملفات بين ندين • رسائل اقتحامية فيديوية في موقع الويب

4.1.10 الرسائل الاقتحامية في خدمة الرسائل القصيرة (SMS)

إن توصية قطاع تقييس الاتصالات X.1242، بعنوان: *نظام ترشيح الرسائل الاقتحامية في خدمة الرسائل القصيرة (SMS) على أساس قواعد يحددها المستعمل*، تحدد هيكل ووظائف نظام ترشيح الرسائل الاقتحامية في خدمة الرسائل القصيرة إلى جانب إدارة خدمة المستعمل وبروتوكولات الاتصال والمتطلبات الوظيفية الأساسية للمطاريف ذات وظائف الرسائل القصيرة. وتحدد الطرائق التي يمكن للمستعملين بواسطتها إدارة (استعلام وحذف واستعادة) الرسائل القصيرة المرشحة. ويمكن أن يستند الترشيح إلى خصائص مثل العنوان أو رقم الهاتف أو الوقت أو المحتوى. وترد في تذييل توصية قطاع تقييس الاتصالات X.1242 متطلبات برمجيات المطراف لدعم ترشيح الرسائل الاقتحامية في خدمة الرسائل القصيرة.

2.10 الشفرات الضارة وبرمجيات التجسس والبرمجيات الخادعة

لعلّ الخطر الأكبر الذي يهدد الأنظمة والشبكات يأتي من الشفرات الضارة (الفيروسات والديدان وأحصنة طروادة، وغيرها)، لكن برمجيات التجسس والبرمجيات الخادعة الأخرى (أي البرمجيات التي تؤدي أنشطة غير مصرح بها) تشكل أيضاً خطراً لا يُستهان به. وما لم تنفذ المنظمات والأفراد مجموعة من التدابير الاستباقية (بما في ذلك جدران الوقاية والتدابير المضادة للفيروسات والتدابير المضادة للبرمجيات التجسسية) ضد هذه التهديدات، فإن اختراق أجهزتهم الحاسوبية مؤكد عملياً. بيد أن التدابير المضادة المتاحة تختلف من حيث الفعالية ولا تتكامل دوماً فيما بينها.

وعلى نحو متزايد، تطالب الهيئات التنظيمية في العديد من البلدان ضمانات من مقدمي الخدمات بشأن تدابير الأمن والسلامة التي اتخذوها، وتتطلب من مقدمي الخدمات بذل المزيد من الجهد لمساعدة المستعملين على تحقيق استعمال سالم وآمن للإنترنت.

تُعد توصية قطاع تقييس الاتصالات X.1207، بعنوان: *مبادئ توجيهية لمقدمي خدمات الاتصالات للتصدي لمخاطر برمجيات التجسس والبرمجيات المحتملة غير المطلوبة*، معياراً يهدف إلى ما يلي:

أ) تعزيز الممارسات الفضلى فيما يتعلق بالإخطارات الواضحة وموافقات المستعملين وتحكم المستعملين لخدمات استضافة مواقع الويب؛

ب) تعزيز الممارسات الأمنية الفضلى (عن طريق مقدمي خدمات الاتصالات) لدى المستعملين المنـــزليين بشأن الاستعمال السالم والآمن للحواسيب الشخصية والإنترنت.

وتوفر توصية قطاع تقييس الاتصالات X.1207 توجيهات واضحة لمقدمي الخدمة بشأن إدارة المخاطر الأمنية والاستعمال السالم والآمن للمنتجات ومراقبة الشبكة والاستجابة والدعم والتحديث في الوقت المناسب وتأمين استضافة مواقع الويب. وتُقدم المشورة بشأن توجيه المستعمل وتثقيفه وبشأن تدابير الحماية التقنية للمستعملين النهائيين. ويرد تذييل غير مكمل يوفر وصلات لمواد إضافية من الموارد.

3.10 التبليغ عن التحديثات البرمجية ونشرها

يمكن للشفرة الضارة أن تنتشر بسرعة مقلقة. وحتى بوجود أرقى تدابير الحماية، يمكن للتهديدات الجديدة أن تنتشر بسرعة تعرض للخطر الأنظمة والشبكات التي لا تحوي آخر التحديثات. ويكون تعرضها للخطر على أشده في "اليوم الصفر" (أي في الوقت الذي لم يوضع فيه بعد توقيع أو رقعة مضادة للفيروس لدى ظهور تهديدات جديدة أو لا سابق معرفة بها). وفي هذه البيئة، من الأهمية بمكان أن تُوزع التحديثات وتُركب في وقتها. غير أن عدداً من المشاكل يكتنف توزيع هذه التحديثات وتنفيذها.

وتحوي غالبية البرمجيات الجاهزة، بما في ذلك أنظمة التشغيل والأنظمة المصممة لتوفير الحماية الأمنية (مكافحة الفيروسات ومكافحة التجسس وجدران الوقاية وما إلى ذلك)، ميزة تسمح بالتحديث التلقائي، ولكن على المستعمل أن يفعلها. وحيثما لا يتعدى الأمر تبليغ المستعمل بتوفر التحديثات (أو ربما بأن التحديثات قد حُمِّلت)، على المستعمل أن يبادر إلى السماح بتحميل و/أو تثبيت هذه التحديثات. وتتطلب العديد من التحديثات أن يعاد تشغيل الأنظمة بعد التثبيت، وهو أمر قد يقوم به المستعمل فوراً أو قد يؤجله. وفي المنظمات التي تحسن إدارة برنامج الأمن، تُدار التحديثات مركزياً عادة، مما يفرض تحديث أنظمة المستعمل النهائي. وفي المقابل، يبقى تحديث الأنظمة الفردية (مثل الحواسيب المنـــزلية) والتحديث ضمن المنظمات الصغيرة أمراً عشوائياً تماماً.

والملاحظة الأخرى على التحديث الروتيني هو أن بائعي البرامج لا يتبعون ممارسات ثابتة لتبليغ المستعملين بتوفر التحديثات ولتحذيرهم من مغبة عدم تثبيت التحديثات. كما أنهم لا يلتزمون بطريقة موحدة لإطلاع المستعملين على آخر الممارسات الفضلى في الحفاظ على أمن البرمجيات. وبالإضافة إلى ذلك، لا توجد طريقة متسقة للتبليغ عن مشاكل يصادفها المستعمل بعد تنفيذ التحديث.

ويرد في توصية قطاع تقييس الاتصالات X.1206، بعنوان: *إطار محايد تجاه البائع للتبليغ الأوتوماتي بالمعلومات المتعلقة بالأمن ونشر التحديثات*، بحث في الصعوبات المرتبطة بمواكبة أحدث البرمجيات. وتعرض التوصية سبيلاً محايداً تجاه البائع لمعالجة المشاكل. فحالما تُسجل أصول المستعمل، يمكن أن تتوفر تلقائياً إلى المستعملين أو مباشرة إلى التطبيقات أحدث المعلومات عن نقاط الضعف مع رقع برمجية أو تحديثات. وتوفر التوصية إطاراً يمكن لأي بائع استعماله للتبليغ ولتقديم معلومات عن نقاط الضعف ولنشر الرقع البرمجية/التحديثات المطلوبة. كما تحدد نسق المعلومات الذي ينبغي استعماله ضمن المكونات وفيما بينها.

وتمكِّن توصية قطاع تقييس الاتصالات X.1206 مدراء النظام من معرفة حالة أي من الأصول التي يتولون المسؤولية عنها. فهي تصف إشكالات صيانة الأصول من منظور التعرّف على الأصول وكذلك من منظوري نشر المعلومات وإدارة الأنظمة/الشبكة. كما تورد شرحاً للأمن الذي ينبغي أن يؤخذ في الاعتبار في الإطار المحايد تجاه البائع.

وترد في توصية قطاع تقييس الاتصالات X.1206 تعاريف لهياكل بيانات المكونات اللازمة لهذا العمل، بما في ذلك الرسم التخطيطي ذو الصلة بلغة الترميز القابلة للتوسيع (XML)، إلى جانب نسق المعلومات الذي ينبغي استعماله ضمن المكونات المنفذة لهذا الإطار وفيما بينها.

11. مستقبل تقييس أمن تكنولوجيا المعلومات والاتصالات

11 مستقبل تقييس أمن تكنولوجيا المعلومات والاتصالات

على مدى ما يزيد عن ثلاثين عاماً، عكف قطاع تقييس الاتصالات على وضع معايير تكنولوجيا المعلومات والاتصالات. وقد تسارع هذا العمل كثيراً في السنوات الأخيرة مع النمو السريع في استخدام الإنترنت وغيرها من الشبكات، ومع إدراك الحاجة لحماية المستعملين والأنظمة من التهديدات للأمن المتعاظمة عدداً ونوعاً.

وقد ألقى هذا الدليل نظرة عامة واسعة على بعض المبادرات الرئيسية وإنجازات لجان الدراسات في قطاع تقييس الاتصالات فيما يتعلق بالأمن في مسعىً لتعميق الفهم بالعمل وتحدي القضايا التقنية الذي يواجهه مستعملو الشبكة ومنفذوها. ويُشجع القراء على أن يستفيدوا من الموارد الطائلة على الخط لقطاع تقييس الاتصالات كي يطلعوا على تفاصيل أوفى عن المواضيع المعروضة هنا، وأن يستعينوا بالتوصيات والوثائق الإرشادية لبناء بيئة أكثر أمناً ولتعزيز ثقة المستعمل في العمليات على الخط.

وفي الأفق المستقبلي، ستستمر شبكات الاتصالات وشبكات الحاسوب في التقارب. وستواصل شبكات الجيل التالي والخدمات القائمة على شبكة الإنترنت نموها السريع فتزداد أهميتها، وستظل التهديدات تستشري وسيبقى تصميم ووضع تدابير مضادة فعالة حيالها تحدياً ماثلاً. وسيتمثل تحدٍ آخر في تحقيق ما هو أفضل وأكثر أمناً في تصميم وتنفيذ الأنظمة والشبكات بحيث تتضاءل نقاط الضعف الكامنة.

والدول الأعضاء المائة وواحد وتسعون في الاتحاد الدولي للاتصالات ومعهم أكثر من خمسمائة وواحد وخمسين من أعضاء القطاعات سيستمرون في الاستجابة لهذه التحديات من خلال الاستمرار في وضع التوصيات والمبادئ التوجيهية التقنية بشأن الأمن ضمن برنامج عمل طموح نابع من احتياجات الأعضاء ويسترشد بالهيكل التنظيمي المؤسس في الجمعية العالمية لتقييس الاتصالات في عام 2008. وكلما أمكن ذلك، وللحد من الازدواجية في الجهود والتركيز على الموارد، سيتعاون قطاع تقييس الاتصالات مع منظمات أخرى تعمل في وضع المعايير لتحقيق حلول متوائمة بأكبر قدر ممكن من الكفاءة والسرعة.

12. مصادر معلومات إضافية

12 مصادر معلومات إضافية

يقدم هذا الدليل لمحة عامة واسعة عن أعمال الأمن في قطاع تقييس الاتصالات. ويمكن الحصول مجاناً على معلومات أوفى بكثير في تفاصيلها، بما في ذلك العديد من المعايير، عبر موقع قطاع تقييس الاتصالات على شبكة الإنترنت.

1.12 لمحة عامة عن أعمال لجنة الدراسات 17

بادئ ذي بدء، توفر صفحة الاستقبال للجنة الدراسات 17 وصلات إلى معلومات عن أعمال لجنة الدراسات 17، بما في ذلك البرامج التعليمية والعروض وملخصات للتوصيات قيد الإعداد والموظفون الرئيسيون. أما الوصلتان إلى لجنة الدراسات الرئيسية المعنية بأمن الاتصالات ولجنة الدراسات الرئيسية المعنية بإدارة الهوية (IdM)، فهما يوفران معلومات عن أنشطة لجنتي الدراسات الرائدتين وعن نتائج أعمالهما.

2.12 الخلاصة الوافية للأمن

تحوي الخلاصة الوافية معلومات متعلقة بالأمن في توصيات الاتحاد الدولي للاتصالات ومعلومات تتصل بأنشطة الأمن في الاتحاد. وهي تتألف من خمسة أجزاء يمكن تحميل كل منها:

- قائمة بالتوصيات الموافَق عليها المتعلقة بأمن الاتصالات، وهي تشمل تلك المعدة لأغراض الأمن وتلك التي تصف أو تستعمل وظائف تقع في مجال اهتمام الأمن واحتياجاته؛
- قائمة بتعاريف الأمن التي وافق عليها قطاع تقييس الاتصالات والمستخرجة من توصياته الموافَق عليها؛
- موجز عن لجان الدراسات في قطاع تقييس الاتصالات ممن تتصل أنشطتها بالأمن؛
- موجز عن التوصيات الخاضعة للمراجعة ضمن لجان الدراسات في قطاع تقييس الاتصالات لاعتبارات أمنية؛
- موجز عن أنشطة الأمن الأخرى في الاتحاد الدولي للاتصالات.

3.12 خارطة طريق معايير الأمن

خارطة طريق معايير الأمن هي مورد على الخط يوفر معلومات عن المعايير المعمول بها لأمن تكنولوجيا المعلومات والاتصالات وعن العمل الجاري في المنظمات الرئيسية لوضع المعايير. وعلاوة على المعلومات بشأن العمل الأمني لقطاع تقييس الاتصالات، تتضمن خارطة الطريق معلومات عن أعمال معايير الأمن في المنظمة الدولية للتوحيد القياسي (ISO)/اللجنة الكهرتقنية الدولية (IEC) والتحالف لإيجاد حلول في صناعة الاتصالات (ATIS) والوكالة الأوروبية لأمن الشبكات والمعلومات (ENISA) ومعهد المهندسين الكهربائيين والالكترونيين (IEEE) وفريق مهام هندسة الإنترنت (IETF) ومنظمة النهوض بالمعايير الإعلامية المهيكلة (OASIS) ومشروع شراكة الجيل الثالث (3GPP) ومشروع شراكة الجيل الثالث 2 (3GPP2).

وشأنها شأن الخلاصة الوافية، تقع خارطة الطريق في خمسة أجزاء، ويمكن النفاذ إلى معظم معلوماتها مباشرة على الخط:

- الجزء 1، *منظمات وضع معايير تكنولوجيا المعلومات والاتصالات وأعمالها*، والذي يحتوي على معلومات بشأن هيكل خارطة الطريق وبشأن كل واحدة من منظمات المعايير المذكورة. كما ترد في الجزء 1 وصلات إلى مسارد ومفردات الأمن الموجودة؛
- الجزء 2، *معايير أمن تكنولوجيا المعلومات والاتصالات الموافَق عليها*، والتي تضم قاعدة بيانات يمكن البحث فيها لمعايير الأمن الموافَق عليها مع وصلات مباشرة إلى معظم المعايير؛

- الجزء 3، *معايير الأمن قيد الإعداد*؛
- الجزء 4، *الاحتياجات المستقبلية ومعايير الأمن الجديدة المقترحة*؛
- الجزء 5، *الممارسات الأمنية الفضلى*.

4.12 المبادئ التوجيهية لتنفيذ الأمن

ترد في الإضافة 3 لسلسلة توصيات قطاع تقييس الاتصالات X.849-X.800، إضافة بشأن المبادئ التوجيهية لتنفيذ أمن النظام والشبكة، معلومات أساسية بتفاصيل أوفى بشأن بعض المواضيع التي نوقشت في هذا الدليل، والمبادئ التوجيهية لتنفيذ أمن النظام والشبكة والتي يمكن استخدامها لتحقيق برنامج أمن شبكة. وتتناول هذه المبادئ التوجيهية أربعة مجالات: سياسة الأمن التقنية؛ وتحديد الأصول؛ والتهديدات ومواطن الضعف والتخفيف منها؛ وتقييم الأمن. وتبين المبادئ التوجيهية العناصر الرئيسية اللازمة لبناء وإدارة السياسة التقنية اللازمة لإدارة الشبكات التي يمكن أن تشمل عدة مشغلين وأن تحتوي على منتجات وأنظمة من باعة متعددين. كما أنها توفر المبادئ التوجيهية بشأن القضايا التنظيمية.

5.12 معلومات إضافية عن الدليل والاستيقان وإدارة الهوية

للاطلاع على معلومات أوفى بشأن سلسلة توصيات قطاع تقييس الاتصالات X.500، فإن مصدر المعلومات الموثوق هو سلسلة توصيات قطاع تقييس الاتصالات X.500 نفسها. ويمكن الاطلاع على معلومات تعليمية إضافية وعلى دليل المنفّذ في العنوان الإلكتروني: www.x500standard.com . وترد معلومات إضافية في الوصلات التالية:

الوصلة http://www.x500standard.com/index.php?n=X509.X509ProtectingDirectory ترد معلومات عن الاستيقان من المستعمل؛

والوصلة http://www.x500standard.com/index.php?n=X500.AccessControl ترد معلومات أوفى عن التحكم في النفاذ؛

والوصلة http://www.x500standard.com/index.php?n=X500.DataPrivacyProtection ترد وصفاً أكثر استفاضة لميزات خصوصية البيانات في توصيات X.500.

الملحق ألف – تعاريف الأمن

الملحـــق ألف

تعاريف الأمن

يحوي الجدول التالي تعاريف المصطلحات المستعملة في الدليل. وترد جميع التعاريف في التوصيات الراهنة لقطاع تقييس الاتصالات. وهنالك قائمة أشمل بتعاريف الأمن في الخلاصة الوافية لتعاريف الأمن التي وافق عليها قطاع تقييس الاتصالات والمستخرجة من توصيات هذا القطاع التي تحتفظ بها لجنة الدراسات 17.

المصطلح بالإنكليزية	المصطلح بالعربية	التعريف	المرجع
access control	التحكم في النفاذ	1. منع استخدام غير مرخص به لمورد ما، بما في ذلك منع استخدام مورد بطريقة غير مرخص بها. 2. قصر تدفق المعلومات من موارد نظام ما إلى أشخاص مرخص لهم أو برامج أو عمليات أو موارد نظام أخرى على الشبكة مرخص لها بذلك.	X.800 J.170
access control list	قائمة التحكم في النفاذ	قائمة بالكيانات المرخص لها بالنفاذ إلى مورد ما، مشفوعة بحقوق هذه الكيانات في النفاذ.	X.800
access control policy	سياسة التحكم في النفاذ	مجموعة القواعد التي تحدد الشروط التي يمكن أن يتم بموجبها أي نفاذ.	X.812
accidental threats	التهديدات العرضية	التهديدات التي تنشأ دون سابق قصد. ومن الأمثلة على التهديدات التي تتحقق عرضاً أعطال النظام وهفوات التشغيل وعيوب البرمجية.	X.800
accountability	المساءلة	الخاصية التي تضمن أن أعمال كيان ما يمكن تتبعها إلى ذلك الكيان فقط.	X.800
algorithm	خوارزمية	عملية رياضية يمكن استخدامها لتخليط تدفق البيانات وإزالة تخليطها.	J.93
attack	الهجوم	الأنشطة المضطلع بها لتجاوز أو استغلال جوانب القصور في آليات أمن النظام. وبالهجوم مباشرة على نظام ما، تستغل الأنشطة جوانب القصور في الخوارزميات أو المبادئ أو خصائص آلية الأمن في النظام. ويحدث الهجوم غير المباشر عندما تتجاوز الآلية أو عندما تجعل النظام يستخدم الآلية بطريقة غير صحيحة.	H.235
attribute	النعت	في سياق مناولة الرسائل، يكون النعت بند معلومات أو مكوّناً في قائمة نعوت يصف قائمة مستعمل أو قائمة توزيع كما يمكنه أيضاً أن يحدد موقعها بالنسبة إلى البنية المادية أو التنظيمية لنظام مناولة رسائل (أو الشبكة التي يستند إليها).	X.400
Attribute Authority (AA)	سلطة تحديد النعت (AA)	1. سلطة تعين امتيازات من خلال إصدار شهادات النعوت. 2. كيان موثوق به من كيان أو أكثر لاستحداث وتوقيع شهادات النعوت. ملاحظة – يمكن أن تقوم سلطة إصدار الشهادات بمهمة سلطة تحديد النعوت.	X.509 X.842
attribute certificate	شهادة النعت	هيكل بيانات وقعته رقمياً سلطة تحديد النعت ويربط بعض قيم النعوت بمعلومات تُعرِّف هوية حامليها.	X.509

المصطلح بالإنكليزية	المصطلح بالعربية	التعريف	المرجع
authentication	الاستيقان	1. عملية تأييد صحة هوية. ملاحظة – انظر الكيان الأصلي والمحقق وشكلي الاستيقان المميزين (استيقان أصل البيانات + استيقان الكيان). ويمكن أن يكون الاستيقان منفرداً أو متبادلاً. ويوفّر الاستيقان المنفرد تأكيد هوية كيان أصلي واحد فقط. ويوفّر الاستيقان المتبادل تأكيد هويتي كلا الكيانين الأصليين.	X.811
		2. توفير تأكيد للهوية المدّعاة لكيان ما.	X.811
		3. انظر استيقان أصل البيانات، واستيقان الكيان الند. ولا يُستخدم مصطلح "الاستيقان" فيما يتعلق بسلامة البيانات؛ إذ يُستخدم مصطلح "سلامة البيانات" بدلا منه.	X.800
		4. تأييد صحة هوية الأغراض ذات الصلة بإنشاء علاقة ترابط. وقد تشمل مثلاً استيقان الكيانات، واستيقان التطبيقات واستيقان الناس مستعملي التطبيقات. ملاحظة – عُرّف هذا المصطلح لتوضيح أن الأمر يتناول نطاق استيقان أوسع مما يشمله استيقان الكيان الند الوارد في التوصية X.800 للجنة الاستشارية الدولية للبرق والهاتف CCITT.	X.217
		5. عملية التحقق من الهوية المدّعاة من كيان لدى كيان آخر.	J.170
		6. العملية التي تهدف إلى تمكين النظام من التحقق يقيناً من هوية طرف ما.	J.93
authentication exchange	تبادل الاستيقان	1. آلية القصد منها التأكد من هوية كيان بواسطة تبادل المعلومات.	X.800
		2. تتابع لعملية نقل واحدة أو أكثر لتبادل معلومات الاستيقان لأغراض القيام بعملية استيقان.	X.811
authentication service	خدمة الاستيقان	توفر الدليل على أن هوية غرض أو موضوع هي حقاً الهوية المزعومة. وتبعاً لنمط الجهة الفاعلة وغرض تعرف الهوية قد يستدعي الأمر الأنواع التالية من الاستيقان: استيقان المستعمل، استيقان الكيان الند، استيقان أصل البيانات. ومن أمثلة الآلية المستخدمة في تنفيذ خدمة الاستيقان كلمات المرور وأرقام التعرف الشخصية (PINs) (والاستيقان البسيط) والطرائق المستندة إلى التجفير (الاستيقان القوي).	M.3016.2
authority	السلطة	كيان مسؤول عن إصدار الشهادات. وهنالك نوعان من السلطة؛ سلطة إصدار الشهادات التي تُصدر شهادات المفاتيح العمومية، وسلطة النعوت التي تصدر شهادات النعوت.	X.509
authorization	الترخيص	1. منح حقوق تشمل منح النفاذ استناداً إلى حقوق النفاذ. ملاحظة – ينطوي هذا التعريف ضمناً على حقوق أداء نشاط ما (مثل النفاذ إلى البيانات)؛ وعلى أن الحقوق مُنحت لعملية أو كيان أو فرد ما.	X.800
		2. منح الإذن على أساس هوية مستيقنة.	H.235
		3. عملية تمكين النفاذ إلى خدمة أو جهاز ما إذا كان لدى المرء تصريح بالنفاذ.	J.170
availability	التيسر	خاصية قابلية النفاذ والاستخدام عند الطلب من قبل كيان مرخص له بذلك.	X.800
capability	المقدرة	علامة تستخدم كمعرّف لمورد بحيث تضفي حيازة العلامة حقوق نفاذ إلى المورد.	X.800

المصطلح بالإنكليزية	المصطلح بالعربية	التعريف	المرجع
certificate	الشهادة	مجموعة من البيانات المتعلقة بالأمن تصدرها سلطة الأمن أو طرف ثالث موثوق به مع معلومات أمن تستخدم لتوفير سلامة البيانات وخدمات الاستيقان من أصل البيانات (شهادة الأمن – ITU-T X.810). وفي هذه التوصية يشير المصطلح إلى شهادات "المفاتيح العمومية" وهي قيم تمثل **مالكي** المفاتيح العمومية (ومعلومات اختيارية أخرى) كما تم الاستيقان منها ووقعتها سلطة موثوق بها في نسق لا يمكن تزويره.	H.235
certificate policy	سياسة الشهادة	مجموعة معينة من القواعد تشير إلى قابلية تطبيق الشهادة على مجموعة و/أو صنف معين من التطبيقات له متطلبات أمن مشتركة. فقد تشير سياسة شهادة معينة مثلاً إلى مدى قابلية تطبيق نمط شهادة ما على الاستيقان من معاملات تبادل البيانات الإلكترونية لتبادل البضائع في نطاق سعر معين.	X.509
Certificate Revocation List (CRL)	قائمة إبطال الشهادات	1. قائمة موقعة تضم مجموعة من الشهادات لم يعد يعتبرها مُصدر الشهادة صالحة. وبالإضافة إلى المصطلح العمومي لهذه القائمة، تعرف بعض أنواع محددة من هذه القائمة لتشمل مجالات معينة. 2. قائمة تشمل الأرقام المسلسلة للشهادات التي أُبطلت (لأن المفتاح أصبح مكشوفاً مثلاً أو لأن الشخص المعني لم يَعُد يعمل مع الشركة) والتي لم تنته فترة صلاحيتها بعد.	X.509 Q.817
Certification Authority (CA)	سلطة إصدار الشهادات	1. سلطة موثوق بها من قبل مستعمل أو أكثر لاستحداث وتخصيص شهادات مفاتيح عمومية. ويمكن لسلطة إصدار الشهادات، اختيارياً، أن تستحدث مفاتيح المستعملين. 2. كيان يوثق به (في سياق سياسة أمن) لإصدار شهادات أمن تحتوي على صنف أو أكثر من أصناف البيانات المتعلقة بالأمن.	X.509 X.810
ciphertext	نص التجفير	بيانات منتجة من خلال استخدام التجفير. ولا يتاح المحتوى الدلالي للبيانات الناتجة. ملاحظة – قد يخضع النص المُجفر نفسه للتجفير، بحيث يكون الناتج نصاً مضاعف التجفير.	X.800
cleartext	نص واضح	بيانات مفهومة يكون محتوى دلالاتها متاحاً.	X.800
confidentiality	السرية	ضمان عدم كشف المعلومات أو إتاحتها لأفراد أو كيانات أو عمليات غير مرخص لها بذلك.	X.800
confidentiality service	خدمة السرية	توفر خدمة السرية حماية من الكشف غير المرخص به للبيانات المتبادلة. ويميز بين الأنواع التالية من الخدمات السرية: سرية بحسب المجال؛ سرية التوصيل؛ سرية تدفق البيانات.	M.3016.2
credentials	بيانات التصديق	بيانات تنقل لإثبات هوية الكيان المدّعاة.	X.800
cryptanalysis	تحليل التجفير	1. تحليل نظام مجفر و/أو مدخلاته ومخرجاته لاستخراج متغيرات سرية و/أو بيانات حساسة بما في ذلك نص واضح. 2. عملية استرجاع نص عادي لرسالة أو مفتاح تجفير دون النفاذ إلى المفتاح. 3. علم استرجاع نص عادي للرسالة دون النفاذ إلى المفتاح (إلى المفتاح الإلكتروني في أنظمة التجفير الإلكترونية).	X.800 J.170 J.93
cryptographic algorithm	خوارزمية تجفير	وظيفة رياضية تحسب النتيجة من قيمة أو قيم عديدة مدخلة.	H.235

المصطلح بالإنكليزية	المصطلح بالعربية	التعريف	المرجع
cryptographic system, cryptosystem	نظام التجفير	1. مجموعة تحويلات من نص عادي إلى نص مجفر والعكس بالعكس، وتقوم المفاتيح بانتقاء التحويل (التحويلات) اللازمة. وتُعرّف التحويلات عادة بواسطة خوارزمية رياضية. 2. خوارزمية تحول بيانات مدخلة إلى شيء لا يمكن تمييزه (تجفير)، كما تُحول البيانات التي لا يمكن تمييزها إلى نسقها الأصلي (فك التجفير). ويرد وصف تقنيات التجفير RSA (ريفست وشامير وأدلمان) في توصية قطاع تقييس الاتصالات X.509	X.509 Q.815
cryptography	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).	X.800
data confidentiality	سرية البيانات	تستخدم لتوفير حماية البيانات من إفشاء غير مرخص به. وتعتمد خدمة سرية البيانات على إطار الاستيقان. ويمكن أن تستخدم للحماية من اعتراض البيانات.	X.509
data integrity	سلامة البيانات	ضمان عدم تغيير البيانات أو إتلافها بطريقة غير مرخص بها.	X.800
data origin authentication	الاستيقان من أصل البيانات	1. التأكد من أن مصدر البيانات المتلقاة هو المصدر المزعوم. 2. التأكد من هوية العنصر الرئيسي المسؤول عن وحدة بيانات محددة.	X.800 X.811
decipherment	فك التشفير	عكس عملية تشفير قابلة لذلك.	X.800
decryption	فك التجفير	انظر فك التشفير.	X.800
delegation	التفويض	نقل امتياز من كيان يتمتع به إلى كيان آخر.	X.509
denial of service	رفض الخدمة	منع نفاذ مرخص له إلى الموارد أو تأخير عمليات حرجة التوقيت.	X.800
digital signature	التوقيع الرقمي	1. بيانات ملحقة أو تحويل مجفر (انظر تجفير) لوحدة بيانات تسمح لمتلقي وحدة بيانات أن يبرهن على مصدر وسلامة وحدة البيانات وتحميها من التزوير، من جانب المتلقي مثلاً. 2. تحويل مجفّر لوحدة بيانات يسمح لمتلقي وحدة بيانات أن يبرهن على مصدر وسلامة وحدة البيانات ويحمي مرسل ومتلقي وحدة البيانات من التزوير من قبل أطراف ثالثة، ويحمي المرسل من التزوير من جانب المتلقي.	X.800 X.843
directory service	خدمة الدليل	خدمة البحث عن معلومات واسترجاعها من كتالوج أغراض محددة جيداً يمكن أن يتضمن معلومات عن الشهادات وأرقام الهواتف وظروف النفاذ والعناوين وغيرها. مثال ذلك خدمة الدليل التي تمتثل للتوصية ITU-T X.500.	X.843
eavesdropping	التنصت	انتهاك السرية بمراقبة الاتصال.	M.3016.0

المصطلح بالإنكليزية	المصطلح بالعربية	التعريف	المرجع
encipherment	التشفير	1. التحويل المجفر للبيانات (انظر علم التجفير) لإنتاج نص مجفر. ملاحظة – قد يكون التشفير غير قابل للعكس، وفي هذه الحالة لا يمكن إجراء عملية فك التشفير المقابلة. 2. التشفير (التجفير) عملية تجعل البيانات غير قابلة للقراءة من قبل كيانات غير مرخص لها بذلك، بواسطة تطبيق خوارزمية مجفرة. وفك التشفير (التجفير) عملية عكسية يتحول فيها نص مجفر إلى نص عادي.	X.800 H.235
encryption	التجفير	1. طريقة لترجمة معلومات في نص عادي إلى نص مجفر. 2. عملية تخليط إشارات لمنع النفاذ غير المصرح له. (انظر أيضاً التشفير)	J.170 J.93
end-to-end encipherment	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).	X.800
entity	كيان	1. إنسان أو منظمة أو مكوّن حاسوب أو جزء من برمجية. 2. أي شيء ملموس أو مجرّد ذو أهمية. وإذا كانت كلمة كيان تستخدم بوجه عام للإشارة إلى أي شيء فإنها في سياق النمذجة تقتصر على الإشارة إلى أشياء في نطاق الموضوع الذي يجري نمذجته.	X.842 X.902
entity authentication	استيقان الكيان	التأكد من هوية عنصر رئيسي في سياق علاقة اتصال. ملاحظة – لا يمكن استيقان هوية العنصر الرئيسي إلا عند تفعيل هذه الخدمة. ويمكن ضمان مواصلة الاستيقان بالطرائق الموصوفة في البند 7.2.5 في توصية قطاع تقييس الاتصالات X.811.	X.811
evidence	الإثبات	معلومات يمكن أن تستخدم، إما في حد ذاتها أو بالاقتران مع معلومات أخرى، لتسوية نزاع. ملاحظة – من أشكال الإثبات التوقيعات الرقمية والأغلفة الآمنة وعلامات الأمن. وتستخدم التوقيعات الرقمية في تقنيات المفاتيح العمومية في حين تستخدم الأغلفة الآمنة وعلامات الأمن مع تقنيات المفاتيح السرية.	X.813
forgery	التزوير	كيان يصطنع معلومات ويدَّعي أن هذه المعلومات متلقاة من كيان آخر أو أرسلت إلى كيان آخر.	M.3016.0
hash function	وظيفة الفرم	وظيفة (رياضية) تختصر مجموعة كبيرة (ربما كبيرة جداً) من القيم إلى مقدار صغير منها.	X.810
indirect attack	هجوم غير مباشر	هجوم على نظام لا يقوم على أساس أوجه القصور في آلية أمن معينة (مثال ذلك هجمات تتجاوز الآلية أو هجمات تعتمد على النظام الذي يستخدم الآلية بطريقة غير صحيحة).	X.814
integrity	السلامة	ضمان عدم تعديل البيانات بطريقة غير مرخص بها. (انظر أيضاً سلامة البيانات)	H.235
integrity service	خدمة السلامة	توفّر وسيلة لضمان صحة البيانات المتبادلة وحمايتها من التعديل أو الحذف أو الإنشاء (الإدراج) أو التكرار. ويميز بين الأنواع التالية من خدمات السلامة: سلامة بحسب المجال، سلامة التوصيل دون استرجاع؛ سلامة التوصيل مع الاسترجاع.	M.3016.2

المصطلح بالإنكليزية	المصطلح بالعربية	التعريف	المرجع
intentional threats	تهديدات مقصودة	تهديدات تتراوح بين الفحص العابر باستعمال أدوات رصد متيسرة والهجمات المتطورة باستخدام المعارف الخاصة بالنظام. ويمكن اعتبار التهديد المقصود، إذا تحقّق، بمثابة "هجوم".	X.800
IPCablecom	الاتصالات باستخدام بروتوكول الإنترنت	مشروع لقطاع تقييس الاتصالات في الاتحاد يتضمن معمارية وسلسلة توصيات تمكّن من تقديم الخدمات في الوقت الفعلي على شبكات التلفزيون الكبلي باستخدام مودمات كبلية.	J.160
Kerberos		بروتوكول استيقان شبكة مفاتيح سرية يستخدم طائفة من الخوارزميات للتجفير وقاعدة بيانات مركزية للاستيقان.	J.170
key	مفتاح	1. متوالية رموز تتحكم في عمليات التجفير وفك التجفير. 2. قيمة رياضية مدخلة في خوارزمية تجفير مختارة.	X.800 J.170
key exchange	بدالة مفاتيح	تبادل مفاتيح عمومية بين كيانات لكي تُستخدم لتجفير الاتصال بين الكيانات.	J.170
key management	إدارة مفاتيح	توليد المفاتيح وتخزينها وتوزيعها وإلغائها وأرشفتها وتطبيقها طبقاً لسياسة الأمن.	X.800
man-in-the-middle attack	هجوم طرف متوسط بين طرفين	هجوم يتمكن المهاجم فيه من أن يراد من قراءة الرسائل بين طرفين ودس رسائل بينهما وتعديلها دون علم أي منهما بأن الوصلة بينهما مخترقة.	X. 1151
masquerade	التنكر	إدعاء كيان بأنه كيان آخر.	X.800
mutual authentication	الاستيقان المتبادل	التأكد من هويتي العنصرين الرئيسيين.	X.811
non-repudiation	عدم التنصل	1. المقدرة على منع المرسل من أن ينكر فيما بعد أنه أرسل رسالة أو قام بإجراء ما. 2. الحماية من إنكار أحد الكيانات المشاركة في اتصال أنه شارك في الاتصال بأكمله أو في جزء منه. 3. عملية لا يستطيع بموجبها مرسل رسالة (طلب رؤية على أساس الدفع مثلاً) أن ينكر أنه أرسل رسالة.	J.170 H.235 J.93
notarization	التوثيق	تسجيل البيانات لدى طرف ثالث موثوق به يسمح لاحقاً بتأكيد دقة خصائص البيانات من حيث المحتوى والأصل والوقت والتسليم مثلاً.	X.800
passive threat	تهديد سلبي	تهديد بإفشاء غير مرخص به لمعلومات دون تغيير في حالة النظام.	X.800
password	كلمة المرور	1. معلومات الاستيقان السرية وتتألف عادة من سلسلة سمات. 2. سلسلة سمات يدخلها المستعمل: هي بمثابة مفتاح الأمن المخصص الذي يتقاسمه المستعمل المتنقل مع الميدان الأصل. وينبغي استخدام كلمة سر المستعمل هذه والسر المشتق الذي يتقاسمه المستعمل لغرض استيقان المستعمل.	X.800 H.530
physical security	أمن مادي	تدابير مستخدمة لتوفير حماية مادية لموارد من تهديدات متعمدة أو عارضة.	X.800
principal	العنصر، الطرف، الجهة	كيان يمكن استيقان هويته.	X.811

المصطلح بالإنكليزية	المصطلح بالعربية	التعريف	المرجع
privacy	الخصوصية	1. 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. 2. أسلوب اتصالات حيث لا يمكن تفسير الاتصال إلا من جانب الأطراف المخولة ذلك صراحة. ويتحقق هذا عموماً من خلال التجفير وتقاسم مفتاح (مفاتيح) التجفير.	X.800 H.235
private key;	مفتاح خاص؛	1. (في نظام تجفير مفتاح عمومي) هو ذلك المفتاح من زوج المفاتيح لدى مستعمل ما معروف لديه فقط. 2. مفتاح يستخدم مع خوارزمية تجفير لا تناظرية وحيازته مقيدة (تقتصر عادة على كيان واحد فقط). 3. المفتاح المستخدم في تجفير المفتاح العمومي الذي يخص كياناً منفرداً وينبغي أن يظل سرّاً.	X.509 X.810 J.170
privilege	امتياز	نعت أو خاصية منسوبة إلى كيان من قبل سلطة.	X.509
Privilege Management Infrastructure (PMI)	بنية تحتية لإدارة الامتيازات	البنية التحتية القادرة على دعم إدارة الامتيازات لدعم خدمة ترخيص شاملة ذات علاقة مع بنية تحتية لمفاتيح عمومية.	X.509
public key	مفتاح عمومي	1. (في نظام تجفير مفتاح عمومي) هو ذلك المفتاح من زوج المفاتيح لدى مستعمل ما معروف عموماً. 2. مفتاح يستخدم مع خوارزمية تجفير لا تناظرية ويمكن إتاحته عموماً 3. المفتاح المستخدم في تجفير المفتاح العمومي الذي يخص كياناً فردياً ويوزع عموماً. وتستخدم كيانات أخرى هذا المفتاح لتجفير بيانات ترسل إلى صاحب المفتاح.	X.509 X.810 J.170
public key certificate	شهادة مفتاح عمومي	1. المفتاح العمومي للمستعمل، مع بعض المعلومات الأخرى، جُعل منيعاً للتزوير بواسطة التجفير مع المفتاح الخاص لدى سلطة إصدار الشهادات التي أصدرته. 2. قيم تمثل مفتاحاً عمومياً لدى صاحبه (ومعلومات اختيارية أخرى) تحققت منه ووقعته سلطة موثوق بها في نسق لا يمكن تزويره. 3. ارتباط بين مفتاح عمومي لكيان ما ونعت أو أكثر يتعلق بهويته، ويعرف أيضاً بالشهادة الرقمية.	X.509 H.235 J.170
Public Key Cryptography	تجفير مفتاح عمومي	تقنية تجفير قائمة على خوارزمية ذات مفتاحين، خاص وعمومي، حيث تجفّر الرسالة بالمفتاح العمومي ولكن لا يمكن فك تجفيرها إلا بالمفتاح الخاص. ويُعرف أيضاً باسم نظام المفتاح الخاص–العمومي. ملاحظة – معرفة المفتاح العمومي لا تؤدي إلى معرفة المفتاح الخاص. مثال: يستنبط الطرف A زوجاً من المفاتيح ويرسل المفتاح العمومي علناً إلى جميع من يرغبون في الاتصال بالطرف A، لكنه يحتفظ بالمفتاح الخاص سرّاً. وبينما يمكن لأي شخص يحوز المفتاح العمومي أن يُجفّر رسالة للطرف A فإن الطرف A فقط هو الذي يمكنه فك تجفير الرسائل بالمفتاح الخاص.	J.93
Public Key Infrastructure (PKI)	البنية التحتية للمفاتيح العمومية	البنية التحتية القادرة على دعم إدارة مفاتيح عمومية قادرة على دعم خدمات الاستيقان والتجفير وسلامة البيانات وعدم التنصل.	X.509

المصطلح بالإنكليزية	المصطلح بالعربية	التعريف	المرجع
relying party	الطرف المعتمِد	مستعمل أو وكيل يعتمد على البيانات الواردة في شهادة عند اتخاذ قراراته.	X.509
replay	التكرار	تكرار رسالة أو جزء من رسالة لإنتاج أثر غير مرخص به. على سبيل المثال يمكن تكرار رسالة صحيحة تتضمن معلومات الاستيقان من قبل كيان آخر بغية استيقان ذاته (باعتباره غير ما هو حقاً).	X.800
repudiation	الإنكار	1. إنكار أحد الكيانات المشاركة في اتصال ما أنها شاركت في الاتصال بأكمله أو في جزء منه. 2. كيان مشارك في تبادل اتصال ما ثم ينكر ذلك فيما بعد. 3. (في حالة نظام مناولة الرسائل) عندما ينكر مستعمل خدمة نقل الرسائل أو خدمة نقل الرسائل بالذات لاحقاً تقديم أو تلقي أو إرسال رسالة ويشمل ذلك: إنكار المصدر، إنكار التقديم، إنكار التسليم.	X.800 M.3016.0 X.402
revocation list certificate	شهادة قائمة الإبطال	شهادة أمن بقائمة شهادات أمن قد أبطلت.	X.810
secret key	مفتاح سري	مفتاح يستخدم في خوارزمية تجفير لا تناظرية. وامتلاك مفتاح سري مقصور (على كيانين عادة).	X.810
security	الأمن	يستخدم مصطلح "الأمن" بمعنى التقليل إلى أدنى حد من مواطن ضعف الأصول والموارد. والأصل هو أي شيء له قيمة. وموطن الضعف هو أي نقطة يمكن أن تُستغل لانتهاك نظام ما أو المعلومات التي يتضمنها. والتهديد انتهاك محتمل للأمن.	X.800
security alarm	إنذار الأمن	رسالة تتولد عندما يكشف عن حدث متصل بالأمن معرّف في سياسة الأمن على أنه حالة إنذار. والقصد من إنذار الأمن أن يحظى باهتمام كيانات معينة في الوقت المناسب.	X.816
security audit	تدقيق الأمن	استعراض وفحص مستقلين لسجلات وأنشطة نظام ما من أجل اختبار كفاءة ضوابط النظام لضمان الامتثال للسياسة القائمة والإجراءات التشغيلية ولكشف انتهاكات الأمن والتوصية بأي تغييرات يشار بها في مجالات التحكم والسياسة والإجراءات.	X.800
security audit trail	سجل تدقيق الأمن	بيانات مجمعة قد تُستخدم لتيسير تدقيق الأمن.	X.800
security certificate	شهادة الأمن	مجموعة بيانات متعلقة بالأمن تصدرها سلطة أمنية أو طرف ثالث موثوق به مع معلومات أمن تستخدم لتوفير سلامة البيانات وخدمات الاستيقان من أصل البيانات. ملاحظة – تعتبر جميع الشهادات شهادات أمن. واعتمد مصطلح شهادة الأمن في السلسلة ITU-T X.800 لتجنب تضارب المصطلحات مع التوصية ITU-T X.509.	X.810
security domain	ميدان الأمن	1. مجموعة من المستعملين والأنظمة تخضع لسياسة أمن مشتركة. 2. مجموعة الموارد التي تخضع لسياسة أمنية واحدة.	X.841 X.411
security information (SI)	معلومات الأمن	المعلومات اللازمة لتنفيذ خدمات الأمن.	X.810

المصطلح بالإنكليزية	المصطلح بالعربية	التعريف	المرجع
security management	إدارة الأمن	تتألف إدارة الأمن من جميع الأنشطة اللازمة لإنشاء جوانب أمن نظام ما والمحافظة عليها وإنمائها. ومن المواضيع التي تشملها: إدارة خدمات الأمن؛ إنشاء آليات الأمن؛ إدارة المفاتيح (جزء الإدارة)؛ تحديد الهويات، والمفاتيح، ومعلومات التحكم في النفاذ وغيرها؛ إدارة سجل تدقيق الأمن وإنذارات الأمن.	M.3016.0
security model	نموذج الأمن	إطارٌ لوصف خدمات الأمن التي تصد التهديدات المحتملة في خدمة نقل الرسائل وكذلك عناصر الأمن التي تدعم تلك الخدمات.	X.402
security policy	سياسة الأمن	1. مجموعة القواعد التي تضعها سلطة الأمن والتي تحكم استخدام وتوفير خدمات وتسهيلات الأمن. 2. مجموعة معايير لتوفير خدمات الأمن. ملاحظة – انظر سياسة الأمن القائمة على الهوية والقائمة على القواعد. تتناول سياسة الأمن الكاملة بالضرورة شواغل كثيرة تقع خارج نطاق التوصيل البيني للأنظمة المفتوحة.	X.509 X.800
security service	خدمة الأمن	خدمة توفرها طبقة في أنظمة الاتصالات المفتوحة تضمن الأمن الكافي للأنظمة أو لنقل البيانات.	X.800
security threat	تهديد أمني	خرق أمني محتمل.	X. 800
security token	علامة الأمن	مجموعة بيانات تحميها خدمة أمن أو أكثر، مع معلومات أمن تستخدم في توفير خدمات الأمن، تُنقل بين كيانات الاتصالات.	X.810
sensitivity	الحساسية	خاصية مورد تدل على قيمته أو أهميته.	X.509
shared secret	سر متقاسم	مفتاح الأمن لخوارزميات تجفير؛ قد يكون مشتقاً من كلمة المرور.	H.530
signature	التوقيع	انظر التوقيع الرقمي.	X.800
simple authentication	الاستيقان البسيط	الاستيقان بواسطة ترتيبات كلمة سر بسيطة.	X.509
Source of Authority (SOA)	مصدر السلطة	سلطة نعوت يثق بها متحقق الامتياز لمورد معين باعتبارها السلطة النهائية لتخصيص مجموعة من الامتيازات.	X.509
spam	الرسائل الاقتحامية	بريد إلكتروني طفيلي وغير مرغوب.	H.235
spoofing	انتحال	انتحال صفة مشروع لمورد أو مستعمل	X.509
strong authentication	الاستيقان القوي	الاستيقان بواسطة شهادات مشتقة بالتجفير.	X.811
Sybil attack	هجوم سيبيل	هجوم يشوَّه جراءه نظام السمعة لشبكة الند إلى الند باستحداث عدد كبير من الكيانات ذات الأسماء المستعارة واستعمالها لاكتساب نفوذ هائل	
threat	التهديد	احتمال انتهاك الأمن.	X.800
Token	علامة	انظر علامة أمنية	
Trojan horse	"حصان طروادة"	عندما يدخل "حصان طروادة" إلى النظام يكون له وظيفة غير مرخص بها بالإضافة إلى وظيفته المرخص بها. والترحيل الذي ينسخ أيضاً رسائل إلى قناة غير مرخص لها يقوم بدور "حصان طروادة".	X.800
trust	الثقة	يقال إن الكيان X يثق في الكيان Y للقيام بمجموعة أنشطة فقط في حالة ما إذا اطمأن الكيان X إلى أن الكيان Y سوف يتصرف بأسلوب معين فيما يتعلق بالأنشطة.	X.810
trusted functionality	عنصر وظيفي موثوق به	عنصر وظيفي يبدو صحيحاً فيما يتعلق ببعض المعايير، كما وردت في سياسة الأمن مثلاً.	X.800

المصطلح بالإنكليزية	المصطلح بالعربية	التعريف	المرجع
trusted third party (TTP)	طرف ثالث موثوق به	سلطة أمن أو وكيلها الموثوق به (من كيانات أخرى) فيما يتعلق ببعض الأنشطة المتعلقة بالأمن (في سياق سياسة الأمن).	X.810
ubiquitous sensor network (USN)	شبكة الاستشعار في كل مكان	شبكة تستعمل أجهزة استشعار زهيدة الكلفة قليلة الاستهلاك القدرة لتنمية وعي بسياق ما من أجل تقديم خدمات المعلومات والمعرفة لأي شخص في أي مكان وفي أي وقت. ويمكن لشبكة الاستشعار في كل مكان أن تغطي منطقة جغرافية واسعة ويمكن أن تدعم مجموعة متنوعة من التطبيقات.	
unauthorized access	النفاذ غير المرخص به	كيان يحاول النفاذ إلى بيانات منتهكاً سياسة الأمن النافذة.	M.3016.0
user authentication	استيقان المستعمل	إقامة الدليل على هوية المستعمل أو عملية التطبيق.	M.3016.0
verifier	المتحقق	الكيان الذي يتطلب هوية مستيقنة أو يمثّل هذا الكيان. ويشمل المتحقق الوظائف اللازمة للشروع في عمليات تبادل الاستيقان.	X.811
vulnerability	موطن الضعف	أي نقطة يمكن استغلالها لانتهاك نظام ما أو المعلومات التي يحتوي عليها.	X.800
X.509 certificate	شهادة X.509	مواصفة شهادة مفتاح عمومي أُعدت كجزء من دليل معايير التوصية ITU-T X.500.	J.170

الملحق باء – العبارات المقتضبة والمختصرات المستعملة في هذا الدليل

الملحـــق باء

العبارات المقتضبة والمختصرات المستعملة في هذا الدليل

المختصر	المعنى
ACI	معلومات التحكم في النفاذ
AES	خوارزمية معيارية للتجفير المتطور
ASN.1	ترميز تركيب مجرد رقم واحد
ASP	مزوّد خدمة التطبيق
ATIS	التحالف لإيجاد حلول في صناعة الاتصالات
A/V	السمعي المرئي
BioAPI	السطح البيني لبرمجة تطبيقات الاستدلال الأحيائي
BPON	شبكة بصرية منفعلة ذات نطاق عريض
B2C	من مصلحة الأعمال إلى الزبون
CA	سلطة إصدار شهادات. منظمة موثوق بها تقبل طلبات لإصدار الشهادات من كيانات وتقوم بالاستيقان من الطلبات وإصدار الشهادات وتحتفظ بحالة المعلومات عن الشهادات.
CDMA	النفاذ المتعدد بتقسيم شفري
CMIP	بروتوكول معلومات إدارة مشتركة
CORBA	معمارية وسيط لطلب غرض مشترك
CP	سياسة الشهادة
CPS	بيان ممارسة إصدار الشهادات
CRL	قائمة إبطال الشهادات
DNS	خدمة مخدّم/نظام اسم الميدان
DSL	عروة مشترك رقمية
EAP	بروتوكول الاستيقان القابل للتوسيع
ENISA	الوكالة الأوروبية لأمن معلومات الشبكة
ETSI	المعهد الأوروبي لمعايير الاتصالات
FMC	التقارب بين الاتصالات الثابتة والمتنقلة
FW	الجدار الواقي
GK	حارس بوابة
GPRS	النظام العام للاتصالات الراديوية بأسلوب الرزم
GSM	النظام العالمي للاتصالات المتنقلة
GW	بوابة
HFX	تجفير فاكس هوثورن
HKM	خوارزمية إدارة مفاتيح هوثورن

المختصر	المعنى
HTTP	بروتوكول نقل النصوص التشعبية
ICT	تكنولوجيا المعلومات والاتصالات
ID	معرّف
IdM	إدارة الهوية
IEC	اللجنة الكهرتقنية الدولية
IEEE	معهد المهندسين الكهربائيين والالكترونيين
IETF	فريق مهام هندسة الإنترنت
IKE	بدالة مفاتيح الإنترنت هي آلية إدارة مفاتيح تستخدم للتفاوض واشتقاق المفاتيح المرتبطة بالأمن في أمن بروتوكول الإنترنت
IM	الرسائل الفورية
IMS	النظام الفرعي متعدد الوسائط بواسطة بروتوكول الإنترنت
IMT-2000	الاتصالات المتنقلة الدولية 2000
IP	بروتوكول الإنترنت
IPSec	أمن بروتوكول الإنترنت
IPTV	التلفزيون القائم على بروتوكول الإنترنت
IPX	تبادل رزم الإنترنت
ISMS	نظام إدارة معلومات الأمن
ISO	منظمة المعايير الدولية
ITU-T	قطاع تقييس الاتصالات في الاتحاد الدولي للاتصالات
LAN	شبكة منطقة محلية
LDAP	بروتوكول نفاذ سريع إلى الدليل
MD5	ملخص الرسالة رقم 5 (خوارزمية فرم آمنة)
MIS	نظام معلومات الإدارة
MTA	وكيل نقل الرسائل (في المراسلات) مكيف مطراف الوسائط (في تكنولوجيا الكبل)
MWSSG	بوابة الأمن لخدمات الويب المتنقلة
NAT	ترجمة عناوين الشبكة
NGN	شبكة الجيل التالي
OASIS	منظمة النهوض بالمعايير الإعلامية المهيكلة
OMG	فريق إدارة الأغراض
OSI	توصيل بيني للأنظمة المفتوحة
P2P	من الند إلى الند
PC	حاسوب شخصي
PDA	مساعد بيانات شخصي
PIN	رقم تعرّف الهوية الشخصية

المختصر	المعنى
PII	معلومات يمكن تعرّف هوية أصحابها شخصياً
PKI	بنية تحتية للمفاتيح العمومية
PKINIT	استيقان أولي من تجفير المفاتيح العمومية
PMI	البنية التحتية لإدارة الامتيازات
PSS	خدمة حماية معلومات يمكن تعرّف هوية أصحابها شخصياً
PSTN	الشبكة الهاتفية العمومية التبديلية
QoS	نوعية الخدمة
RBAC	التحكم في النفاذ على أساس الأدوار
RFID	التعرف بواسطة الترددات الراديوية
RSA	ريفست وشامير وأدلمان (خوارزمية المفاتيح العمومية)
RTP	بروتوكول الوقت الفعلي
SAML	لغة ترميز تأكيد الأمن
SG	لجنة دراسات
SHA1	خوارزمية الفرم الآمن 1
SIP	بروتوكول استهلال الدورة. بروتوكول (تشوير) تحكم في طبقة التطبيق من أجل استهلال وتعديل وإنهاء دورة مع مشارك أو أكثر.
SMS	خدمة الرسائل القصيرة
SMTP	بروتوكول نقل البريد البسيط
SNMP	بروتوكول بسيط لإدارة الشبكة
SoA	مصدر السلطة
SOA	معمارية ذات توجه خدمي
SPAK	بروتوكول الاستيقان الآمن القائم على كلمة مرور مع تبادل المفاتيح
SSL	طبقة مقبس آمن
SSO	الدخول الواحد
TCP/IP	بروتوكول التحكم في الإرسال بتبديل الرزم/بروتوكول الإنترنت
TLS	أمن مستوى النقل
TMN	شبكة إدارة الاتصالات
UE	معدات المستعمل
UICC	بطاقة دارة متكاملة عامة
USN	شبكة الاستشعار في كل مكان
VoIP	نقل الصوت باستعمال بروتوكول الإنترنت
VPN	شبكة افتراضية خاصة
WAN	شبكة المنطقة الواسعة
Wi-Fi	الأمانة اللاسلكية (علامة تجارية لتحالف Wi-Fi للمنتجات المرخصة بموجب معايير IEEE 802.11)
WTSA	الجمعية العالمية لتقييس الاتصالات

المختصر	المعنى
XACML	لغة ترميز التحكم في النفاذ القابلة للتوسيع
XML	لغة الترميز القابلة للتوسيع
3G	الجيل الثالث
3GPP	مشروع شراكة الجيل الثالث
3GPP2	مشروع شراكة الجيل الثالث 2

الملحق جيم – موجز عن لجان الدراسات
ذات الصلة بالأمن
في قطاع تقييس الاتصالات

الملحـــق جيم

موجز عن لجان الدراسات ذات الصلة بالأمن في قطاع تقييس الاتصالات

يتخلل عمل غالبية لجان الدراسات بعض الجوانب على الأقل من أمن الاتصالات و/أو تكنولوجيا المعلومات والاتصالات. وتتولى كل لجنة دراسات مسؤولية التصدي لقضايا الأمن في مجال اختصاصها، غير أن لجنة الدراسات 17 التي تركز على الأمن في المقام الأول عُينت بصفة لجنة الدراسات الرئيسية في مجال الأمن. ويلخص الجدول 8 أدوار لجان الدراسات التي تتحمل مسؤوليات ذات صلة بالأمن، ويدرج مسؤوليات لجان الدراسة الرئيسية لكل منها فيما يخصها.

الجدول 8 – لجان الدراسات التي تتحمل مسؤوليات ذات صلة بالأمن

لجنة الدراسات	الاسم	المسؤوليات/الدور الأمني
SG 2	الجوانب التشغيلية لتوفير الخدمات وإدارة الاتصالات	لجنة الدراسات الرئيسية المعنية بتعريف الخدمات والترقيم والتسيير لجنة الدراسات الرئيسية المعنية باتصالات الإغاثة في حالات الطوارئ/الإنذار المبكر لجنة الدراسات الرئيسية المعنية بإدارة الاتصالات
SG 5	البيئة وتغير المناخ	لجنة الدراسات الرئيسية المعنية بالتوافق الكهرمغنطيسي والآثار الكهرمغنطيسية لجنة الدراسات الرئيسية المعنية بتكنولوجيات المعلومات والاتصالات وتغير المناخ
SG 9	الإرسال التلفزيوني والصوتي والشبكات الكبلية المتكاملة عريضة النطاق	لجنة الدراسات الرئيسية المعنية بشبكات الكبلات المتكاملة عريضة النطاق وشبكات التلفزيون
SG 11	متطلبات وبروتوكولات التشوير ومواصفات الاختبار	لجنة الدراسات الرئيسية المعنية بالتشوير والبروتوكولات لجنة الدراسات الرئيسية المعنية بالشبكات الذكية لجنة الدراسات الرئيسية المعنية بمواصفات الاختبار
SG 12	الأداء ونوعية الخدمة ونوعية الخبرة	لجنة الدراسات الرئيسية المعنية بنوعية الخدمة ونوعية الخبرة
SG 13	شبكات المستقبل بما في ذلك شبكات الخدمة المتنقلة وشبكات الجيل التالي	لجنة الدراسات الرئيسية المعنية بشبكات المستقبل وشبكات الجيل التالي لجنة الدراسات الرئيسية المعنية بإدارة التنقلية وتقارب الاتصالات الثابتة–المتنقلة
SG 15	البنى التحتية لشبكات النقل البصرية وشبكات النفاذ	لجنة الدراسات الرئيسية المعنية بالنقل في شبكة النفاذ لجنة الدراسات الرئيسية المعنية بالتكنولوجيا البصرية لجنة الدراسات الرئيسية المعنية بشبكات النقل البصرية
SG 16	التشفير متعدد الوسائط وأنظمته وتطبيقاته	لجنة الدراسات الرئيسية المعنية بتشفير الوسائط المتعددة وأنظمتها وتطبيقاتها لجنة الدراسات الرئيسية المعنية بالتطبيقات في كل مكان ("كل الأشياء إلكترونياً" مثل الصحة الإلكترونية) لجنة الدراسات الرئيسية المعنية بالاتصالات/إمكانية النفاذ إلى تكنولوجيا المعلومات والاتصالات للأشخاص المعوقين
SG 17	الأمن	لجنة الدراسات الرئيسية المعنية بأمن الاتصالات لجنة الدراسات الرئيسية المعنية بإدارة الهوية لجنة الدراسات الرئيسية المعنية باللغات وتقنيات الوصف

الملحق دال – توصيات الأمن المشار إليها كمراجع في هذا الدليل

الملحـــق دال

توصيات الأمن المشار إليها كمراجع في هذا الدليل

يضم هذا الملحق قائمة كاملة بجميع توصيات قطاع تقييس الاتصالات المشار إليها كمراجع في هذا الدليل مع وصلاتها الإلكترونية بحيث يتسنى للقراء الذين يستخدمون نسخة إلكترونية من النص أن يُوصلوا مباشرةً لتحميل التوصيات. وكما ورد في متن النص، فقد وضع قطاع تقييس الاتصالات العديد من المعايير المتعلقة بالأمن بالتعاون مع المنظمات الأخرى لوضع المعايير. فترد في هذا الجدول أيضاً التوصيات المتعلقة بالأمن المنشورة حالياً بنصوص مشتركة/توائم مع نصوص تلك المنظمات. ويمكن الاطلاع على المجموعة الكاملة لتوصيات قطاع تقييس الاتصالات على الخط في العنوان الإلكتروني: www.itu.int/rec/T-REC/en. أما توصيات قطاع تقييس الاتصالات المتعلقة بالأمن فهي متاحة عبر الجزء 2 (قاعدة بيانات) من خارطة طريق معايير الأمن (www.itu.int/ITU-T/studygroups/com17/ict/index.html).

التوصية	العنوان	النص المكافئ
E.408	متطلبات أمن شبكات الاتصالات	
E.409	تنظيم الحوادث والتعامل مع الحوادث الأمنية: مبادئ توجيهية لمنظمات الاتصالات	
G.827	أداء التيسّر ومعلماته وأهدافه على المسيرات الرقمية الدولية ذات معدل البتات الثابت من طرف إلى طرف	
G.1000	جودة خدمة الاتصالات: إطار وتعاريف	
G.1030	تقدير الأداء من طرف إلى طرف في شبكات بروتوكول الإنترنت لتطبيقات البيانات	
G.1050	نموذج شبكة لتقييم أداء الإرسال المتعدد الوسائط باستعمال بروتوكول الإنترنت	
G.1081	نقاط مراقبة نوعية أداء تلفزيون بروتوكول الإنترنت	
H.235.0	إطار الأمن لأنظمة تعدد الوسائط للسلسلة H H.323 وأخرى قائمة على أساس H.245	
H.235.1	H.323 الأمن: مواصفة الأمن الأساسي	
H.235.2	H.323 الأمن: مواصفة الأمن بالتواقيع	
H.235.3	H.323 الأمن: مواصفة الأمن الهجينة	
H.235.4	H.323 الأمن: الأمن المباشر والانتقائي للنداء المسيّر	
H.235.5	H.323 الأمن: إطار للاستيقان المأمون خلال تبادل رسائل التسجيل والقبول والوضع (RAS) بواسطة أسرار مشتركة ضعيفة	
H.235.6	H.323 الأمن: مواصفة التجفير الصوتي بإدارة مفاتيح أصلية H.245/H.235	
H.Imp235	دليل المنفذين إلى توصية قطاع تقييس الاتصالات H.235 V3: "الأمن والتجفير لمطاريف الوسائط المتعددة في السلسلة H (القائمة على توصيات قطاع تقييس الاتصالات H.323 وغيرها من توصيات قطاع تقييس الاتصالات H.245)"	
H.323	أنظمة الاتصالات لوسائط متعددة قائمة على الرزم	
H.350	معمارية خدمات الدليل للمؤتمرات متعددة الوسائط	
H.460.17	*استعمال توصيل تشوير النداء H.225.0 كوسيلة نقل لرسائل التسجيل والقبول والوضع الراهن RAS في إطار H.323*	

التوصية	العنوان	النص المكافئ
H.460.18	*عبور تشوير H.323 من خلال أجهزة ترجمة عناوين الشبكة وجدران الوقاية*	
H.460.19	*عبور وسائط H.323 من خلال ترجمة عناوين الشبكة وجدران الوقاية*	
H.510	تنقلية الأنظمة والخدمات متعددة الوسائط وفق توصية قطاع تقييس الاتصالات H.323	
H.530	إجراءات الأمن التناظرية لتنقلية H.323 في توصية قطاع تقييس الاتصالات H.510	
J.160	الإطار المعماري لتقديم خدمات في الوقت الحرج على شبكات تلفزيون كبلية تستعمل مودمات كبلية	
J.170	مواصفات أمن الاتصالات الكبلية باستخدام بروتوكول الإنترنت IPCablecom	
J.360	إطار لمعمارية الاتصالات الكبلية القائمة على بروتوكول الإنترنت 2 – الوثيقة الرئيسية	
M.3010	مبادئ شبكة إدارة الاتصالات	
M.3016.0	*أمن مستوي الإدارة: نظرة عامة*	
M.3016.1	*أمن مستوي الإدارة: متطلبات الأمن*	
M.3016.2	*أمن مستوي الإدارة: خدمات الأمن*	
M.3016.3	*أمن مستوي الإدارة: آليات الأمن*	
M.3016.4	*أمن مستوي الإدارة: نموذج المواصفة*	
M.3208.2	إدارة التوصيل لتوصيلات وصلة الخدمة الموفرة مسبقاً لإنشاء خدمة دارة مؤجرة	
M.3210.1	خدمات إدارة شبكة إدارة الاتصالات (TMN) لإدارة أمن الاتصالات المتنقلة الدولية 2000	
Q.816	خدمات إدارة شبكة إدارة الاتصالات (TMN) القائمة على معمارية وسيط لطلب غرض مشترك (CORBA)	
Q.834.3	وصف بلغة النمذجة الموحدة (UML) لمتطلبات السطح البيني لإدارة الشبكات البصرية المنفعلة عريضة النطاق	
Q.834.4	مواصفة السطح البيني لمعمارية وسيط لطلب غرض مشترك (CORBA) من أجل الشبكات البصرية المنفعلة عريضة النطاق القائمة على متطلبات السطح البيني للغة النمذجة الموحدة (UML)	
Q.1701	إطار شبكات الاتصالات المتنقلة الدولية–2000	
Q.1702	رؤية طويلة الأجل لجوانب الشبكة في أنظمة الاتصالات المتنقلة الدولية ما بعد عام 2000	
Q.1703	إطار قدرات الخدمة والشبكة لجوانب الشبكة في أنظمة الاتصالات المتنقلة الدولية ما بعد عام 2000	
Q.1741.1	مراجع الاتصالات المتنقلة الدولية–2000 لإصدار 1999 من النظام العمومي للاتصالات المتنقلة المتطورة للشبكة الأساسية للنظام العالمي للاتصالات المتنقلة مع شبكة نفاذ إلى شبكة نفاذ عالمية راديوية للأرض	3GPP
Q.1742.1	مراجع الاتصالات المتنقلة الدولية 2000 للمعهد الأمريكي الوطني للمعايير 41 للشبكة الأساسية المتطورة لشبكة نفاذ متعدد لتقسيم شفري 2000	3GPP2
T.4	تقييس مطاريف فاكس من الزمرة 3 لإرسال الوثائق	
T.36	مقدرات الأمن لاستخدام مطاريف الفاكس من الزمرة 3	
T.37	إجراءات نقل بيانات الفاكس عبر التخزين والإرسال على الإنترنت	
T.38	إجراءات اتصالات فاكس من الزمرة 3 في الوقت الفعلي عبر شبكات بروتوكول الإنترنت	

التوصية	العنوان	النص المكافئ
T.563	الخصائص المطرافية لأجهزة الفاكس من الزمرة 4	
X.500	الدليل: نظرة عامة على المفاهيم والنماذج والخدمات	ISO/IEC 9594-1
X.501	الدليل: نماذج	ISO/IEC 9594-2
X.509	الدليل: أطر شهادات المفاتيح العمومية والنعوت	ISO/IEC 9594-8
X.511	الدليل: تعريف الخدمة المجردة	ISO/IEC 9594-3
X.518	الدليل: إجراءات التشغيل الموزع	ISO/IEC 9594-4
X.519	الدليل: مواصفات البروتوكول	ISO/IEC 9594-5
X.520	الدليل: أنماط النعوت المنتقاة	ISO/IEC 9594-6
X.521	الدليل: أصناف الغرض المنتقاة	ISO/IEC 9594-7
X.525	الدليل: النسخ	ISO/IEC 9594-9
X.530	الدليل: استعمال إدارة الأنظمة في إدارة الدليل	ISO/IEC 9594-10
X.711	بروتوكول معلومات الإدارة المشتركة: المواصفة	ISO/IEC 9596-1
X.736	إدارة الأنظمة: وظيفة الإبلاغ عن إنذارات الأمن	ISO/IEC 10164-7
X.740	إدارة الأنظمة: وظيفة تعقب التدقيق الأمني	ISO/IEC 10164-8
X.741	إدارة الأنظمة: أغراض ونعوت التحكم في النفاذ	ISO/IEC 10164-9
X.780	المبادئ التوجيهية لشبكة إدارة الاتصالات في تعريف الأغراض التي تديرها معمارية CORBA	
X.780.1	المبادئ التوجيهية لشبكة إدارة الاتصالات في تعريف الأغراض ذات التفاصيل العامة التي تديرها معمارية CORBA	
X.780.2	المبادئ التوجيهية لشبكة إدارة الاتصالات في تعريف الأغراض ذات التوجه الخدمي التي تديرها معمارية CORBA وفي تعريف أغراض الواجهة	
X.781	المتطلبات والمبادئ التوجيهية لقوالب بيانات مطابقة التنفيذ المرتبطة بالأنظمة القائمة على معمارية CORBA	
X.790	وظيفة إدارة الخلل بالنسبة لتطبيقات قطاع تقييس الاتصالات	
X.800	معمارية الأمن للتوصيل البيني للأنظمة المفتوحة لتطبيقات اللجنة الاستشارية الدولية للبرق والهاتف CCITT	ISO/IEC 7498-2
X.802	نموذج الأمن في الطبقات السفلى	ISO/IEC TR 13594
X.803	نموذج الأمن في الطبقات العليا	ISO/IEC 10745
X.805	معمارية أمن لأنظمة توفر الاتصالات من طرف إلى طرف	ISO/IEC 18028-2
X.810	أطر الأمن للأنظمة المفتوحة: نظرة عامة	ISO/IEC 10181-1
X.811	أطر الأمن للأنظمة المفتوحة: إطار الاستيقان	ISO/IEC 10181-2
X.812	أطر الأمن للأنظمة المفتوحة: إطار التحكم في النفاذ	ISO/IEC 10181-3
X.813	أطر الأمن للأنظمة المفتوحة: إطار عدم التنصل	ISO/IEC 10181-4
X.814	أطر الأمن للأنظمة المفتوحة: إطار السرية	ISO/IEC 10181-5
X.815	أطر الأمن للأنظمة المفتوحة: إطار سلامة البيانات	ISO/IEC 10181-6
X.816	أطر الأمن للأنظمة المفتوحة: إطار تدقيق الأمن والإنذارات	ISO/IEC 10181-7

التوصية	العنوان	النص المكافئ
X.830	أمن الطبقات العليا العمومية: نظرة عامة ونماذج وترميز	ISO/IEC 11586-1
X.831	أمن الطبقات العليا العمومية: تعريف خدمة عنصر خدمة تبادل الأمن	ISO/IEC 11586-2
X.832	أمن الطبقات العليا العمومية: مواصفة بروتوكول عنصر خدمة تبادل الأمن	ISO/IEC 11586-3
X.833	أمن الطبقات العليا العمومية: مواصفة حماية قواعد تركيب النقل	ISO/IEC 11586-4
X.834	أمن الطبقات العليا العمومية: شكل الإعلان عن تطابق تنفيذ بروتوكول عنصر خدمة تبادل الأمن	ISO/IEC 11586-5
X.835	أمن الطبقات العليا العمومية: شكل الإعلان عن تطابق تنفيذ بروتوكول حماية قواعد تركيب النقل	ISO/IEC 11586-6
X.841	تكنولوجيا المعلومات – تقنيات الأمن – أغراض معلومات أمن لمراقبة النفاذ	ISO/IEC 15816
X.842	تكنولوجيا المعلومات – تقنيات الأمن – مبادئ توجيهية لاستخدام وإدارة خدمات الطرف الثالث الموثوق به	ISO/IEC TR 14516
X.843	تكنولوجيا المعلومات – تقنيات الأمن – مواصفة خدمات الطرف الثالث الموثوق به لدعم تطبيق التواقيع الرقمية	ISO/IEC 15945
الإضافة 3 لسلسلة X: X.849-X.800	إضافة بشأن المبادئ التوجيهية لتنفيذ أمن النظام والشبكة	
X.1031	أدوار المستعملين النهائيين وشبكات الاتصالات ضمن معمارية الأمن	
X.1034	مبادئ توجيهية للاستيقان القائم على بروتوكول الاستيقان الموسع ولإدارة المفاتيح في شبكة اتصالات البيانات	
X.1035	*بروتوكول تبادل المفاتيح المستيقنة بكلمة مرور*	
X.1036	*الإطار العام لاستحداث سياسات أمن الشبكة وتخزينها وتوزيعها وإنفاذها*	
X.1051	تقنيات الأمن – المبادئ التوجيهية لإدارة أمن المعلومات في منظمات الاتصالات، استناداً إلى معيار ISO/IEC 27002	ISO/IEC 27011
X.1055	المبادئ التوجيهية لإدارة المخاطر ومواصفاتها في منظمات الاتصالات	
X.1056	المبادئ التوجيهية لإدارة حوادث الأمن في منظمات الاتصالات	
X.1081	إطار لتوصيف جوانب الأمن والسلامة للاستدلال الأحيائي عن بعد	
X.1082	الاستدلال الأحيائي عن بعد ذي الصلة بالفيزيولوجيا البشرية	ISO/IEC 80000-14
X.1083	الاستدلال الأحيائي – بروتوكول العمل البيني للسطوح البينية لبرمجة تطبيقات الاستدلال الأحيائي (BioAPI)	ISO/IEC 24708
X.1084	آلية نظام الاستدلال الأحيائي – الجزء 1: البروتوكول العام للاستيقان بالاستدلال الأحيائي وملامح نموذج النظام العامة لأنظمة الاتصالات في شبكة مفتوحة	
X.1086	إجراءات حماية الاستدلال الأحيائي عن بعد – الجزء 1: مبدأ توجيهي للتدابير التقنية والإدارية المضادة في أمن بيانات الاستدلال الأحيائي	
X.1088	إطار الاستدلال الأحيائي للمفاتيح الرقمية – إطار لتوليد المفاتيح الرقمية بالاستدلال الأحيائي وحمايتها	
X.1089	البنية التحتية للاستيقان بالاستدلال الأحيائي عن بعد	
X.1111	إطار تكنولوجيات الأمن للشبكة المنـــزلية	
X.1112	مواصفة شهادة جهاز للشبكة المنـــزلية	

التوصية	العنوان	النص المكافئ
X.1113	مبدأ توجيهي بشأن آليات الاستيقان من مستعمل في خدمات الشبكة المنـــزلية	
X.1114	إطار التخويل للشبكة المنـــزلية	
X.1121	إطار تكنولوجيات الأمن لاتصالات البيانات المتنقلة من طرف إلى طرف	
X.1122	المبدأ التوجيهي لتنفيذ الأنظمة المتنقلة الآمنة على أساس البنية التحتية للمفاتيح العمومية	
X.1123	خدمة الأمن التفاضلية لاتصالات البيانات المتنقلة الآمنة من طرف إلى طرف	
X.1124	معمارية الاستيقان للاتصالات المتنقلة من طرف إلى طرف	
X.1125	نظام ترابطي تفاعلي في اتصالات البيانات المتنقلة	
X.1141	لغة التشفير المتداولة في توكيد الأمن (SAML 2.0)	OASIS SAML 2.0
X.1142	لغة ترميز التحكم في النفاذ القابلة للتوسيع الأساسية (XACML 2.0)	OASIS XACML 2.0
X.1143	معمارية الأمن لأمن الرسالة في خدمات الويب المتنقلة	
X.1151	مبدأ توجيهي لبروتوكول الاستيقان الآمن القائم على كلمة مرور مع تبادل المفاتيح	
X.1152	التقنيات الآمنة لاتصالات البيانات من طرف إلى طرف باستعمال خدمات طرف ثالث موثوق	
X.1161	إطار لاتصالات آمنة من ند إلى ند	
X.1162	معمارية وعمليات الأمن لشبكة الند إلى الند	
X.1171	التهديدات ومتطلبات حماية المعلومات التي يمكن تعرّف هوية أصحابها شخصياً في التطبيقات التي تستعمل تعرّف الهوية على أساس الوسم	
X.1191	المتطلبات الوظيفية لجوانب أمن التلفزيون القائم على بروتوكول الإنترنت (IPTV) ومعماريته	
X.1205	لمحة عامة عن الأمن السيبراني	
X.1206	إطار محايد تجاه البائع للتبليغ الأوتوماتي بالمعلومات المتعلقة بالأمن ونشر التحديثات	
X.1207	مبادئ توجيهية لمقدمي خدمات الاتصالات للتصدي لمخاطر برمجيات التجسس والبرمجيات المحتملة غير المطلوبة	
X.1231	الاستراتيجيات التقنية في التصدي للرسائل الاقتحامية	
X.1240	التكنولوجيات التي تنطوي عليها مكافحة البريد الإلكتروني الاقتحامي	
X.1241	الإطار التقني للتصدي للرسائل الاقتحامية في البريد الإلكتروني	
X.1242	نظام ترشيح الرسائل الاقتحامية في خدمة الرسائل القصيرة (SMS) على أساس قواعد يحددها المستعمل	
X.1244	الجوانب العامة لمكافحة الرسائل الاقتحامية في تطبيقات الوسائط المتعددة القائمة على بروتوكول الإنترنت	
X.1250	مقدرات مرجعية للإدارة العالمية المعززة للهوية وإمكانية التشغيل البيني	
X.1251	إطار لتحكم المستعمل في الهوية الرقمية	
X.1303	بروتوكول التحذير المشترك (CAP 1.1)	OASIS CAP v1.1
X.Sup6	إضافة إلى سلسلة توصيات X.1240 بشأن التصدي للرسائل الاقتحامية وما يرتبط بها من تهديدات	
X.Sup7	إضافة إلى سلسلة توصيات X.1250: لمحة عامة عن إدارة الهوية في سياق الأمن السيبراني	
Y.2001	نظرة عامة على شبكات الجيل التالي	

التوصية	العنوان	النص المكافئ
Y.2701	متطلبات أمن شبكة الجيل التالي – الإصدار الأول	
Y.2720	إطار إدارة الهوية في شبكات الجيل التالي	

منشورات أخرى

تكنولوجيات المنشأة الخارجية للشبكات العمومية

تطبيق الحواسيب والمعالجات الصغرية في بناء كبلات الاتصالات وتركيبها وحمايتها

طبع في سويسرا
جنيف، 2010