الاتحـــــــــــاد الدولـــــــــــي للاتصـــــــــــالات

ITU-T

قطاع تقييس الاتصالات
في الاتحاد الدولي للاتصالات

X.1550
(2017/03)

السلسلة X: شبكات البيانات والاتصالات بين الأنظمة المفتوحة ومسائل الأمن

تبادل معلومات الأمن السيبراني – تبادل السياسات

نماذج للتحكم في النفاذ لشبكات تبادل معلومات الحوادث العارضة

التوصية ITU-T X.1550

الاتحاد الدولي للاتصالات

توصيات السلسلة X الصادرة عن قطاع تقييس الاتصالات

شبكات البيانات والاتصالات، بين الأنظمة المفتوحة ومسائل الأمن

الشبكات العمومية للبيانات	X.199–X.1
التوصيل البيني للأنظمة المفتوحة	X.299–X.200
التشغيل البيني للشبكات	X.399–X.300
أنظمة معالجة الرسائل	X.499–X.400
الدليل	X.599–X.500
التشغيل البيني لأنظمة التوصيل OSI ومظاهر النظام	X.699–X.600
إدارة التوصيل البيني للأنظمة المفتوحة (OSI)	X.799–X.700
الأمن	X.849–X.800
تطبيقات التوصيل البيني للأنظمة المفتوحة (OSI)	X.899–X.850
المعالجة الموزعة المفتوحة	X.999–X.900
أمن المعلومات والشبكات	
الجوانب العامة للأمن	X.1029–X.1000
أمن الشبكة	X.1049–X.1030
إدارة الأمن	X.1069–X.1050
الخصائص البيومترية	X.1099–X.1080
تطبيقات وخدمات آمنة	
أمن البث المتعدد	X.1109–X.1100
أمن الشبكة المحلية	X.1119–X.1110
أمن الخدمات المتنقلة	X.1139–X.1120
أمن الويب	X.1149–X.1140
بروتوكولات الأمن	X.1159–X.1150
الأمن بين جهتين نظيرتين	X.1169–X.1160
أمن معرفات الهوية عبر الشبكات	X.1179–X.1170
أمن التلفزيون القائم على بروتوكول الإنترنت	X.1199–X.1180
أمن الفضاء السيبراني	
الأمن السيبراني	X.1229–X.1200
مكافحة الرسائل الاقتحامية	X.1249–X.1230
إدارة الهوية	X.1279–X.1250
تطبيقات وخدمات آمنة	
اتصالات الطوارئ	X.1309-X.1300
أمن شبكات المحاسيس واسعة الانتشار	X.1339–X.1310
التوصيات المتعلقة بالبنية التحتية للمفاتيح العمومية	X.1349–X.1340
أمن إنترنت الأشياء	X.1369–X1360
أمن أنظمة النقل الذكية	X.1379–X.1370
تبادل معلومات الأمن السيبراني	
نظرة عامة عن الأمن السيبراني	X.1519–X.1500
تبادل مواطن الضعف/الحالة	X.1539–X.1520
تبادل الأحداث/الأحداث العارضة/المعلومات الحدسية	X.1549–X.1540
تبادل السياسات	**X.1559–X.1550**
طلب المعلومات الحدسية والمعلومات الأخرى	X.1569–X.1560
تعرف الهوية والاكتشاف	X.1579–X.1570
التبادل المضمون	X.1589–X.1580
أمن الحوسبة السحابية	
نظرة عامة على أمن الحوسبة السحابية	X.1601–X.1600
تصميم أمن الحوسبة السحابية	X.1639–X.1602
أفضل الممارسات ومبادئ توجيهية بشأن أمن الحوسبة السحابية	X.1659–X.1640
تنفيذ أمن الحوسبة السحابية	X.1679–X.1660
أمن أشكال أخرى للحوسبة السحابية	X.1699–X.1680

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

التوصية ITU-T X.1550

نماذج للتحكم في النفاذ لشبكات تبادل معلومات الحوادث العارضة

ملخص

تتناول التوصية ITU-T X.1550 النُهج القائمة لتنفيذ سياسات التحكّم في النفاذ لشبكات تبادل معلومات الحوادث العارضة. وتطرح هذه التوصية مجموعة متنوعة من نماذج التحكّم في النفاذ المحكمة ونماذج التبادل ومعايير من أجل تقييم أداء شبكة تبادل معلومات الحوادث العارضة. ويُنظر في الحلول القائمة على المعايير من أجل تيسير تنفيذ نماذج التحكّم المختلفة داخل النماذج المختلفة لتبادل معلومات الأمن السيبراني وفي ظل ظروف بيئات الثقة المتنوعة.

التسلسل التاريخي

الطبعة	التوصية	تاريخ الموافقة	لجنة الدراسات	معرف الهوية الفريد*
1.0	ITU-T X.1550	2017-03-30	17	11.1002/1000/13198

مصطلحات أساسية

التحكم في النفاذ، التخويل، فريق الاستجابة للطوارئ الحاسوبية، فريق الاستجابة للحوادث الأمنية الحاسوبية، تبادل معلومات الأمن السيبراني، إدارة الهوية والنفاذ، شبكة تبادل معلومات الحوادث العارضة؛ الاستجابة للحوادث.

* للنفاذ إلى توصية، ترجى كتابة العنوان http://handle.itu.int/ في حقل العنوان في متصفح الويب لديكم، متبوعاً بمعرف التوصية الفريد. ومثال ذلك، http://handle.itu.int/11.1002/1000/11830-en.

تمهيد

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

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

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

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

ملاحظة

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

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

حقوق الملكية الفكرية

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

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

جدول المحتويات

الصفحة

التوصية ITU-T X.1550

نماذج للتحكم في النفاذ لشبكات تبادل معلومات الحوادث العارضة

1 مجال التطبيق

تتناول هذه التوصية النُهج القائمة لتنفيذ سياسات التحكّم في النفاذ لشبكات تبادل معلومات الحوادث العارضة. وتطرح هذه التوصية مجموعة متنوعة من نماذج التحكّم في النفاذ المحكمة ونماذج التبادل ومعايير من أجل تقييم أداء شبكة تبادل معلومات الحوادث العارضة. ويُنظر في الحلول القائمة على المعايير من أجل تيسير تنفيذ نماذج التحكّم المختلفة داخل النماذج المختلفة لتبادل معلومات الأمن السيبراني وفي ظل ظروف بيئات الثقة المتنوعة.

2 المراجع

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

[ITU-T X.1500] التوصية ITU-T X.1500 (2011)، *نظرة عامة على تبادل معلومات الأمن السيبراني.*

[ITU-T X.1570] التوصية ITU-T X.1570 (2011)، *آليات الاكتشاف في إطار تبادل معلومات الأمن السيبراني.*

3 التعاريف

1.3 المصطلحات المعرَّفة في وثائق أخرى

تستخدم هذه التوصية المصطلحات التالية المعرَّفة في وثائق أخرى:

1.1.3 التحكم في النفاذ (access control) [b-ITU-T X.1252]: إجراء متبع لتحديد ما إذا كان ينبغي منح كيان ما نفاذاً إلى موارد أو مرافق أو خدمات أو معلومات استناداً إلى ما هو محدد مسبقاً من قواعد وحقوق معينة أو إلى سلطة يتمتع بها الطرف الطالب.

2.1.3 التخويل (authorization) [b-ITU-T M.3345]: يمثل الطريقة والشروط التي يمكن أن تستخدم بها الأطراف الفاعلة المعنية بإدارة الخدمة الذاتية وظائف الخدمة الذاتية، وما هي إجراءات الخدمة الذاتية المسموح لهم القيام بها.

3.1.3 تبادل معلومات الحوادث العارضة (incidents exchange) [ITU-T X.1570]: نقل معلومات الأمن السيبراني بين جهتي أمن سيبراني أو أكثر. وقد يكون النقل هذا أحادي الاتجاه أو ثنائي الاتجاه أو متعدد الاتجاهات، أي من عدة جهات إلى عدة جهات.

ملاحظة – يعتبر مصطلح "تبادل معلومات الحوادث العارضة" في هذه التوصية مساوياً لمصطلح "تبادل المعلومات".

4.1.3 ميدان الثقة (trust domain) [b-ITU-T M.3410]: مجموعة من المعلومات والموارد المصاحبة التي تتألف من مستعملين وشبكات ومستودعات بيانات وتطبيقات وتتداول البيانات في مستودعات البيانات هذه. ويمكن لميادين ثقة مختلفة التشارك في نفس المكونات المادية. ويمكن أيضاً لميدان ثقة واحد استغلال مستويات ثقة متنوعة، اعتماداً على ما يرغب المستعملون في معرفته وحساسية المعلومات والموارد المصاحبة.

2.3 مصطلحات معرّفة في هذه التوصية

تعرّف هذه التوصية المصطلحات التالية:

1.2.3 تضارب سياسات التحكم في النفاذ (access control policy conflict): يحدد الإجراءات الخاصة بقاعدتين تناقض إحداهما الأخرى. ولن يتسنى للكيان القائم بتنفيذ السياسات تحديد الإجراء الذي يتعيّن القيام به.

ملاحظة – يستند هذا التعريف إلى تعريف "تضارب السياسات" الوارد في التوصية [b-ITU-T X.1036].

2.2.3 حل حالات التضارب في السياسات دينامياً (incidents policy conflict resolution): استراتيجيات حل حالات التضارب المطبّقة وقت التشغيل.

3.2.3 شبكات تبادل معلومات الحوادث العارضة (incidents exchange networks): تعميم البنية التحتية التشغيلية لتبادل معلومات الأمن السيبراني (CYBEX) استناداً إلى إدارة مركزية أو اتحادية.

4.1.3 معلومات الحوادث العارضة (incidents information): مجموعة فرعية من معلومات الأمن السيبراني أو معلومات أو معارف مهيكلة بخصوص الأدلة الجنائية المتعلقة بحوادث أو أحداث.

ملاحظة – يستند هذا التعريف إلى الوصف الخاص "بتبادل (معلومات الأمن السيبراني)" الوارد في التوصية [b-ITU-T X.1570].

5.2.3 حل حالات التضارب في السياسات سكونياً (static policy conflict resolution): استراتيجيات حل حالات التضارب المطبقة في مرحلة التصميم.

4 المختصرات والأسماء المختصرة

تستعمل هذه التوصية المختصرات التالية:

ABAC التحكّم في النفاذ القائم على النعوت *(Attribute-Based Access Control)*

ACL قائمة التحكّم في النفاذ *(Access Control List)*

CERT فريق الاستجابة للطوارئ الحاسوبية *(Computer Emergency Response Team)*

CSIRT فريق الاستجابة للحوادث الأمنية الحاسوبية *(Computer Security Incident Response Team)*

CYBEX تبادل معلومات الأمن السيبراني *(Cybersecurity information Exchange)*

DAC التحكّم في النفاذ الاستنسابي *(Discretionary Access Control)*

IAM إدارة الهوية والنفاذ *(Identity and Access Management)*

IODEF نسق تبادل وصف الحوادث العارضة *(Incident Object Description Exchange Format)*

IT تكنولوجيا المعلومات *(Information Technology)*

MAC التحكّم في النفاذ الإلزامي *(Mandatory Access Control)*

PBAC التحكّم في النفاذ القائم على السياسات *(Policy-Based Access Control)*

PDP نقطة تقرير السياسات *(Policy Decision Point)*

PERMIS معايير البنية التحتية لإدارة الامتيازات والأدوار *(Privilege and Role Management Infrastructure Standards)*

RAdAC التحكّم في النفاذ المكيّف حسب المخاطر *(Risk-Adaptive Access Control)*

RBAC التحكّم في النفاذ القائم على الأدوار *(Role-Based Access Control)*

RID الدفاع بين الشبكات في الوقت الفعلي *(Real-time Inter-network Defense)*

RIDT نقل الدفاع بين الشبكات في الوقت الفعلي *(Real-time Inter-network Defense Transport)*

STIX شكل مهيكل للتعبير عن معلومات التهديدات *(Structured Threat Information Expression)*

TAXII التبادل المؤتمت الموثوق لمعلومات المؤشرات *(Trusted Automated Exchange of Indicator Information)*

TBAC التحكّم في النفاذ القائم على المهام *(Task-Based Access Control)*

TBAM إدارة التحكّم في النفاذ القائم على المهام *(Task-Based Access Management)*

XACML لغة وسم التحكّم في النفاذ القابلة للتوسيع *(extensible Access Control Markup Language)*

XML لغة الوسم القابلة للتوسيع *(extensible Markup Language)*

5 الاصطلاحات

في سياق هذه التوصية يُنظر إلى "التحكّم في النفاذ" على أنه آلية عامة تدعم إجراءات التخويل.

6 استعراض عام

قد يحتاج الأمر إلى التخفيف من حدة المخاطر لخفض التكلفة المالية للتخفيف من حدة الهجمات الحاسوبية وتوفير الضمان الأمني داخل أي منظمة/هيئة تعاونية أو خدمة/نظام. وتعمل شبكات تبادل معلومات الحوادث العارضة على منع المخاطر المرتبطة بالهجمات الحاسوبية أو الحد منها. وتطرح ممارسات تبادل معلومات الحوادث العارضة للأمن السيبراني مجموعة متنوعة من نماذج تبادل المعلومات التي تنفذ إما في بيئة مركزية أو اتحادية. ويستند تبادل معلومات الحوادث العارضة إلى مستوى من الثقة يرتبط بالمخاطر المصاحبة ويفرز الحاجة إلى ضمان عدم تبادل المعلومات السرية أو الحساسة بصورة غير مناسبة. وهذا الأمر يجعل من بعض نماذج التحكّم في النفاذ أكثر فعالية من الأخرى من منظور الأداء والتنفيذ وضمان الأمن.

وقد شجّع النمو الشامل والدمج المتبادل لأنظمة المعلومات العالمية على تطوير نماذج متقدمة للتحكّم في النفاذ تستند إليها عمليات التخويل. وتسهل لغات سياسات التحكم في النفاذ القائمة تطبيق السياسات الأمنية وتطرح تحديات خاصة بنماذج التحكّم في النفاذ وبيئات التشغيل المختلفة.

ويمكن استعمال الآليات والنُهج المقدمة في هذه التوصية كمواصفات توفر عمليات تنفيذ لسياسات التحكّم في النفاذ من أجل أنساق تبادل معلومات الأمن السيبراني (CYBEX) الأساسية وبروتوكولات النقل مثل: نسق تبادل وصف الحوادث العارضة (IODEF) [b-ITU-T X.1541] والدفاع بين الشبكات في الوقت الفعلي [b-ITU-T X.1580] (RID) بالإضافة إلى نقل الدفاع بين الشبكات في الوقت الفعلي [b-ITU-T X.1581] (RIDT) والشكل المهيكل للتعبير عن معلومات التهديدات [b-stix] (STIX) إضافة إلى التبادل المؤتمت الموثوق لمعلومات المؤشرات [b-taxii] (TAXII) وغيرها.

7 تصنيف شبكات تبادل معلومات الحوادث العارضة

1.7 بيئات التشغيل

تعمل شبكات تبادل معلومات الحوادث العارضة في البيئتين التاليتين:

- ميدان ثقة وحيد (إدارة مركزية)؛
- ميادين ثقة اتحادية (إدارة لامركزية).

2.7 نماذج تبادل معلومات الحوادث العارضة

تمثّل نماذج تبادل معلومات الحوادث العارضة كالتالي:

- "بين النظراء"، تبادل أحادي أو ثنائي الاتجاه للمعلومات بين مشاركين.
- "التبادل النجمي". لهذا النوع من النماذج غالباً محور مركزي يتلقى البيانات من الأعضاء المشاركين (أذرع النجمة). ويمكن للمحور إما توزيع البيانات الواردة مباشرةً على الأعضاء الآخرين، أو توفير خدمات ذات قيمة مضافة وإرسال المعلومات الجديدة (والتي يُفترض أن تكون أكثر فائدة) إلى الأعضاء. وبهذا النهج، يعمل المحور كمركز لتبادل المعلومات يمكنه تيسير تبادل المعلومات مع حماية هويات الأعضاء في نفس الوقت. ويبرز هنا تحدّي يتمثل في أن تبادل المعلومات في هذا النموذج يحتاج إلى مستوى عال من الثقة في المحور [b-MITRE Models].
- "النشر للجميع". يمكّن هذا النموذج أي مشارك من التبادل مع قائمة الأعضاء بالكامل بدلاً من الدخول في محور مركزي. ونظراً إلى أن الأعضاء يتبادلون المعلومات مباشرة فيما بينهم، فإن نشر المعلومات يكون سريعاً ويمكن زيادته بسهولة ليطوّر الكثير من المشاركين [b-MITRE Models].

واستناداً إلى هذه النماذج الثلاثة، يمكن إنشاء النموذجين التاليين المتمحورين حول الخدمة:

- "كشف – طلب – رد". يتألف هذا النموذج من مرحلتين، حيث تستخدم في المرحلة الأولى (اختيارية) آليات الكشف [ITU-T X.1570] لتحديد المصادر المركزية أو الموزعة للمعلومات المتعلقة بالحوادث العارضة. وفي المرحلة الثانية، يتحصّل المستهلكون على المعلومات من خلال البحث في قواعد البيانات، وتستند قرارات الرد إلى نموذج التحكّم في النفاذ.
- "كشف – اشتراك – إخطار". يتألف هذا النموذج من مرحلتين، حيث تستخدم في المرحلة الأولى (اختيارية) آليات الكشف [ITU-T X.1570] لتحديد المصادر المركزية أو الموزعة للمعلومات المتعلقة بالحوادث العارضة. وفي المرحلة الثانية، يتحصّل المستهلكون على البيانات بالاشتراك وتلقّي المعلومات من مصادر مختارة في صورة إخطارات.

3.7 نماذج التحكّم في النفاذ

نماذج التحكّم في النفاذ هي أساس السياسات الأمنية. وتُصاغ عملياً بواسطة لغة وسم قابلة للتوسيع (XML) محددة – لغات (لغات سياسات التحكّم في النفاذ).

وطبقاً للنماذج [b-NIST Models]، تعرض نماذج التحكّم في النفاذ التالية بدءاً من النماذج المحافظة (التي تتبع سياسات أقل تفتيتاً) وصولاً إلى النماذج التكيفية (التي تتبع سياسات أكثر تفتيتاً ومرتبطة بالبيئة):

- **قائمة التحكّم في النفاذ/التحكّم في النفاذ الاستنسابي**. مفهوم قوائم التحكّم في النفاذ (ACL)/التحكم في النفاذ الاستنسابي (DAC)، هو المفهوم الذي يكون فيه لكل مورد على النظام الذي ينبغي التحكّم في النفاذ إليه، يشار إليه كشيء، القائمة المصاحبة الخاصة به للتقابلات بين مجموعة الكيانات التي تطلب النفاذ إلى المورد ومجموعة الإجراءات التي يمكن لكل كيان اتخاذها بشأن المورد.
- **التحكّم في النفاذ الإلزامي**. يستعمل التحكّم في النفاذ الإلزامي (MAC) في الغالبية العظمى من الأنظمة التي تراعى فيها أولوية سرية البيانات. ويعمل النفاذ MAC بتخصيص وسم تصنيف لكل مورد ملف. وتشمل التصنيفات فئة المعلومات ومستوى الحساسية، على سبيل المثال، مقيد أو سرّي أو سرّي للغاية. ويخصص لكل غرض تصنيف مماثل يطلق عليه تصريح. وعندما يحاول الغرض النفاذ إلى مورد محدد، يفحص النظام امتيازات الغرض لتحديد ما إذا كان سيُمنح النفاذ إضافة إلى مقارنة التصريح الخاص بالغرض مقابل تصنيف المورد.
- **التحكّم في النفاذ القائم على الأدوار**. في التحكّم في النفاذ القائم على الأدوار (RBAC)، يحدّد النفاذ إلى مورد ما استناداً إلى العلاقة بين الجهة الطالبة والمنظِّمة أو الجهة المالكة المتحكمة في المورد؛ وسيحدّد دور الجهة الطالبة أو وظيفتها ما إذا كان النفاذ سيُمنح أم سيُرفض.

- **التحكّم في النفاذ القائم على المهام/إدارة التحكم في النفاذ القائم على المهام**. التحكم في النفاذ القائم على المهام (TBAC)/إدارة التحكّم في النفاذ القائم على المهام [b-IEEE TBAC] (TBAM) عبارة تمديد للتحكم RBAC استناداً إلى تعريف مهام الأعمال التي تسمح بتفتيت أقل بالنسبة للتحكم في النفاذ.
- **التحكّم في النفاذ القائم على النعوت**. يستخدم نموذج التحكم في النفاذ القائم على النعوت (ABAC) آليات مثل القوائم ACL التي تضم نعوتاً لهذه الأغراض إلى جانب عمليات التشغيل المسموح بها على هذا المورد. وعندما يتطابق نعت مع النعت الموجود في القائمة ACL، يمنح الغرض الامتياز لإجراء العمليات المذكورة بالنسبة لهذا النعت في القائمة ACL على المورد.
- **التحكم في النفاذ القائم على السياسات**. التحكّم في النفاذ القائم على السياسات (PBAC) عبارة عن تنسيق وتقييس النموذج ABAC على مستوى المؤسسة دعماً لأهداف إدارية محددة. ويجمع النفاذ PBAC نعوتاً من المصدر، والبيئة، والجهة الطالبة مع معلومات عن مجموعة خاصة من الظروف التي طُلب في إطارها النفاذ، ويستعمل مجموعات قواعد تحدد ما إذا كان النفاذ سيُمنح طبقاً لسياسات تنظيمية بالنسبة لهذه النعوت في إطار هذه الظروف.
- **التحكّم في النفاذ المكيف حسب المخاطر**. صمّم نموذج التحكّم في النفاذ المكيف حسب المخاطر RAdAC لتوفير تحكّم في النفاذ في الوقت الفعلي قابل للتكيف ومدرك بالمخاطر. وهو يوسع نماذج التحكّم في النفاذ السابقة بإدخال ظروف بيئية ومستويات للمخاطر ضمن عمليات تقرير التحكم في النفاذ. وهو يجمع معلومات عن مدى أهلية شخص ما (أو آلة ما) للثقة ومعلومات عن البنية التحتية لتكنولوجيا المعلومات بالشركة وعوامل المخاطر البيئية ويستعمل كل هذه المعلومات في وضع مقياس شامل للمخاطر قابل للتقدير الكمّي. ويستعمل النفاذ RAdAC أيضاً عوامل خاصة بتقدير الموقف كمدخلات من أجل عملية اتخاذ القرار. ويمكن لمدخلات تقدير الحالة هذه أن تشمل معلومات عن مستوى التهديد الحالي الذي تواجهه المنظمة استناداً إلى البيانات المجمعة من مصادر أخرى، مثل أفرقة الاستجابة للطوارئ الحاسوبية (CERT) أفرقة الاستجابة للحوادث الأمنية الحاسوبية (CSITR) أو الجهات الموردة للخدمات الأمنية. (انظر [b-IEEE ARES] و[b-NIST RADAC]).

4.7 مستوى الثقة

لتأكيد العلاقة بين مستويات الثقة والمخاطر، يوصى بمستويات الثقة الكمية التالية في شبكات تبادل معلومات الحوادث العارضة: **منخفضة، ومتوسطة، وعالية**. وبديهياً، ينطوي على مستوى الثقة الأعلى، البساطة في المتطلبات ومستوى التفتيت بالنسبة للتحكّم في النفاذ. بمعنى أن مستوى الثقة يؤثر بشكل مباشر على مستوى تعقد آليات التحكّم في النفاذ.

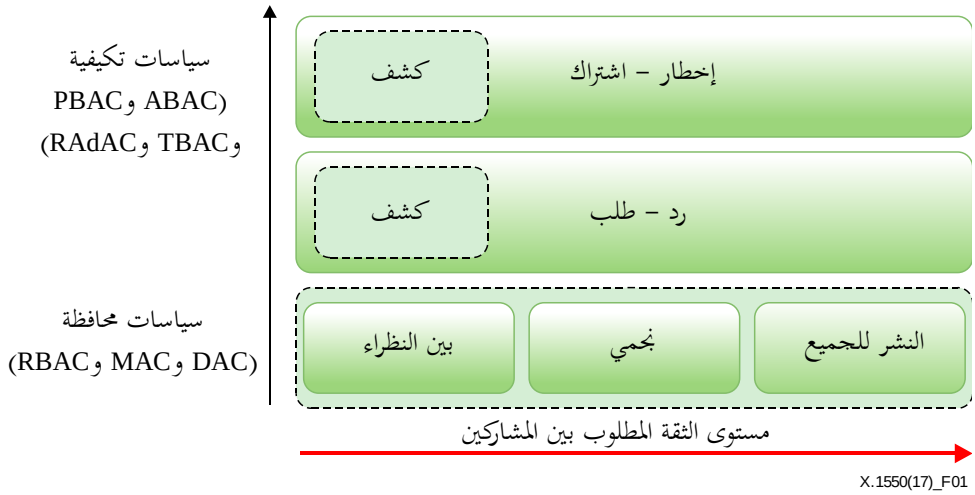
وتقنيات تقييم مستويات الثقة من حيث الكم والكيف تقع خارج نطاق هذه التوصية.

ويُنظر في الارتباطات التالية بين مستويات الثقة ونماذج التبادل:

- "النشر للجميع"، نموذج يحتاج دائماً إلى مستوى **عال** من الثقة بين المشاركين.
- "التبادل النجمي"، نموذج يحتاج دائماً إلى مستوى عال أو متوسط من الثقة (نظراً إلى أن المحور يمكن أن يقوم بترشيح المعلومات.
- "التبادل بين النظراء"، نموذج قد لا يحتاج بوجه عام درجة عالية من الثقة نظراً لأنه يمكن التحكّم في قناة الاتصالات الوحيدة بمجموعة متنوعة من الطرائق.

نماذج تبادل المستويات الأعلى لا تعتمد صراحة على درجة الثقة، ولكن بالنسبة لعدد متزايد من المشاركين وفي وجود بيئات أكثر تعقيداً، قد تحتاج هذه النماذج إلى تحكم في النفاذ أكثر تقدماً.

ومن ثم، ينظر في التصنيف التالي، المعروض في الشكل 1:



الشكل 1 – نماذج التحكم في النفاذ ونماذج التبادل وتصنيف مستويات الثقة

8 تقنيات تيسير تنفيذ سياسات التحكّم في النفاذ

1.8 توصيات بشأن تقييم لغات التعبير عن السياسات

من بين لغات التحكّم في النفاذ الراسخة التي تستعمل لتيسير تنفيذ سياسات التحكّم في النفاذ في أنظمة إدارة الهوية والنفاذ، هناك:

– لغة وسم التحكّم في النفاذ القابلة للتوسيع **(XACML)**. يعرف المعيار لغة إعلانية لسياسات التحكم في النفاذ (للنموذج ABAC) تنفذ بلغة وسم ونموذج معالجة يشرح الكيفية التي تقيّم بها طلبات النفاذ طبقاً للقواعد المحددة في السياسات.

الملاحظة 1 – اعتمد الإصدار 2.0 من اللغة XACML في صورة التوصية [b-ITU-T X.1142]

الملاحظة 2 – اعتمد الإصدار 3.0 من اللغة XACML في صورة التوصية [b-ITU-T X.1144]

– معايير البنية التحتية لإدارة الامتيازات والأدوار **(PERMIS)** عبارة عن نظام تخويل معقّد قائم على السياسات ينفذ صيغة محسنة من التحكّم RBAC (مشابهة للنفاذ ABAC). وتقوم سياسات المعايير PERMIS على اللغة XML وتوفّر سطح بيني للغة XACML يسمح بالتبادل السلس لنقاط تقرير السياسات (PDP) للمعايير PERMIS واللغة XACML.

ويوصى بتقييم إمكانية تطبيق نماذج التحكّم في النفاذ في إطار البيئات المختلفة وتحديد المتطلبات الدنيا لتنفيذها مع لغات السياسات مثل [b-ITU-T X.1142] أو [b-ITU-T X.1144] أو [b-UKENT PERMIS].

ويرد في الجدول 1 مثال لعملية التقييم:

الجدول 1 – تنفيذ نماذج التحكّم في النفاذ في إطار بيئات مختلفة بلغات تعريف السياسات

النموذج/ البيئة	ACL/ DAC	MAC	RBAC	ABAC	TBAC/ TBAM	PBAC	RAdAC
مركزية	[b-ITU-T X.1142]؛ PERMIS	تجريبي XACML	[b-ITU-T X.1142]؛ PERMIS	[b-ITU-T X.1142]؛ PERMIS*	تجريبي	[b-ITU-T X.1142]؛ PERMIS*	[b-ITU-T X.1142]؛ PERMIS*
اتحادية	[b-ITU-T X.1144]؛ PERMIS	تجريبي XACML	[b-ITU-T X.1144]؛ PERMIS	[b-ITU-T X.1144]؛ PERMIS*	تجريبي	–	[b-ITU-T X.1144]

الملاحظة 1 – الإصدار 2 من اللغة XACML [b-ITU-T X.1142] والإصدار 3 منها [b-ITU-T X.1144] منفصلان نظراً إلى أن "التفويض"، المطلوب بالنسبة لمعظم البيئات الاتحادية، يظهر في الإصدار 3 من اللغة.

الملاحظة 2 – تحتاج عمليات تنفيذ النفاذ MAC المعروف إلى تمديد للغة XACML.

الملاحظة 3 – تحتاج عمليات تنفيذ التحكم TBAC/الإدارة TBAM الحالية إلى تمديد للغة XACML والتي تعتبر تجريبية.

الملاحظة 4 – لا يطبق التحكم PBAC طبقاً لتعريفه إلا على البيئات المركزية، بينما قد تحتاج البيئات الاتحادية إلى استعمال التحكّم RAdAC.

الملاحظة 5 – ترد بعض القيود الخاصة بتنفيذ المعايير PERMIS للتحكم ABAC (وPBAC وRAdAC إذا ما اعتبرناهما تمديدين للنموذج ABAC) في [b-UKENT PERMIS]، عندما يضاف إليها الرمز *، أي *PERMIS.

2.8 اعتبارات بشأن حل التضارب بين السياسات

يؤدي التضارب بين سياسات التحكّم في النفاذ إلى إجراءات متناقضة لقاعدتين أو أكثر من قواعد السياسات. والآلية الأساسية للحد من أوجه التضارب بين السياسات تتمثل في تصميم قواعد السياسات بصورة واضحة لا لبس فيها (*حل التضارب السكوني*). وهناك نهج آخر يقوم على تقييم السياسات وقت التشغيل *(حل التضارب الدينامي)* [b-UKENT PERMIS].

وفي حين يعتبر حل التضارب السكوني مجدياً بالنسبة للأنظمة المركزية [b-USB CONFLICT] و [b-SPIIRAN POLICY]، قد يكون من الصعب تحقيق الحل السكوني في بيئة اتحادية دينامية.

وتتسم الاستراتيجيات الأساسية لحل التضارب السكوني بما يلي:

- الرفض – يطغى. القواعد المتضاربة مجمعة، ويفضل الإجراء "الرفض" على "السماح".
- السماح – يطغى. القواعد المتضاربة مجمعة، ويفضل الإجراء "السماح" على "الرفض".
- الأول – يطبق. ينفذ الإجراء الأول ضمن القواعد المتضاربة.

تضم استراتيجيات حل التضارب بين السياسات دينامياً [b-UKENT PERMIS] خوارزميات من أجل اختيار الاستراتيجية السكونية المناسبة فيما يتعلق بالسياق الحالي لطلب النفاذ.

ويوصى بتقييم استراتيجيات حل التضارب من منظور الأداء والتوافق مع نماذج التحكّم في النفاذ في إطار بيئات مختلفة.

وبالنظر إلى تقييم الأداء لحل التضارب بين *السياسات سكونياً* [b- IJCSIT XACML] بالاشتراك مع تحكم دينامي في النفاذ مثل [b-FUSCAT RADAC]، يوصى بتدنية عدد السياسات دون الإخلال بمستوى ضمان الأمن أو استخدام استراتيجيات حل التضارب بين *السياسات دينامياً*.

ويرد في الجدول 2 مثال لعملية التقييم:

الجدول 2 – حل أشكال التضارب بين السياسات بالنسبة لنماذج التحكّم في النفاذ في إطار بيئات مختلفة

النموذج/البيئة	ACL/ DAC	MAC	RBAC	ABAC	TBAC/ TBAM	PBAC (ملاحظة)	RAdAC
مركزية	سكوني	سكوني	سكوني	سكوني	سكوني	سكوني	دينامي
اتحادية	دينامي	دينامي	دينامي	دينامي	دينامي	–	دينامي
ملاحظة – لا يطبّق التحكم PBAC طبقاً لتعريفه إلا في البيئات المركزية.							

3.8 توصيات بشأن تقييم الأداء

على الرغم من أن لغات الوسم (مثل [b-W3C XML] و[b-ECMA JSON]) مصممة بحيث يسهل للإنسان قراءتها، فإن هناك كمية كبيرة من القواعد المتداخلة والمتقدمة يمكن أن تفرض مهمة صعبة تتمثل في توصيف السياسات المنفذة وتدارك أخطائها.

وخدمات تبادل معلومات الحوادث العارضة المعقدة في شبكات تبادل معلومات الحوادث العارضة قد تستوجب استعمال نماذج متقدمة للتحكم في النفاذ. وبالنظر إلى التشغيل في بيئات اتحادية، يمكن لذلك أن يؤدي إلى تدهور أداء شبكات تبادل معلومات الحوادث العارضة، بما يؤدي إلى ظهور قضايا تتعلق بضمان الأمن.

ولأغراض تقييم الجودة/الأداء/الامتثال للسياسات، يمكن حساب مقاييس مقابلة. وآليات تقييم هذه المقاييس بالنسبة لشبكات تبادل معلومات الحوادث العارضة خارج نطاق هذه التوصية. ومع ذلك، يوصى بمجموعة من المعايير والمؤشرات الخاصة بهذا التقييم [b-KIT PERFIAM] و[b-NIST METRICS]:

- **وقت الاستجابة**. وقت الاستجابة بالنسبة لمكونات البنية التحتية لإدارة الهوية والنفاذ (IAM)، ومكونات تبادل المعلومات يمكن من تقييم مقاييس الأداء.
- **قرارات خاطئة للتحكم في النفاذ**. تقييم عدد قرارات الاستيقان أو التخويل الخاطئة في المواقف الصعبة يوفر معلومات عن متانة البنية التحتية الأساسية لإدارة الهوية والنفاذ.
- **المكونات الموثوقة**. التحكم في النفاذ مهمة حساسة تحتاج إلى مستوى معين من الثقة بين الكيانات المتعاونة. وبالتالي، من المفيد وجود مقياس يدرج المكونات الموثوقة بالنسبة لأي قرار للتحكّم في النفاذ وذلك لتحديد التسرّب المحتمل للبيانات.
- **توزيع السياسات**. يستخدم لتقييم إمكانيات توزيع السياسات وأداء هذا التوزيع في أنظمة مركزية أو اتحادية للتحكم في النفاذ.
- **سهولة تخصيص الامتيازات**. تحدد عدد الخطوات اللازمة لتخصيص/تغيير/إلغاء/توثيق إمكانيات الأغراض أو المجموعات.
- **جودة التعبير عن السياسات**. تحدد ما إذا كان التحكم في النفاذ يمكن تعريفه عبر تعبيرات منطقية وقابلة للبرمجة.
- **قدرات التفويض**. تحدد ما إذا كان بمقدور نظام التحكّم في النفاذ تفويض الامتيازات للأغراض.
- **تجميع السياسات وحل التضارب بينها**. يحدد استراتيجيات تجميع السياسات التي تستخدم في حل أوجه التضارب (إن وجدت).
- **التجنّب**. يحدد ما إذا كان أي مكون من المكونات يغفل سياسات التحكّم في النفاذ.
- **السلامة**. تحدد قدرات إنفاذ السلامة مثل القيود الخاصة بقواعد التحكّم في النفاذ التي تستخدم لمنع زيادة الامتيازات.
- **التفتت**. يحدد مستوى التفتت الذي يمكن لنظام تحكّم في النفاذ أن يضبطه. ويمكن أن يعكس ذلك مجموعة من نعوت الأغراض التي يجري تقييمها أثناء عملية التحكم في النفاذ.
- **دمج الاستيقان**. يحدد ما إذا كان بمقدور نظام التحكّم في النفاذ الاندماج مع أنظمة الاستيقان.

بيبليوغرافيا

[b-ITU-T M.3345] Recommendation ITU-T M.3345 (2009), *Principles for self-service management*.

[b-ITU-T M.3410] Recommendation ITU-T M.3410 (2008), *Guidelines and requirements for security management systems to support telecommunications management*.

[b-ITU-T X.1036] Recommendation ITU-T X.1036 (2007), *Framework for creation, storage, distribution and enforcement of policies for network security*.

[b-ITU-T X.1142] Recommendation ITU-T X.1142 (2006), *eXtensible Access Control Markup Language (XACML 2.0)*.

[b-ITU-T X.1144] Recommendation ITU-T X.1144 (2013), *eXtensible Access Control Markup Language (XACML 3.0)*.

[b-ITU-T X.1252] Recommendation ITU-T X.1252 (2010), *Baseline identity management terms and definitions*.

[b-ITU-T X.1541] Recommendation ITU-T X.1541 (2012), *Incident object description exchange format*.

[b-ITU-T X.1580] Recommendation ITU-T X.1580 (2012), *Real-time inter-network defence*.

[b-ITU-T X.1581] Recommendation ITU-T X.1581 (2012), *Transport of real-time inter-network defence messages*.

[b-IEEE TBAC] IEEE IET Software (2008), *Types for task-based access control in workflow systems*.

[b-IEEE ARES] IEEE (2011), *Sixth International Conference on Availability, Reliability and Security (ARES), An Attribute Based Framework for Risk-Adaptive Access Control Models*.

[b-ECMA JSON] ECMA International (2013), *The JSON Data Interchange Format*.

[b-FUSCAT RADAC] Federal University of Santa Catarina (2014), *A Dynamic Risk-based Access Control Architecture for Cloud Computing*.

[b-IJCSIT XACML] International Journal of Computer Science and Information Technology (IJCSIT) (2010), *Design and evaluation of XACML conflict policies detection mechanism*.

[b-KIT PERFIAM] Karlsruhe Institute of Technology (2009), *Performance Evaluation of Identity and Access Management Systems in Federated Environments*.

[b-MITRE Models] The MITRE Corporation (2012), *Cyber Information-Sharing Models*.

[b-NIST METRICS] NIST Internal Report 7874 (2012), *Guidelines for Access Control System Evaluation Metrics*. [b-NIST Models] NIST Computer Security Division (2009), *A survey of access control models*.

[b-NIST RADAC] NIST Computer Security Division (2009), *Risk-adaptable access control (RAdAC)*.

[b-SPIIRAN POLICY] SPIIRAN (2006), *Conflict Detection and Resolution in Security Policies of Computer Networks*.

[b-stix] OASIS CTI TC (2017), *A structured language for cyber threat intelligence*. <https://oasis-open.github.io/cti-documentation/>

[b-taxii] OASIS CTI TC (2017), *A transport mechanism for sharing cyber threat intelligence*. <https://oasis-open.github.io/cti-documentation/>

[b-UKENT PERMIS] The University of Kent (2013), *Adding privacy protection to policy based authorisation systems*.

[b-USB CONFLICT] IEEE First AESS European Conference on Satellite Telecommunications (ESTEL) (2012), *Conflict detection in security policies using Semantic Web technology*.

[b-W3C XML] W3C (1997), *Extensible Markup Language (XML)*.

سلاسل التوصيات الصادرة عن قطاع تقييس الاتصالات

السلسلة A	تنظيم العمل في قطاع تقييس الاتصالات
السلسلة D	مبادئ التعريفة والمحاسبة والقضايا الاقتصادية والسياساتية المتصلة بالاتصالات/تكنولوجيا المعلومات والاتصالات على الصعيد الدولي
السلسلة E	التشغيل العام للشبكة والخدمة الهاتفية وتشغيل الخدمات والعوامل البشرية
السلسلة F	خدمات الاتصالات غير الهاتفية
السلسلة G	أنظمة الإرسال ووسائطه والأنظمة والشبكات الرقمية
السلسلة H	الأنظمة السمعية المرئية والأنظمة متعددة الوسائط
السلسلة I	الشبكة الرقمية متكاملة الخدمات
السلسلة J	الشبكات الكبلية وإرسال إشارات تلفزيونية وبرامج صوتية وإشارات أخرى متعددة الوسائط
السلسلة K	الحماية من التداخلات
السلسلة L	البيئة وتكنولوجيا المعلومات والاتصالات، وتغير المناخ، والمخلفات الإلكترونية، وكفاءة استخدام الطاقة، وإنشاء الكبلات وغيرها من عناصر المنشآت الخارجية وتركيبها وحمايتها
السلسلة M	إدارة الاتصالات بما في ذلك شبكة إدارة الاتصالات وصيانة الشبكات
السلسلة N	الصيانة: الدارات الدولية لإرسال البرامج الإذاعية الصوتية والتلفزيونية
السلسلة O	مواصفات تجهيزات القياس
السلسلة P	نوعية الإرسال الهاتفي والمنشآت الهاتفية وشبكات الخطوط المحلية
السلسلة Q	التبديل والتشوير، والقياسات والاختبارات المرتبطة بهما
السلسلة R	الإرسال البرقي
السلسلة S	التجهيزات المطرافية للخدمات البرقية
السلسلة T	المطاريف الخاصة بالخدمات التليماتية
السلسلة U	التبديل البرقي
السلسلة V	اتصالات البيانات على الشبكة الهاتفية
السلسلة X	**شبكات البيانات والاتصالات بين الأنظمة المفتوحة ومسائل الأمن**
السلسلة Y	البنية التحتية العالمية للمعلومات، والجوانب الخاصة ببروتوكول الإنترنت وشبكات الجيل التالي وإنترنت الأشياء والمدن الذكية
السلسلة Z	اللغات والجوانب العامة للبرمجيات في أنظمة الاتصالات

طُبعت في سويسرا
جنيف، 2018