Unión Internacional de Telecomunicaciones

UIT-T

SECTOR DE NORMALIZACIÓN
DE LAS TELECOMUNICACIONES
DE LA UIT

X.1550

(03/2017)

SERIE X: REDES DE DATOS, COMUNICACIONES DE SISTEMAS ABIERTOS Y SEGURIDAD

Intercambio de información de ciberseguridad – Intercambio de políticas

Modelos de control de acceso para redes de intercambio de incidentes

Recomendación UIT-T X.1550

RECOMENDACIONES UIT-T DE LA SERIE X

REDES DE DATOS, COMUNICACIONES DE SISTEMAS ABIERTOS Y SEGURIDAD

REDES PÚBLICAS DE DATOS	X.1–X.199
INTERCONEXIÓN DE SISTEMAS ABIERTOS	X.200–X.299
INTERFUNCIONAMIENTO ENTRE REDES	X.300–X.399
SISTEMAS DE TRATAMIENTO DE MENSAJES	X.400–X.499
DIRECTORIO	X.500–X.599
GESTIÓN DE REDES DE INTERCONEXIÓN DE SISTEMAS ABIERTOS Y ASPECTOS DE SISTEMAS	X.600–X.699
GESTIÓN DE INTERCONEXIÓN DE SISTEMAS ABIERTOS	X.700–X.799
SEGURIDAD	X.800–X.849
APLICACIONES DE INTERCONEXIÓN DE SISTEMAS ABIERTOS	X.850–X.899
PROCESAMIENTO DISTRIBUIDO ABIERTO	X.900–X.999
SEGURIDAD DE LA INFORMACIÓN Y DE LAS REDES	
Aspectos generales de la seguridad	X.1000–X.1029
Seguridad de las redes	X.1030–X.1049
Gestión de la seguridad	X.1050–X.1069
Telebiometría	X.1080–X.1099
APLICACIONES Y SERVICIOS CON SEGURIDAD	
Seguridad en la multidifusión	X.1100–X.1109
Seguridad en la red residencial	X.1110–X.1119
Seguridad en las redes móviles	X.1120–X.1139
Seguridad en la web	X.1140–X.1149
Protocolos de seguridad	X.1150–X.1159
Seguridad en las comunicaciones punto a punto	X.1160–X.1169
Seguridad de la identidad en las redes	X.1170–X.1179
Seguridad en la TVIP	X.1180–X.1199
SEGURIDAD EN EL CIBERESPACIO	
Ciberseguridad	X.1200–X.1229
Lucha contra el correo basura	X.1230–X.1249
Gestión de identidades	X.1250–X.1279
APLICACIONES Y SERVICIOS CON SEGURIDAD	
Comunicaciones de emergencia	X.1300–X.1309
Seguridad en las redes de sensores ubicuos	X.1310–X.1339
Recomendaciones relacionadas con la PKI	X.1340–X.1349
Seguridad en la Internet de las cosas (IoT)	X.1360–X.1369
Seguridad en los sistema de transporte inteligente (ITS)	X.1370–X.1379
INTERCAMBIO DE INFORMACIÓN DE CIBERSEGURIDAD	
Aspectos generales de la ciberseguridad	X.1500–X.1519
Intercambio de estados/vulnerabilidad	X.1520–X.1539
Intercambio de eventos/incidentes/heurística	X.1540–X.1549
Intercambio de políticas	**X.1550–X.1559**
Petición de heurística e información	X.1560–X.1569
Identificación y descubrimiento	X.1570–X.1579
Intercambio asegurado	X.1580–X.1589
SEGURIDAD DE LA COMPUTACIÓN EN NUBE	
Visión general de la seguridad de la computación en nube	X.1600–X.1601
Diseño de la seguridad de la computación en nube	X.1602–X.1639
Prácticas óptimas y directrices en materia de seguridad de la computación en nube	X.1640–X.1659
Aplicación práctica de la seguridad de la computación en nube	X.1660–X.1679
Otras cuestiones de seguridad de la computación en nube	X.1680–X.1699

Para más información, véase la Lista de Recomendaciones del UIT-T.

Recomendación UIT-T X.1550

Modelos de control de acceso para redes de intercambio de incidentes

Resumen

En la Recomendación UIT-T X.1550 se describen los métodos existentes para la implementación de las políticas de control de acceso en las redes de intercambio de incidentes. En esta Recomendación se describen varios modelos de control de acceso consolidados, modelos de compartición así como criterios para evaluar la calidad de funcionamiento de una red de intercambio de incidentes. Se analizan soluciones normalizadas para facilitar la implementación de modelos de control de acceso diferentes en modelos de compartición de información de ciberseguridad diferentes y en entornos con diversos niveles de confianza.

Historia

Edición	Recomendación	Aprobación	Comisión de Estudio	ID único*
1.0	ITU-T X.1550	2017-03-30	17	11.1002/1000/13198

Palabras clave

Autorización, CERT, control de acceso, CSIRT, CYBEX, IAM, red de intercambio de incidentes, respuesta ante incidentes

* Para acceder a la Recomendación, sírvase digitar el URL http://handle.itu.int/ en el campo de dirección del navegador, seguido por el identificador único de la Recomendación. Por ejemplo, http://handle.itu.int/11.1002/1000/11830-en.

PREFACIO

La Unión Internacional de Telecomunicaciones (UIT) es el organismo especializado de las Naciones Unidas en el campo de las telecomunicaciones y de las tecnologías de la información y la comunicación. El Sector de Normalización de las Telecomunicaciones de la UIT (UIT-T) es un órgano permanente de la UIT. Este órgano estudia los aspectos técnicos, de explotación y tarifarios y publica Recomendaciones sobre los mismos, con miras a la normalización de las telecomunicaciones en el plano mundial.

La Asamblea Mundial de Normalización de las Telecomunicaciones (AMNT), que se celebra cada cuatro años, establece los temas que han de estudiar las Comisiones de Estudio del UIT-T, que a su vez producen Recomendaciones sobre dichos temas.

La aprobación de Recomendaciones por los Miembros del UIT-T es el objeto del procedimiento establecido en la Resolución 1 de la AMNT.

En ciertos sectores de la tecnología de la información que corresponden a la esfera de competencia del UIT-T, se preparan las normas necesarias en colaboración con la ISO y la CEI.

NOTA

En esta Recomendación, la expresión "Administración" se utiliza para designar, en forma abreviada, tanto una administración de telecomunicaciones como una empresa de explotación reconocida de telecomunicaciones.

La observancia de esta Recomendación es voluntaria. Ahora bien, la Recomendación puede contener ciertas disposiciones obligatorias (para asegurar, por ejemplo, la aplicabilidad o la interoperabilidad), por lo que la observancia se consigue con el cumplimiento exacto y puntual de todas las disposiciones obligatorias. La obligatoriedad de un elemento preceptivo o requisito se expresa mediante las frases "tener que, haber de, hay que + infinitivo" o el verbo principal en tiempo futuro simple de mandato, en modo afirmativo o negativo. El hecho de que se utilice esta formulación no entraña que la observancia se imponga a ninguna de las partes.

PROPIEDAD INTELECTUAL

La UIT señala a la atención la posibilidad de que la utilización o aplicación de la presente Recomendación suponga el empleo de un derecho de propiedad intelectual reivindicado. La UIT no adopta ninguna posición en cuanto a la demostración, validez o aplicabilidad de los derechos de propiedad intelectual reivindicados, ya sea por los miembros de la UIT o por terceros ajenos al proceso de elaboración de Recomendaciones.

En la fecha de aprobación de la presente Recomendación, la UIT no ha recibido notificación de propiedad intelectual, protegida por patente, que puede ser necesaria para aplicar esta Recomendación. Sin embargo, debe señalarse a los usuarios que puede que esta información no se encuentre totalmente actualizada al respecto, por lo que se les insta encarecidamente a consultar la base de datos sobre patentes de la TSB en la dirección http://www.itu.int/ITU-T/ipr/.

ÍNDICE

Recomendación UIT-T X.1550

Modelos de control de acceso para redes de intercambio de incidentes

1 Alcance

En la presente Recomendación se describen los métodos existentes para la implementación de las políticas de control de acceso en las redes de intercambio de incidentes. En esta Recomendación se describen varios modelos de control de acceso consolidados, modelos de compartición así como criterios para evaluar la calidad de funcionamiento de una red de intercambio de incidentes. Se analizan soluciones normalizadas para facilitar la implementación de modelos de control de acceso diferentes en modelos de compartición de información de ciberseguridad diferentes y en entornos con diversos niveles de confianza.

2 Referencias

Las siguientes Recomendaciones UIT-T y demás referencias contienen disposiciones que, por referencia a las mismas en este texto, constituyen disposiciones de esta Recomendación. En la fecha de publicación, las ediciones citadas estaban en vigor. Todas las Recomendaciones y demás referencias están sujetas a revisión, por lo que se alienta a los usuarios de esta Recomendación a que consideren la posibilidad de aplicar la edición más reciente de las Recomendaciones y demás referencias que se indican a continuación. Se publica periódicamente una lista de las Recomendaciones UIT-T vigentes. La referencia a un documento en el marco de esta Recomendación no confiere al mismo, como documento autónomo, el rango de Recomendación.

[UIT-T X.1500] Recomendación UIT-T X.1500 (2011), *Aspectos generales del intercambio de información de ciberseguridad.*

[UIT-T X.1570] Recomendación UIT-T X.1570 (2011), *Mecanismos de descubrimiento en el intercambio de información de ciberseguridad.*

3 Definiciones

3.1 Términos definidos en otros documentos

En la presente Recomendación se utilizan los siguientes términos definidos en otros documentos:

3.1.1 control de acceso [b-UIT-T X.1252]: Procedimiento utilizado para determinar si se debe conceder a una entidad acceso a recursos, instalaciones, servicios o informaciones, sobre la base de normas preestablecidas, y la autoridad o los derechos específicos asociados a la parte solicitante

3.1.2 autorización [b-UIT-T M.3345]: Indica, cómo, y bajo qué condiciones, los actores de gestión del autoservicio pueden utilizar funciones de autoservicio y qué acciones de autoservicio pueden utilizar.

3.1.3 intercambio de incidentes [UIT-T X.1570]: Transferencia de información de ciberseguridad entre dos o más entidades de ciberseguridad. Esta transferencia puede ser unidireccional o bidireccional, multidireccional, es decir, de muchos a muchos.

NOTA – En la presente Recomendación el término "intercambio de incidentes" se considera equivalente a "intercambio".

3.1.4 dominio de confianza [b-UIT-T M.3410]: Conjunto de informaciones y recursos asociados como usuarios, redes, repositorios de datos y aplicaciones que manipulan los datos en esos repositorios de datos. Diferentes dominios de confianza pueden compartir los mismos componentes físicos. Y, un dominio de confianza único puede utilizar niveles de confianza diferentes, dependiendo de lo que pueden saber los usuarios y de la sensibilidad de la información y los recursos asociados.

3.2 Términos definidos en la presente Recomendación

En la presente Recomendación se definen los siguientes términos:

3.2.1 conflicto de política de control de acceso: Define las acciones de dos normas contradictorias entre sí. La entidad que aplica la política no podrá determinar qué acción ejecutar.

NOTA – Esta definición se basa en la definición de "conflicto de política" que puede encontrarse en [b-UIT-T X.1036].

3.2.2 resolución dinámica de conflicto de política: Estrategia de resolución de conflicto aplicada en la fase de funcionamiento.

3.2.3 redes de intercambio de incidentes: Generalización de las infraestructuras operacionales de intercambio de información de ciberseguridad (CYBEX) con gestión centralizada o federada.

3.2.4 información de incidentes: Subconjunto de información de ciberseguridad, información o conocimientos estructurados relativos al análisis de incidentes o eventos.

NOTA – Esta definición se basa en la descripción de "intercambio (de información de seguridad)" que puede encontrarse en [b-UIT-T X.1570].

3.2.5 resolución estática de conflicto de política: Estrategia de resolución de conflicto aplicada en la fase de diseño.

4 Siglas y acrónimos

En esta Recomendación se utilizan los siguientes acrónimos y abreviaturas:

ABAC Control de acceso basado en atributos (*attribute based access control*)

ACL Lista de control de acceso (*access control list*)

CERT Equipo de respuesta ante emergencias informáticas (*computer emergency response team*)

CSIRT Equipo de respuesta ante incidentes de seguridad informática (*computer security incident response team*)

CYBEX Intercambio de información de ciberseguridad (*CYBersecurity information EXchange*)

DAC Control de acceso discrecional (*discretionary access control*)

IAM Gestión de identidad y acceso (*identity and access management*)

IODEF Formulario para el intercambio de descripciones de objetos de incidentes (*incident object description exchange format*)

IT Tecnología de la información (*information technology*)

MAC Control de acceso obligatorio (*mandatory access control*)

PBAC Control de acceso basado en políticas (*policy based access control*)

PDP Punto de decisión de política (*policy decision point*)

PERMIS Normas para infraestructuras de gestión de privilegios y funciones (*privilege and role management infrastructure standards*)

RAdAC Control de acceso adaptable al riesgo (*risk-adaptive access control*)

RBAC Control de acceso basado en roles (*role based access control*)

RID Defensa entre redes en tiempo real (*real-time inter-network defense*)

RIDT Transporte de la defensa entre redes en tiempo real (*real-time inter-network defense transport*)

STIX Expresión estructurada de información de amenaza (*structured threat information expression*)

TAXII Intercambio automatizado confiable de información de indicadores (*trusted automated exchange of indicator information*)

TBAC Control de acceso basado en tareas (*task based access control*)

TBAM Gestión de acceso basado en tareas (*task based access management*)

XACML Lenguaje de marcaje de control de acceso extensible (*eXtensible access control markup language*)

XML Lenguaje de marcaje extensible (*eXtended markup language*)

5 Convenios

En el contexto de la presente Recomendación, el "control de acceso" se considera un mecanismo genérico que soporta unos procedimientos de autorización.

6 Visión general

La reducción del riesgo puede ser necesaria para reducir los costes financieros asociados a la protección frente a los ataques informáticos y para proporcionar seguridad en una organización o colaboración, un sistema o un servicio. Las redes de intercambio de incidentes funcionan para prevenir o reducir el riesgo de los ataques informáticos. Las prácticas de intercambio de incidentes de ciberseguridad definen varios modelos de compartición de información con entornos centralizados o federados. La compartición de información de incidentes se basa en un nivel de confianza relacionado con los riesgos asociados, e impone la necesidad de asegurar que no se comparte información confidencial o sensible de manera inadecuada. Algunos modelos de control de acceso son, en consecuencia, más efectivos que otros en términos de calidad de funcionamiento, de implementación y de aseguramiento de la seguridad.

El crecimiento global y la integración de los sistemas de información mundiales han propiciado el desarrollo de modelos avanzados de control de acceso que son la base de los procesos de autorización. Los lenguajes existentes de políticas de control de acceso facilitan el desarrollo de políticas de seguridad pero plantean dificultades específicas en algunos modelos de control de acceso y entornos de funcionamiento.

Los mecanismos y enfoques presentados en esta Recomendación pueden utilizarse como perfiles para facilitar la definición de las políticas de control de acceso para los formatos y los protocolos de transporte de intercambio de información de ciberseguridad (CYBEX) utilizados, como pueden ser, entre otros: Formato para el intercambio de descripciones de objetos de incidentes (IODEF) [b-UIT-T X.1541], Defensa entre redes en tiempo real (RID) [b-UIT-T X.1580] + Transporte de mensajes de defensa entre redes en tiempo real (RIDT) [b-UIT-T X.1581], Expresión estructurada de información de amenaza (STIX) [b-stix] + Intercambio automatizado confiable de información de indicadores (TAXII) [b-taxii].

7 Taxonomía de las redes de intercambio de incidentes

7.1 Entornos de funcionamiento

Las redes de intercambio de incidentes funcionan en los siguientes entornos:

– Dominio de confianza único (gestión centralizada);

– Dominios de confianza federados (gestión descentralizada).

7.2 Modelos de intercambio de información de incidentes

Los modelos de intercambio de información de incidentes son los siguientes:

– "Entre pares", intercambio de información unidireccional o bidireccional entre dos participantes.

– "En estrella". Este tipo de red en estrella (*Hub-Spoke*) suele tener un Centro que recibe los datos de los miembros participantes. En este caso, el Centro puede redistribuir los datos que recibe directamente a los otros miembros o puede ofrecer servicios de valor añadido y enviar solo la información nueva (probablemente la más útil) a los miembros. Con este modelo, el Centro actúa como un centro de intercambio de información que facilita el intercambio de la misma pero protege la identidad de sus miembros. Un problema de este modelo es que la compartición de información requiere un alto nivel de confianza en el Centro. [b-MITRE Models].

– "Envío a todos". Este modelo permite a cualquier participante compartir la información con toda la lista de miembros en vez de pasar por un Centro. Como los miembros comparten directamente entre ellos, la distribución de la información es rápida y puede escalar fácilmente a muchos participantes. [b-MITRE Models].

Sobre la base de los tres modelos anteriores, pueden construirse los siguientes modelos orientados al servicio:

– "Indagación-petición-respuesta". Este modelo se compone de dos etapas donde en la primera etapa (opcional) se utilizan mecanismos de indagación [UIT-T X.1570] para identificar las fuentes, centralizadas o distribuidas, de información sobre incidentes. En la segunda etapa, los clientes adquieren la información realizando la petición a las bases de datos, las decisiones de respuesta se basan en el modelo de control de acceso.

– "Indagación-suscripción-notificación". Este modelo se compone de dos etapas donde en la primera etapa (opcional) se utilizan mecanismos de indagación [UIT-T X.1570] para identificar las fuentes, centralizadas o distribuidas, de información sobre incidentes. En la segunda etapa, los clientes adquieren la información mediante suscripción y la reciben desde fuentes seleccionadas en forma de notificaciones.

7.3 Modelos de control de acceso

Los modelos de control de acceso son la base de las políticas de seguridad. En la práctica, se definen con dialectos específicos del lenguaje de marcaje extensible (XML) (lenguajes de políticas de control de acceso).

A continuación, se describen los siguientes modelos de control de acceso, definidos en [b-NIST Models], empezando por los modelos más conservadores (que consideran una políticas menos granulares) hasta los modelos adaptables (que consideran unas políticas más granulares y dependientes del entorno):

– **ACL/DAC**. En el concepto de listas de control de acceso (ACL)/Control de acceso discrecional (DAC) cada recurso de un sistema cuyo acceso debe controlarse, denominado objeto, tiene su propia lista de correspondencias entre el conjunto de entidades que solicitan el acceso al recurso y el conjunto de acciones que cada entidad puede realizar con el recurso.

– **MAC**. El control de acceso obligatorio (MAC) se utiliza más a menudo en los sistemas donde la confidencialidad de los datos es prioritaria. MAC funciona mediante la asignación de una etiqueta de clasificación a cada recurso de almacenamiento. La clasificación incluye una categoría de información y un nivel de sensibilidad, por ejemplo confidencial, secreto o muy secreto. Cada sujeto tiene asignado una clasificación similar denominada acreditación. Cuando un sujeto intenta acceder a un recurso específico, el sistema controla los privilegios del sujeto para determinar si permite el acceso, y también compara la acreditación del sujeto con la clasificación del recurso.

– **RBAC**. En el control de acceso basado en roles (RBAC), el acceso a un recurso se define en función de la relación existente entre el solicitante y la organización o propietario que controlan el recurso; la función del controlador determinará si se concede o deniega el acceso.

– **TBAC/TBAM**. El control de acceso basado en tareas (TBAC)/gestión de acceso basado en tareas (TBAM) [b-IEEE TBAC] es una extensión del RBAC basado en la definición de tares de negocio que permiten una granularidad más fina del control de acceso.

– **ABAC**. El modelo de control de acceso basado en atributos (ABAC) emplea mecanismos como las listas de control de acceso (ACL) que contienen los atributos de los sujetos junto con las operaciones autorizadas en cada recurso. Cuando un atributo corresponde con el de la lista ACL, se concede al sujeto el privilegio adecuado para poder realizar las operaciones sobre el recurso indicadas en la ACL para este atributo.

– **PBAC**. El control de acceso basado en políticas (PBAC) es una armonización y una normalización del modelo ABAC para empresas con el fin de poder tener en cuenta los objetivos específicos de la dirección. El PBAC combina los atributos del recurso, el entorno y el solicitante con información del conjunto concreto de circunstancias en las cuales se realiza la solicitud de acceso, y utiliza conjuntos de reglas que determinan si se autoriza el acceso, en función de una política de organización, para esos atributos y en esas circunstancias.

– **RAdAC**. El modelo de control de acceso adaptable al riesgo (RAdAC) se diseñó para proporcionar un control de acceso en tiempo real, adaptable y con conocimiento del riesgo. El RAdAC amplía otros modelos de control de acceso anteriores al introducir las condiciones del entorno y los niveles de riesgo en el proceso de decisión del control de acceso. Combina la información de fiabilidad de una persona, o máquina, información sobre la infraestructura de tecnología de la información (TI) y factores de riesgo del entorno, y utiliza todas estas informaciones para realizar una valoración global del riesgo cuantificable. El RAdAC también utiliza factores de situación para el proceso de toma de decisión. Estos factores de situación pueden incluir información sobre el nivel de amenaza actual que tiene una organización en función de los datos obtenidos de otras fuentes como equipos de respuesta ante emergencias informáticas (CERT), equipos de respuesta ante incidentes de seguridad informática (CSIRT) o empresas de seguridad. (Véase [b-IEEE ARES] y [b-NIST RADAC].)

7.4 Nivel de confianza

Con el fin de subrayar la dependencia entre los niveles de confianza y los riegos, se recomiendan los siguientes niveles cuantitativos de confianza en las redes de intercambio de incidentes: **bajo**, **medio**, **alto**. Es implícito que cuanto más alto sea el nivel de confianza, menores serán los requisitos y la granularidad del control de acceso. Es decir que el nivel de confianza influye directamente en la complejidad de los mecanismos de control de acceso.

Las técnicas para evaluar los niveles cuantitativos y cualitativos de confianza quedan fuera del alcance de esta Recomendación.

Se considera la siguiente relación entre los niveles de confianza y los modelos de compartición:

– El modelo "envío a todos" requiere habitualmente un nivel de confianza **alto** entre participantes.

– El modelo "en estrella" suele requerir un nivel de confianza alto o medio (pues el Centro puede filtrar información).

– El modelo "entre pares", en general puede no necesitar un nivel de confianza alto, pues el canal de comunicación único puede controlarse mediante diferentes métodos.

Los modelos de compartición de alto nivel no dependen explícitamente del nivel de confianza, pero con un número creciente de participantes y en presencia de entornos más complejos, estos modelos pueden requerir modelos de control de acceso más avanzados.

En consecuencia, se considera la siguiente clasificación (Figura 1):

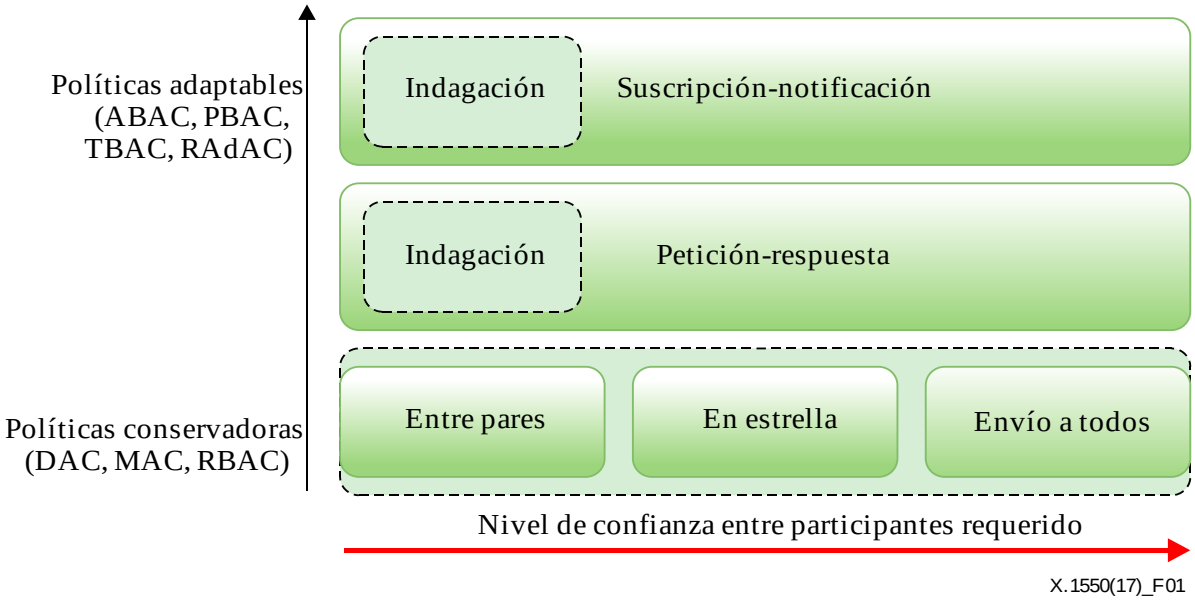

Figura 1 – Clasificación de modelos de control de acceso, modelos de compartición y niveles de confianza

8 Técnicas para facilitar la implementación de las políticas de control de acceso

8.1 Recomendaciones para la evaluación de los lenguajes de expresión de políticas

Entre los lenguajes de control de acceso consolidados utilizados para facilitar la implementación de las políticas de control de acceso en los sistemas de gestión de identidad y acceso (IAM) se encuentran los siguientes:

– Lenguaje de marcaje de control de acceso extensible (**XACML)**. La norma define un lenguaje declarativo de política de control de acceso (para el modelo ABAC) creado con un lenguaje de marcaje y un modelo de procesamiento que describe cómo evaluar las peticiones de acceso en función de las reglas definidas en la política.

  NOTA 1 – Se adoptó XACML 2.0 como [b-UIT-T X.1142].

  NOTA 2 – Se adoptó XACML 3.0 como [b-UIT-T X.1144].

– Normas para infraestructuras de gestión de privilegios y funciones (**PERMIS)** es un sofisticado sistema de autorización basado en políticas que implementa una versión mejorada de RBAC (similar al ABAC). La política del PERMIS se basa en XML y ofrece una interfaz XAMCL que permite intercambiar indistintamente los puntos de decisión de políticas (PDP) de PERMIS y XACML.

Se recomienda evaluar la aplicabilidad de los modelos de control de acceso en diversos entornos y determinar los requisitos mínimos para su implementación con lenguajes como [b-UIT-T X.1142], [b-UIT-T X.1144] o [b-UKENT PERMIS].

En el Cuadro 1 se incluye un ejemplo de evaluación.

Cuadro 1 – Implementación de modelos de control de acceso en diversos entornos con lenguajes de definición de políticas

Modelo/ Entorno	ACL/ DAC	MAC	RBAC	ABAC	TBAC/ TBAM	PBAC	RAdAC
Centralizado	[b-UIT-T X.1142]; PERMIS	XACML Experimental	[b-UIT-T X.1142]; PERMIS	[b-UIT-T X.1142]; PERMIS*	Experimental	[b-UIT-T X.1142]; PERMIS*	[b-UIT-T X.1142]; PERMIS*
Federado	[b-UIT-T X.1144]; PERMIS	XACML Experimental	[b-UIT-T X.1144]; PERMIS	[b-UIT-T X.1144]; PERMIS*	Experimental	--	[b-UIT-T X.1144]

NOTA 1 – XACMLv2 [b-UIT-T X.1142] y XACMLv3 [b-UIT-T X.1144] están separados pues la "delegación", necesaria en la mayoría de los entornos federados, aparece en XACMLv3.

NOTA 2 – Las implementaciones conocidas de MAC necesitan la extensión XACML.

NOTA 3 – Actualmente, la implementación de TBAC/TBAM necesita la extensión XACML considerada experimental.

NOTA 4 – PBAC por definición solo puede utilizarse en entornos centralizados, en los entornos federados puede ser necesaria la utilización de RAdAC.

NOTA 5 – Cuando figura un asterisco, es decir PERMIS*, en [b-UKENT PERMIS] se indican algunas limitaciones de las implementaciones de ABAC con PERMIS (y de PBAC y RAdAC si se consideran un modelo ABAC extendido).

8.2 Consideraciones sobre la resolución de conflictos de política

El conflicto de política de control de acceso es el resultado de las acciones contradictorias de dos o más reglas de política. Los mecanismos básicos para evitar los conflictos de política es un diseño sin ambigüedades de las reglas de política (*resolución estática de conflicto*). Otro enfoque se basa en la evaluación de las políticas durante el funcionamiento (*resolución dinámica de conflicto*) [b-UKENT PERMIS].

Mientras que la resolución estática de conflictos se considera factible en los sistemas centralizados [b-USB CONFLICT], [b-SPIIRAN POLICY] puede resultar difícil conseguir una resolución estática en un entorno federado dinámico.

Las estrategias básicas de resolución de conflicto son:

– Denegación prioritaria. Se combinan las acciones en conflicto, la acción "denegación" es prioritaria respecto de la acción "permiso".

– Permiso prioritario. Se combinan las acciones en conflicto, la acción "permiso" es prioritaria respecto de la acción "denegación".

– Se aplica la primera. Se ejecuta la primera acción de las reglas en conflicto.

Las estrategias [b-UKENT PERMIS] para la resolución dinámica de conflictos de política contienen algoritmos para la selección de la estrategia estática adecuada en relación con el contexto actual de la petición de acceso.

Se recomienda evaluar las estrategias de resolución de conflictos desde una perspectiva de calidad de funcionamiento y de compatibilidad con los modelos de control de acceso en diversos entornos.

Considerando la evaluación de la calidad de funcionamiento de la resolución *estática* de conflictos de política [b-IJCSIT XACML] junto con el control de acceso dinámico como [b-FUSCAT RADAC], se recomienda minimizar el número de políticas sin reducir el nivel de garantías de seguridad o utilizar unas estrategias de resolución *dinámica* de conflictos de política.

En el Cuadro 2 se incluye un ejemplo de evaluación.

Cuadro 2 – Resolución de conflictos de política para los controles de acceso en diversos entornos

Modelo/ Entorno	ACL/ DAC	MAC	RBAC	ABAC	TBAC/ TBAM	PBACÇ (Nota)	RAdAC
Centralizado	Estática	Estática	Estática	Estática	Estática	Estática	Dinámica
Federado	Dinámica	Dinámica	Dinámica	Dinámica	Dinámica	--	Dinámica
NOTA – PBAC solo es aplicable, por definición, en entornos centralizados.							

8.3 Recomendaciones sobre la evaluación de la calidad de funcionamiento

Aunque los lenguajes de marcaje (como [b-W3C XML], [b-ECMA JSON]) pretenden ser legibles para las personas, la cantidad significativa de reglas de acceso anidadas y avanzadas pueden suponer una difícil tarea para poder describir o corregir políticas implementadas.

Los servicios de compartición de incidentes complejos en las redes de intercambio de incidentes pueden implicar la utilización de modelos avanzados de control de acceso. En el caso del funcionamiento en entornos federados, pueden degradar la calidad de funcionamiento de las redes de intercambio de incidentes y perjudicar la garantía de la seguridad.

Con el fin de evaluar la calidad, el funcionamiento y la conformidad de las políticas, se pueden calcular los valores correspondientes. Los mecanismos de medición de estos valores para las redes de intercambio de incidentes no están en el alcance de esta Recomendación. Sin embargo, se recomienda, [b-KIT PERFIAM] y [b-NIST METRICS], un conjunto de criterios y valores para una evaluación de este tipo:

– **Tiempo de respuesta**. Tiempo de respuesta para los componentes de la infraestructura de gestión de identidad y acceso (IAM), los componentes de compartición de información permiten la evaluación de los valores básicos de la calidad de funcionamiento.

– **Decisiones de control de acceso erróneas**. La evaluación del número de decisiones de autentificación o autorización erróneas en situaciones de esfuerzo da información sobre la robustez de la infraestructura IAM que las soporta.

– **Componentes de confianza**. El control de acceso es una tarea sensible que requiere un cierto nivel de confianza entre las entidades que colaboran. En consecuencia, un valor que determina los componentes de confianza para una decisión de control de acceso es útil para determinar posibles filtraciones de datos.

– **Distribución de política**. Se utiliza para evaluar la capacidad y el funcionamiento de la distribución de la política en los sistemas centralizados o federados de control de acceso.

– **Facilidad de asignación de privilegios**. Determina el número de etapas necesarias para asignar, cambiar, suprimir y heredar capacidades de un sujeto o grupo.

– **Calidad de expresión de la política**. Determina si el control de acceso puede definirse con expresiones lógicas y programables.

– **Capacidades de delegación**. Determina si el sistema de control de acceso es capaz de delegar privilegios a los sujetos.

– **Combinación y resolución de la política**. Determina las estrategias de combinación utilizadas para la resolución de conflictos (en caso de producirse) de la política.

– **Bypass**. Determina si algún componente elude las políticas de control de acceso.

– **Protección**. Determina las capacidades de aseguramiento de la protección tales como las limitaciones de las reglas de control de acceso con el fin de evitar el aumento de privilegios.
– **Granularidad**. Determina el nivel de granularidad que puede controlar un sistema de control de acceso. Podría reflejar un conjunto de atributos de sujetos evaluados durante un proceso de control de acceso.
– **Integración con la autentificación**. Determina si un sistema de control de acceso es capaz de integrarse con los sistemas de autentificación.

Bibliografía

[b-UIT-T M.3345] Recomendación UIT-T M.3345 (2009), *Principios para la autogestión del servicio*.

[b-UIT-T M.3410] Recomendación UIT-T M.3410 (2008), *Directrices y requisitos para los sistemas de gestión de la seguridad para el soporte de la gestión de telecomunicaciones*.

[b-UIT-T X.1036] Recomendación UIT-T X.1036 (2007), *Marco para la creación, almacenamiento, distribución y aplicación de políticas de seguridad de red.*

[b-UIT-T X.1142] Recomendación UIT-T X.1142 (2006), *Lenguaje de marcaje de control de acceso extensible (XACML 2.0).*

[b-UIT-T X.1144] Recomendación UIT-T X.1144 (2013), *Lenguaje de marcaje de control de acceso extensible (XACML) 3.0.*

[b-UIT-T X.1252] Recomendación UIT-T X.1252 (2010), *Términos y definiciones sobre gestión de identidad de referencia.*

[b-UIT-T X.1541] Recomendación UIT-T X.1541 (2012), *Formato para el intercambio de descripciones de objetos de incidentes.*

[b-UIT-T X.1580] Recomendación UIT-T X.1580 (2012*), Defensa entre redes en tiempo real*.

[b-UIT-T X.1581] Recomendación UIT-T X.1581 (2012), *Transporte de mensajes de defensa entre redes en tiempo real*.

[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)*.

SERIES DE RECOMENDACIONES DEL UIT-T

Serie A	Organización del trabajo del UIT-T
Serie D	Principios de tarificación y contabilidad y cuestiones económicas y políticas de las telecomunicaciones/TIC internacionales
Serie E	Explotación general de la red, servicio telefónico, explotación del servicio y factores humanos
Serie F	Servicios de telecomunicación no telefónicos
Serie G	Sistemas y medios de transmisión, sistemas y redes digitales
Serie H	Sistemas audiovisuales y multimedia
Serie I	Red digital de servicios integrados
Serie J	Redes de cable y transmisión de programas radiofónicos y televisivos, y de otras señales multimedia
Serie K	Protección contra las interferencias
Serie L	Medio ambiente y TIC, cambio climático, ciberdesechos, eficiencia energética, construcción, instalación y protección de los cables y demás elementos de planta exterior
Serie M	Gestión de las telecomunicaciones, incluida la RGT y el mantenimiento de redes
Serie N	Mantenimiento: circuitos internacionales para transmisiones radiofónicas y de televisión
Serie O	Especificaciones de los aparatos de medida
Serie P	Calidad de la transmisión telefónica, instalaciones telefónicas y redes de líneas locales
Serie Q	Conmutación y señalización, y mediciones y pruebas asociadas
Serie R	Transmisión telegráfica
Serie S	Equipos terminales para servicios de telegrafía
Serie T	Terminales para servicios de telemática
Serie U	Conmutación telegráfica
Serie V	Comunicación de datos por la red telefónica
Serie X	**Redes de datos, comunicaciones de sistemas abiertos y seguridad**
Serie Y	Infraestructura mundial de la información, aspectos del protocolo Internet, redes de próxima generación, Internet de las cosas y ciudades inteligentes
Serie Z	Lenguajes y aspectos generales de soporte lógico para sistemas de telecomunicación

Impreso en Suiza
Ginebra, 2017