国 际 电 信 联 盟

ITU-T X.1550

(03/2017)

国际电信联盟
电信标准化部门

X系列：数据网、开放系统通信和安全性

网络安全信息交流 – 策略的交换

事件交换网络的访问控制模型

ITU-T X.1550 建议书

国际电信联盟

ITU-T X系列建议书

数据网、开放系统通信和安全性

公用数据网	X.1–X.199
开放系统互连	X.200–X.299
网间互通	X.300–X.399
报文处理系统	X.400–X.499
号码簿	X.500–X.599
OSI组网和系统概貌	X.600–X.699
OSI管理	X.700–X.799
安全	X.800–X.849
OSI应用	X.850–X.899
开放分布式处理	X.900–X.999
信息和网络安全	
一般安全问题	X.1000–X.1029
网络安全	X.1030–X.1049
安全管理	X.1050–X.1069
远程生物特征测定	X.1080–X.1099
安全应用和服务	
组播安全	X.1100–X.1109
家庭网络安全	X.1110–X.1119
移动安全	X.1120–X.1139
网页安全	X.1140–X.1149
安全协议	X.1150–X.1159
对等网络安全	X.1160–X.1169
网络身份安全	X.1170–X.1179
IPTV安全	X.1180–X.1199
网络空间安全	
网络安全	X.1200–X.1229
反垃圾信息	X.1230–X.1249
身份管理	X.1250–X.1279
安全应用和服务	
应急通信	X.1300–X.1309
泛在传感器网络安全	X.1310–X.1339
PKI相关建议书	X.1340–X.1349
网络安全信息交换	
网络安全概述	X.1500–X.1519
脆弱性/状态信息交换	X.1520–X.1539
事件/事故/探索法信息交换	X.1540–X.1549
策略的交换	**X.1550–X.1559**
探索法和信息请求	X.1560–X.1569
标识和发现	X.1570–X.1579
确保交换	X.1580–X.1589
云计算安全	
云计算安全概述	X.1600–X.1601
云计算安全设计	X.1602–X.1639
云计算安全最佳做法和导则	X.1640–X.1659
云计算安全的落实工作	X.1660–X.1679
其他云计算安全问题	X.1680–X.1699

欲了解更详细信息，请查阅ITU-T建议书目录。

ITU-T X.1550 建议书

事件交换网络的访问控制模型

摘要

ITU-T X.1550建议书介绍了实施事件交换网访问控制策略的现有方法。本建议书阐述了各种十分成熟的访问控制模型，分享了事件交换网性能评估的模型和标准。本文考虑到将基于标准的方案，用于在不同网络安全信息内部和在不同的信息环境下推进落实不同的访问控制模型。

沿革

版本	建议书	批准日期	研究组	唯一识别码*
1.0	ITU-T X.1550	2017-03-30	17	11.1002/1000/13198

关键词

访问控制、授权、计算应急响应团队（CERT）、计算机安全事件响应团队（CSIRT）、网络安全信息交流（CYBEX）、身份和接入管理（IAM）、事件交换网、事件响应。

* 欲查阅建议书，请在您的网络浏览器地址域键入URL http://handle.itu.int/，随后输入建议书的唯一识别码，例如，http://handle.itu.int/11.1002/1000/11830-en。

前言

国际电信联盟（ITU）是从事电信领域工作的联合国专门机构。ITU-T（国际电信联盟电信标准化部门）是国际电信联盟的常设机构，负责研究技术、操作和资费问题，并且为在世界范围内实现电信标准化，发表有关上述研究项目的建议书。

每四年一届的世界电信标准化全会（WTSA）确定ITU-T各研究组的研究课题，再由各研究组制定有关这些课题的建议书。

WTSA第1号决议规定了批准建议书须遵循的程序。

属ITU-T研究范围的某些信息技术领域的必要标准，是与国际标准化组织（ISO）和国际电工技术委员会（IEC）合作制定的。

注

本建议书为简明扼要起见而使用的“主管部门”一词，既指电信主管部门，又指经认可的运营机构。

遵守本建议书的规定是以自愿为基础的，但建议书可能包含某些强制性条款（以确保例如互操作性或适用性等），只有满足所有强制性条款的规定，才能达到遵守建议书的目的。“应该”或“必须”等其它一些强制性用语及其否定形式被用于表达特定要求。使用此类用语不表示要求任何一方遵守本建议书。

知识产权

国际电联提请注意：本建议书的应用或实施可能涉及使用已申报的知识产权。国际电联对无论是其成员还是建议书制定程序之外的其它机构提出的有关已申报的知识产权的证据、有效性或适用性不表示意见。

至本建议书批准之日止，国际电联尚未收到实施本建议书可能需要的受专利保护的知识产权的通知。但需要提醒实施者注意的是，这可能并非最新信息，因此特大力提倡他们通过下列网址查询电信标准化局（TSB）的专利数据库：http://www.itu.int/ITU-T/ipr/。

目录

ITU-T X.1550 建议书

事件交换网络的访问控制模型

1 范围

本建议书介绍了实施事件交换网访问控制策略的现有方法。本建议书阐述了各种十分成熟的访问控制模型，分享了事件交换网性能评估的模型和标准。本文考虑到将基于标准的方案，用于在不同网络安全信息内部和在不同的信息环境下推进落实不同的访问控制模型。

2 参考文献

参考文献下列ITU-T建议书和其他参考文献的条款，通过在本建议书中的引用而构成本建议书的条款。在出版时，所指出的版本是有效的。所有的建议书和其他参考文献都面临修订，使用本建议书的各方应探讨使用下列建议书和其他参考文献最新版本的可能性。当前有效的ITU-T建议书清单定期出版。

本建议书中引用某个独立文件，并非确定该文件具备建议书的地位。

[ITU-T X.1500] ITU-T X.1500 (2011)建议书 – 网络安全信息交换概述。

[ITU-T X.1570] ITU-T X.1570 (2011)建议书 – 网络安全信息交换中的发现机制。

3 定义

3.1 他处定义的术语

本建议书采用了下列其它资料定义的术语：

3.1.1 访问控制[b-ITU-T X.1252]：用来确定一实体是否应按照预先确定的规则和请求方的具体权利或相关授权被授予获得资源、设施、服务或信息的程序。

3.1.2 授权[b-ITU-T M.3345]：该功能阐述了自我服务管理行动方如何以及在何条件下能够使用自我服务功能或允许他们采取何种自我服务操作。

3.1.3 事件交换[ITU-T X.1570]：两个或两个以上网络安全实体之间网络安全信息的传送，该传送可为单向、双向或多向传送，即多个至多个实体的传送。

注–在本建议书中，“事件交换”视为等同于“交换”。

3.1.4 可信域[b-ITU-T M.3410]：由用户、网络、数据库和使用数据库中数据的应用组成的一系列信息及相关资源。不同的可信域可能共同相同的物理组件。此外，单一可信域可应用不同的信任等级，划分的标准取决于用户有必要了解的信息以及信息和相关资源的敏感性。

3.2 本建议书定义的术语

本建议书定义下列术语：

3.2.1 访问控制策略冲突[b-ITU-T X.1036]：该功能定义了两种原则相互冲突的操作。实施策略的实体将无法判定执行什么操作。

注：该定义基于[b-ITU-T X.1036]中给出的“策略冲突”定义。

3.2.2 动态策略冲突解决方案：在运行阶段应用的冲突解决策略。

3.2.3 事件交换网络：在集中式或联盟式管理的基础上实现网络安全信息交流（CYBEX）操作基础设施的通用化。

3.2.4 事件信息：网络安全信息、结构化的信息或有关事故或事件取证的信息子集。

注–本定义基于[b-ITU-T X.1570]中有关“（网络安全信息）交换”的说明。

3.2.5 静态策略冲突解决方案：在设计阶段应用的冲突解决策略。

4 缩写词和首字母缩略语

ABAC	Attribute Based Access Control	基于属性的访问控制
ACL	Access Control List	访问控制清单
CERT	Computer Emergency Response Team	计算应急响应团队
CSIRT	Computer Security Incident Response Team	计算机安全事件响应团队
CYBEX	CYBersecurity information EXchange	网络安全信息交流
DAC	Discretionary Access Control	随意性访问控制
IAM	Identity and Access Management	身份和访问管理
IODEF	Incident Object Description Exchange Format	事件对象说明交换格式
IT	Information Technology	信息技术
MAC	Mandatory Access Control	强制访问控制
PBAC	Policy Based Access Control	基于策略的访问控制
PDP	Policy Decision Point	策略决定点
PERMIS	PrivilEge and Role Management Infrastructure Standards	优先权和职责管理的基础设施标准
RAdAC	Risk-Adaptive Access Control	风险自适应访问控制
RBAC	Role Based Access Control	基于职责的访问控制
RID	Real-time Inter-network Defense	实时网络间的防卫
RIDT	Real-time Inter-network Defense Transport	实时网络间的防卫传输
STIX	Structured Threat Information Expression	结构化威胁信息的表达
TAXII	Trusted Automated Exchange of Indicator Information	可信自动指示信息交换
TBAC	Task Based Access Control	基于任务的访问控制
TBAM	Task Based Access Management	基于任务的接入管理
XACML	eXtensible Access Control Markup Language	可扩展访问控制标识语言

XML eXtended Markup Language 可扩展标识语言

5 惯例

在本建议书中，“访问控制”被视作支持授权程序的一般机制。

6 概述

为降低缓解计算受攻击风险并在组织/协作或业务/系统内部提供安全保障，可能需要采取风险缓解措施。事件交换网负责防止或降低与计算机攻击相关的风险。网络安全事件交换实践引入了在集中或联盟式环境下使用的各类信息分享模型。事件信息共享是基于与相关风险关联的信任的水平，并需确保不会不当分享保密或敏感信息。这使一些访问控制模型在性能、实施和安全保障方面更加有效。

全球信息系统的使用的总体发展和共同集成推动授权进程所依赖的高级访问控制模型得以发展。现有访问控制策略语言，会促进部署安全策略并对不同访问控制模型和操作环境提出挑战。

本建议书阐述的机制和方法或可作为提供访问控制策略的属性，用于底层网络安全信息交流（CYBEX）格式以及下述传输协议：事件对象说明交换格式(IODEF) [b-ITU-T X.1541]、实时网络间防卫(RID) [b-ITU-T X.1580] + 实时网络间防卫传输(RIDT) [b-ITU-T X.1581]、结构化威胁信息表达(STIX) [b-stix] + 可信自动指示信息交换(TAXII) [b-taxii]等。

7 事件交换网分类

7.1 操作环境

事件交换网在下述环境内进行操作：

– 单一可信域（集中管理）；

– 联盟式可信域（分散管理）。

7.2 事件信息交换模型

事件信息交换模型的表达如下：

– “对等”，两参与方的单向或双向信息交换。

– “星形拓扑”。此类模型通常拥有一个中心枢纽用于从参与方（即辐射轴）接收数据。中心枢纽既可以直接将来向数据重新分配给其它成员，也可提供增值服务并将新（假设更为有用）的数据发给成员。在这种方法中，枢纽是作为清算中心，在保护成员身份的同时促进信息共享。与此相关的挑战是在这种模型中共享信息需要对枢纽有高度信任[b-MITRE模型]。

– “向全体发送”。这种模型支持所有参与方与全体成员分享信息，而无需经过中心枢纽。由于成员相互间可直接共享信息，因此信息传播很快且很容易与多个参与方形成匹配[b-MITRE模型]。

基于上述三种模型，可建立以下面向服务的模型：

– “发现-请求-响应”。这是一种两阶段模型，第一阶段（可选）的发现机制[ITU-T X.1570]须用于确定与事件相关的集中或分布源。在第二阶段，消费者通过查询数据库获取信息，并依据访问控制模型给出回复决定。

– “发现-签约-通知”。这是一种两阶段模型，第一阶段（可选）的发现机制[ITU-T X.1570]用于确定与事件相关的集中或分布源。在第二阶段，消费者通过签约并以通知的形式接收选定源的信息来获取数据。

7.3 访问控制模型

访问控制模型是安全策略的基础。实际上，这些策略利用特定的扩展标识语言（XML）– 方言（访问控制策略语言）形成正式的策略。

根据[b-NIST Models]，下文介绍了从保守模型（考虑更少的粒度）至自适应模型（考虑粒度更大且依赖环境的策略）的下述访问控制模型：

– **ACL/DAC**。访问控制清单（ACL）/随意访问控制 （DAC）概念是指，方向需得到控制的某系统的各项资源（称之为对象）均拥有自己的映射清单，其映射存在于要求访问资源的实体与各实体可对资源采取的一系列行动之间。

– **MAC**。强制访问控制 （MAC）常用于数据保密性优先级最高的系统。MAC的工作是将分类标签分配给各文件资源。分类包括信息的类别和敏感度水平，例如，秘密、机密或最高机密。每个对象均分配有一个类别，这里称之为级别。当某对象试图访问特定资源时，系统将检查对象的权限并判定是否允许访问，同时将对象的级别与资源分类进行比对。

– **RBAC**。判定基于职责的访问控制 （RBAC）是否可访问某一资源，是根据请求者与控制相关资源的组织或其所有人之间的关系；请求者的职责或职能将决定其访问请求会得到批准还是遭到拒绝。

– **TBAC/TBAM**。基于任务的访问控制 （TBAC）/基于任务的接入管理 （TBAM） [b-IEEE TBAC] 是RBAC的扩展，它是基于允许访问控制拥有更小粒度的商业任务定义。

– **ABAC**。基于属性的访问控制 （ABAC）模型采用ACL等机制，其中包含对象的属性及允许对相关资源执行的操作。当与ACL中的属性相同时，对象便有权对资源执行ACL为该属性指配的操作。

– **PBAC**。基于策略的访问控制 （PBAC）是一种企业级ABAC模型的统一化和标准化，其目的是为特定管理目标提供支持。PBAC组合了来自资源、环境和请求者的属性以及访问申请所在特定环境的信息，同时使用在这种情况下，根据组织的属性策略，是否允许访问做出具体规定的规则集合。

– **RAdAC**。风险自适应访问控制（RAdAC）模型的制造实现了实时、自适应、具备风险意识的访问控制。该方法通过在访问控制决议流程中引入环境条件和风险水平，对其它早期访问控制模型进行了拓展。这一做法综合了个人（或设备）可信度、公司信息技术 （IT） 基础设施和环境风险因素方面的信息，并将所有这些信息用于打造总体可量化的风险标准。RAdAC亦将背景因素作为决策进程的输入内容。这些背景输入信息可能包含从计算应急响应团队（CERT）（计算安全事件响应团队，CSIRT）等其它来源所采集数据基础之上得出的某组织当前面临的威胁水平（见[b-IEEE ARES]、[b-NIST RADAC]。）

7.4 信任水平

为强调信任水平与风险之间的相关度，建议在事件交换网络内使用下述标准量化信任的级别：**低、中、高**。我们可判断出信任水平越高，访问控制的要求和粒度越简单。换言之，信任水平直接影响访问控制机制的复杂度。

定性和定量评估信任水平的技术不在本建议书的讨论范围之内。

本文考虑了信任水平与共享模型之间的下述相关性：

– “向全体发送”模型通常需要参与方之间具有**高**信任度。

– “星形拓扑”模型通常需要高或中等水平的信任（因为“枢纽”可能会筛选信息）。

– “对等”模型，通常不需要高信任度，因为单一的通信信道可能采取各类方法控制。

高水平的共用模型并未明确表示要依赖于信任的程度，但在环境更复杂且参与方数量不断增多的情况下，这些模型可能需要更加高级的访问控制模型。

因此，如图1所示，考虑使用下述分类：

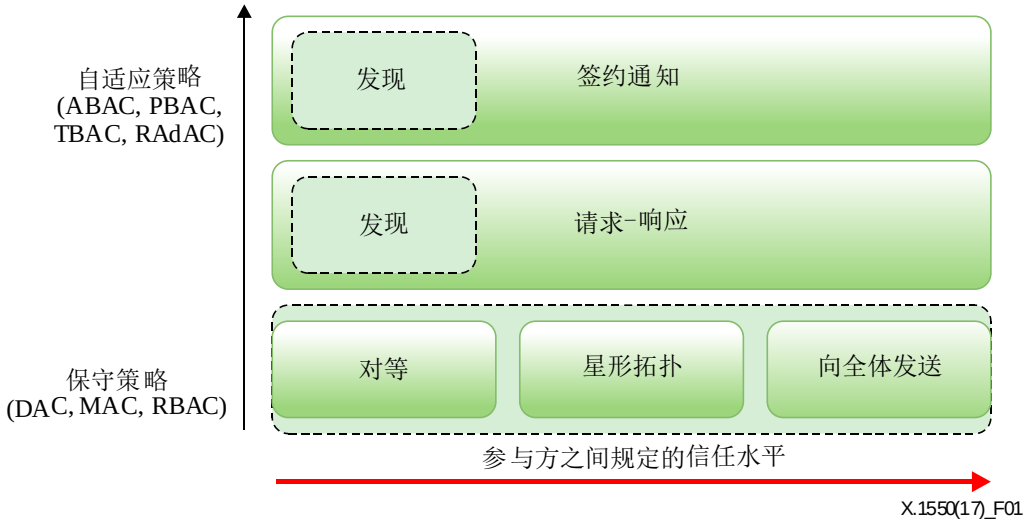

图1 – 访问控制模型、共用模型和信任水平分类

8 有助于落实访问控制策略的技术

8.1 评估策略表述语言的建议书

用于推进身份和接入管理（IAM）系统内访问控制策略技术落实的成熟访问控制语言包括：

– 可扩展访问控制标识语言 – **XACML**。此标准定义了标识语言中所用的断言访问控制策略语言（针对ABAC模型），以及阐述如何根据策略定义的规则评估接入请求的处理模型。

注 1 – XACML 2.0已作为[b-ITU-T X.1142]获得通过。

注 2 – XACML 3.0已作为[b-ITU-T X.1144]获得通过。

– 优先权和职责管理基础设施标准（**PERMIS**）是一种先进的基于策略的授权系统，该系统使用更高版本的RBAC（与ABAC类似）。PERMIS策略是基于XML，其提供的XACML接口允许PERMIS和XACML策略决定点（PDP）无缝交换。

建议在各种环境下评估访问控制模型的适用性，并判定其与[b-ITU-T X.1142]、[b-ITU-T X.1144]或[b-UKENT PERMIS]等策略语言共同实施的最低要求。

示例评估见表1：

表 1 – 在策略定义语言的不同环境下实施访问控制模型

模型/环境	ACL/ DAC	MAC	RBAC	ABAC	TBAC/ TBAM	PBAC	RAdAC
集中	[b-ITU-T X.1142]; PERMIS	试验XACML	[b-ITU-T X.1142]; PERMIS	[b-ITU-T X.1142]; PERMIS*	试验	[b-ITU-T X.1142]; PERMIS*	[b-ITU-T X.1142]; PERMIS*
联盟	[b-ITU-T X.1144]; PERMIS	试验XACML	[b-ITU-T X.1144]; PERMIS	[b-ITU-T X.1144]; PERMIS*	试验	–	[b-ITU-T X.1144]

注1 – XACMLv2 [b-ITU-T X.1142]和XACMLv3 [b-ITU-T X.1144]自“下放”之后便分离，大多数联盟环境均需要，且出现在XACMLv3中。

注2 – 已知MAC的实施需要XACML扩展。

注3 – 当前试验性的TBAC/TBAM实施需要XACML扩展。

注4 – 根据定义，PBAC仅适用于集中环境，联盟环境可能要使用RAdAC。

注5 – 当包含星号时（即PERMIS*），PERMIS实施ABAC（如被视作ABAC模型的扩展，则还包括PBAC和RAdAC）的部分限制请参见[b-UKENT PERMIS]。

8.2 有关的策略冲突解决方案

访问控制策略冲突会造成两种或多种策略规则采取互相冲突的行动。缓解策略冲突的基本机制是制定明确的策略规则设计（*静态冲突解决*）。另一种方法是基于运行时间策略评估（*动态冲突解决*）[b-UKENT PERMIS]。

在静态冲突解决方案适用于集中系统[b-USB冲突]、[b-SPIIRAN 策略]的同时，在动态联盟环境中实现静态解决方案可能存在挑战。

基本静态冲突解决策略的特点：

– Deny-override。冲突的规则得到合并，倾向于采用“拒绝”操作而非“允许”；

– Permit-override。冲突的规则得到合并，倾向于采用“允许”操作而非“拒绝”；

– First-applicable。冲突规则中出现的第一种操作得到执行。

策略[b-UKENT PERMIS]，为选择与当前访问请求背景相对应的适当静态策略而制定的动态策略冲突解决特征算法。

建议从各种环境访问控制模型的性能与兼容性的角度，对冲突解决策略做出评估。

考虑到静态策略冲突解决方案[b- IJCSIT XACML]与动态访问控制（例如[b-FUSCAT RADAC]）结合的评估，建议尽量减少策略的数量，但又不破坏安全保障的水平或使用动态策略冲突解决策略。

评估示例请见表2：

表2 – 各种环境下访问控制模型的策略冲突解决方案

模型/环境	ACL/ DAC	MAC	RBAC	ABAC	TBAC/ TBAM	PBAC	RAdAC
集中式	静态	静态	静态	静态	静态	静态	动态
联盟式	动态	动态	动态	动态	动态	–	动态
注 – 根据定义PBAC仅适用于集中式的环境。							

8.3 有关性能评估的建议书

尽管标识语言（例如[b-W3C XML]、[b-ECMA JSON]）旨在能让人类读懂，但大量嵌套和高级的访问规则可能给实施策略的剖析与调试提出挑战。

事件交换网络中的复杂事件共享业务可能意味着使用了高级的访问控制模型。考虑到在联盟环境下的操作，这一做法可能会降低事件交换网络的性能，从而带来安全保障问题。

为了评估策略的质量/性能/一致性，可能会计算相应的指标。事件交换网络此类指标的评估不属于本建议书的研究范围。但是，[b-KIT PERFIAM]和[b-NIST METRICS]就此类评估的系列标准与指标提出了建议：

– **响应时间。**IAM基础设施组件和信息共享组件的响应时间支持对基本性能指标做出评估。

– **错误的访问控制决定。**评估在紧张情况下错误鉴权或授权的数量，给出了底层IAM架构的强健性。

– **可信组件。**访问控制是一项敏感的任务，需要合作实体间有一定的信任水平。因此，列出访问控制决定可信组件的指标有助于判定可能出现的数据泄露。

– **策略分配。**用于评估集中式或联盟式访问控制系统策略分配的能力与性能。

– **权限指配便利水平。**确定指配/改变/删除/继承某对象或群组的能力所需要的步骤。

– **策略表达的质量。**判定是否可通过逻辑和可编程的表达式实施访问控制。

– **放权能力。**确定访问控制系统是否有能力给某些对象下放权限。

– **策略组合与解决方案。**判定是否使用策略组合来解决冲突（如有）。
– **旁路。**判定任何组件是否要忽略访问控制策略。
– **安全。**判定用于防止权利上交等访问控制限制方面的安全执行能力。
– **粒度。**判定某访问控制系统能控制的粒度水平。这能够反映访问控制过程中评估的一批对象的属性。
– **鉴权集成。**判定访问控制系统是否能与鉴权系统集成。

参考资料

[b-ITU-T M.3345] ITU-T M.3345 (2009) 建议书，自助管理原则

[b-ITU-T M.3410] ITU-T M.3410 (2008) 建议书，支持电信管理的安全管理系统指南与要求

[b-ITU-T X.1036] ITU-T X.1036 (2007) 建议书，网络安全政策的制定、存储、发布和充实框架

[b-ITU-T X.1142] ITU-T X.1142 (2006) 建议书，可扩展访问控制标识语言(XACML 2.0)

[b-ITU-T X.1144] ITU-T X.1144 (2013) 建议书，可扩展访问控制标识语言(XACML 3.0)

[b-ITU-T X.1252] ITU-T X.1252 (2010) 建议书，基线身份管理的术语和定义

[b-ITU-T X.1541] ITU-T X.1541 (2012) 建议书，事件对象描述交换格式

[b-ITU-T X.1580] ITU-T X.1580 (2012) 建议书，实时网间防御

[b-ITU-T X.1581] ITU-T X.1581 (2012) 建议书，实时网际防御讯息的传输

[b-IEEE TBAC] IEEE IET 软件(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).

ITU-T 建议书系列

系列A	ITU-T工作的组织
系列D	资费及结算原则和国际电信/ICT的经济和政策问题
系列E	综合网络运行、电话业务、业务运行和人为因素
系列F	非话电信业务
系列G	传输系统和媒介、数字系统和网络
系列H	视听及多媒体系统
系列I	综合业务数字网
系列J	有线网络和电视、声音节目及其他多媒体信号的传输
系列K	干扰的防护
系列L	环境与ICT、气候变化、电子废物、节能；线缆和外部设备的其他组件的建设、安装和保护
系列M	电信管理，包括TMN和网络维护
系列N	维护：国际声音节目和电视传输电路
系列O	测量设备的技术规范
系列P	电话传输质量、电话设施及本地线路网络
系列Q	交换和信令
系列R	电报传输
系列S	电报业务终端设备
系列T	远程信息处理业务的终端设备
系列U	电报交换
系列V	电话网上的数据通信
系列X	**数据网、开放系统通信和安全性**
系列Y	全球信息基础设施、互联网协议问题、下一代网络、物联网和智慧城市
系列Z	用于电信系统的语言和一般软件问题

瑞士印刷
2018年，日内瓦