SDN. 801：

访问控制原理与机制

SDN. 801: Access Control Concept and Mechanisms

黄术群 译
林望重 校

国防科技保密通信重点实验室

目 录

1 引 言

本文论述实现访问控制(AC)的概念、工具和机理,以便全面理解MISSI [多级信息系统安全(倡议)]的访问控制。本文也作为在MISSI组件中实现访问控制特性的指南。本文从介绍访问控制的一般原理入手,介绍关于访问控制的工具、机理及将它们应用于现实世界通信系统的进程的更详细的知识。单个协议文本提供了本文所讨论的完成这些"工具和机理"所必需的特定进程的细节,当实现MISSI组件时,请参考1.3节的文献[7,8,10]的最新版本。

1.1 结构

本文由六个部分组成,这些章节既采用通用的格式,又采用MISSI组件的格式来讨论访问控制,每一部分的写法也不一样。因此,从通用的和MISSI的角度对访问控制进行了详细的叙述。

第一节包括了前几节出现的术语的缩写和定义,同时给出了进一步阅读的参考资料。

第二节给出了访问控制的概貌,包括描述应用MISSI的AC组件的环境和通用的访问控制系统的一般先决条件和管理要求,以及用于各种访问控制系统的一般机制。

第三节讲的是MISSI访问控制的要求和目标。

第四节描述常用的实现访问控制的工具,这些工具被用来满足第三节定义的MISSI访问控制的要求和目标。

第五节详细阐述了MISSI的访问控制机理的实现方法,这一节还叙述了如何运用第四节提到的工具来实现MISSI的访问期间控制,以满足第三节描述的要求和目标。

第六节详细叙述了实现访问控制的专用的信息处理要求，还包含了为在存储—转发环境中实现访问控制的处理指令。

附录 A 描述了通用服务(GENSER)安全策略，它是安全策略定义的内容和格式的一个例子。

1.2 缩写词

AA	属性机构 /授权机构(Attribute Authority / Authorization Administrator)
AC	属性证书
ACI	访问控制信息
ACL	访问控制表
ADF	访问控制判定函数
AEF	访问控制实施函数
CA	证书机构
CMB	信息担保配置管理局
COMSEC	通讯安全
CRL	无效证书表
DAC	随意访问控制
DMS	国防文电系统
DN	识别名称
IBAC	基于身份的访问控制
ID	标识符
ICRL	间接无效证书表
ISO	国际标准化组织
KEA	密钥交换算法
LIF	LRBAC 信息文件
LMA	本地管理机构

LRBAC	基于本地规则的访问控制
MAC	强制性访问控制
MISSI	多级信息系统安全倡议
MMP	MISSI 管理协议
MSP	文电安全协议
OID	目标标识符
OPI	主要权利局(Office of Primary Interest)
OSI	开放系统互连
PCA	决策形成机构
PDU	协议数据单元
PRBAC	基于分区原则的访问控制
RBAC	基于规则的访问控制
SAA	辅助属性机构
SDA	安全域机构
SPIF	安全策略信息文件
SSL	标准的安全标签
UA	用户代理

1.3 参考文献

[1] 略(原文如此,下同)

[2] 略

[3] W. Ford, Computer Communication Security : Principles , Standard Protocols and Techniques , PTR Prentice Hall , Englewood Cliffs, NJ, 1994.

[4] ISO/IEC 9594: Information Technology – Open System Interconnection – The Directory(Also ITU – T Recommendation X. 500).

[5] ITU – T Recommendation X. 509(06/97), Information Tech-

nology – Open System Interconnection – The Directory: Authentication Framework.

[6] MCCB – 04.02.013, ON636203, SDN.700, Registration Procedures for Technical Objects (INFOSEC Arc), Revision 1 of Product Baseline, 970207.

[7] SDN.701, Message Security Protocol 4.0, Revision A, 1997 – 02 – 06.

[8] 4 – 023, ON636206, SDN.702: Abstract Syntax for MCCB – 0 Utilization with Common Security Protocol (CSP), Version 3 X.509 Certificates and Version 2 Certificate Revocation Lists, Revision C 12 May, 1999.

[9] (略)

[10] MCCB – 04.02.028, ON636207, SDN.706, X.509 Certificate and Certificate Revocation List Profiles and Certificate Path Processing Rules for MISSI, Revision D, 12 May, 1999.

[11] Allied Communication Publication (ACP) 123, Common Messaging Strategy and Procedures, November 1994.

[12] DoD 5200.1 – HF, DoD Guide to Marking Classified Documents, September 1996.

[13] ACP 120, Common Security, Protocol October 1997.

[14] Recommendation X.411, Message Handling Systems – Message Transfer System: Abstract Service Definition and Procedures, September 1992.

1.4 定义

下列定义包括由ISO(国际标准化组织)提出的适用于MISSI的术语,以及在MISSI AC中提出的术语。这些定义以ISO/IEC 10181系统

为基础，该系统提供了国际上公认的访问控制的相关术语的定义，对ISO提出的术语做了标记。

访问控制判定函数(ADF)(Access Control Decision Function)——一种通过把访问控制策略应用于控制请求从而做出访问控制决定的专用函数。

访问控制实施函数(AEF)(Access Control Enforcement Function)——一种专用函数，它是每次访问请求时访问者和目标之间访问路径的一部分，同时该函数也执行由ADF作出的决定。

访问控制信息(ACI)(Access Control Information)——用于访问控制目的的所有信息，包括上下文的信息(ISO)。

访问控制策略(Access Control Policy)——定义可进行访问的条件的一组规则。

访问控制策略机构(Access Control Policy Authority)——负责制定访问一个或一类目标的策略(访问策略)的机构(即安全机构)。

授权(Authorization)——传递访问者特权的ACI。

授权机构(AA)(Authorization Administrator)——根据访问控制策略采用一种特殊机制对访问者的授权活动进行传递和约束(即限定访问者的ACI)的安全域机构。

访问者(Initiator)——打算访问其它实体的实体(基于计算机功能或进程)(ISO)。

限定访问者的访问控制信息(Initiator-Bound Access Control Information)——限定访问者的ACI(即授权书)(ISO)。

对象(Object)——一种任何形式的资源，包括数据库、数据库的特定项目、主机、进程和加密的E-mail文电等。

分区(Partition)——共用同一种安全策略的能通过通信系统联系的一组实体。一个分区可再分成被称为利益通信的子区。

允许授权(Permissive Authorization)——满足允许敏感度的授权。

允许敏感度(Permissive Sensitivity)—— 一种敏感度,在该敏感度上,如果一个访问者有一组或多组相关的允许权,将部分满足访问控制判定函数。

受限授权(Restrictive Authorization)—— 满足受限敏感度的授权。

受限敏感度(Restrictive Sensitivity)—— 一种敏感性,在该敏感度上,一个访问者只有具备所有相关的受限授权,才部分满足访问控制判定函数。

安全机构(Security Authority)—— 负责定义、完善或实施安全策略的实体。(ISO)

安全域(Security Domain)—— 一组安全机构和一组相关的安全活动,在这些活动中,各成员都遵从由安全机构为专门的活动所规定的安全策略(即访问域)。(ISO)

安全域管理机构(Security Domain Authority(SDA))—— 负责为一个安全域完善安全决策的安全管理机构。

安全策略(Security Authority)—— 一组用来提供安全服务的准则。(ISO)

敏感度(Sensitivity)—— 传递由目标主人施加于一个或一类目标的专门的独立的访问控制条件的访问控制信息。目标的敏感度对应于访问者的授权。

目标(Target)—— 可以被访问的实体(对象)。(ISO)

限定目标的访控制信息(Target - bound Access Control Information)—— 限定目标的访问控制信息。(SIO)

目标管理员(Target Custodian)—— 维持对一个目标的物理控制并执行 ADF 和 AEF 函数的功能的实体。

目标主人(Target owner)—— 确定和限定一个目标的敏感度的安全域机构。

2 概述

授权是给系统用户授予访问系统资源的权力或特权的行为。访问控制是实现授权的一种方式。下面的章节提供一个关于实现 MISSI 专门访问控制系统的原理、方法和机理的高水平的论述。

2.1 环境

用来提供通信系统安全的 MISSI 专门的组件的运行环境如图 2-1 所示:

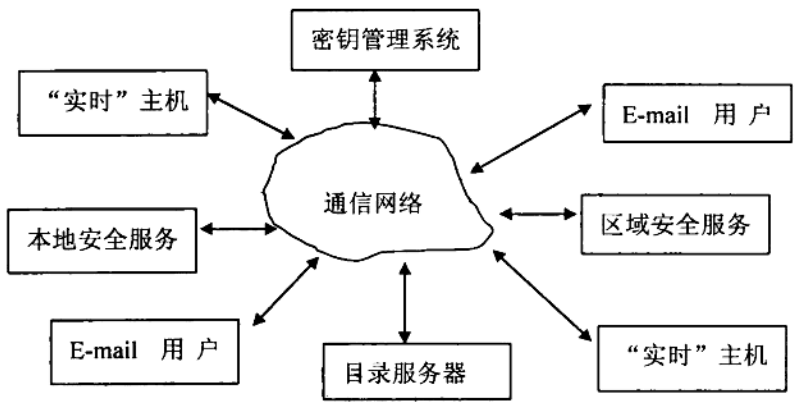

图 2-1 最普通的通信环镜

上图表示联系全球的通信网络,“公共的通信网络”代表通信媒体(如因特网)的结构组合。这个通信网络可以是多种形式的通信实体,如:参与网络活动的所有的访问者、对象和目标。这些实体包括实时用户,如全球网(WWW)主机;一对通过存储-转发机制通信的实体,如 E-mail 用户;还包括网络支撑,如保护局域网或宽域网的防火墙或网关设备。

在通信系统中增加安全装置以保护各种局域网和宽域网中的信息的同时也引入了新的实体,这些实体包括目录服务器,完成本地和区域

基本访问控制，以及对称密钥的管理的安全服务。在通信系统中把这些实体连接在一起时，就需要研制一种访问控制系统。那些强制连接在通信系统中的实体之间执行合适的访问控制策略的机理定义了MISSI访问控制。通常应当注意，在这个系统中，所描述的应用通信机理的元素有多种情况。

2.2 访问者(Initiators)、对象(Objects)和目标(Targets)

访问控制涉及访问者和通常被称为目标的特定对象之间的交互(interaction)。访问者可能是一个自动进程(如对一个节点地址的自动目录访问，或是单个用户发起的进程)。对象是存在于网络中的任何形式的资源(如数据库、数据库的一个特定项目、一台主机、一个进程、一条加密的E-mail消息等等)。目标是访问者所寻找的特定对象。重要的是应当记住：当对象被访问者寻找时，它就变成了目标。

2.3 安全策略

最简形式的安全策略是一套为有关的鉴别使命提供安全服务的准则。就MISSI访问控制而言，安全策略是一个更高的系统级的安全策略的子集，这个较高的系统级的安全策略定义了访问者与目标之间强制性访问控制的策略的方法，这些访问控制机理必须具备以下两点：

* 允许某个特定策略所许可的通信；
* 拒绝某个特定策略所不许可的通信。

安全策略是访问控制机理作出判断的依据。

2.4 管理

必须能有效地管理访问控制机理，这种管理仅仅是一整套管理服务的一部分，如果要向用户提供安全通信，必须执行这些管理服务。本文中的管理系指对使用MISSI通信协议的访问控制机理的检查和对访

问控制的尝试(不管成功或失败)的实时审计。

对采用 MISSI 通信协议的访问控制实现的审计系指一种“策略”,它控制 MISSI 组件的测试和认证。对访问控制的企图(不管成功与否)的检查必须是每个系统或实体(或潜在的目标资源)的连续操作。

访问控制管理过程可用类似于众所周知的物理访问控制(例如访问银行的金库)的过程来理解。当一个被授权的人员打开金库或进入开着门的金库时,需要登记,一个真实的或不变的记录保存着这一次访问行为;同样,当发生一次非授权访问(如一个小偷企图访问金库)时,这种企图必定会被警报系统注意到,且会被一个专门隐藏的摄象机记录下来。

这种情况可与 MISSI 的保护设备相比较,目标主人希望知道访问他们的目标的那些人的身份,以便把目标保管员以欺骗行为访问某个目标的事件记录在案。多数目标本身都希望知道非法访问者的身份,使得系统企图获得访问 MISSI 所控制的资源更可能被检测出来。当某个特定的访问者对目标的访问被拒绝时,是否通知访问者访问失败的原因或根本没有反应便返回,那就是安全策略的事情了。

2.5 访问控制技术

控制访问系统资源有两种常用技术。分别定义如下:

* **访问请求过滤**:当一个访问者试图访问一个目标时,将运行一个检验程序以确认他是否有权访问这个目标。一个要求访问目标的访问者是一个可计费的个人或者是一个代表可计费的独立的程序。

* **隔离**:不给予非授权的用户有任何访问敏感资源的机会。

访问请求过滤包括访问控制策略、访问控制表、技能和安全标识。当一个访问者请求访问一个目标时,访问控制策略就是用来验证访问者的策略,这种验证包括确认访问者是否已经获得那个目标的访问权限(MISSI AC 系统)。另一方面,隔离包括物理的、人员的、硬件的和操

作系统的安全的各种手段。

2. 6 一般的访问控制策略

在一个网络系统中,有四种基本的实现 AC 的方法,这些方法包括基于标签的、基于目录的、基于技能的和基于上下文的访问控制。每一种方法都建立一种不同的操作安全策略,它为获得 ACI 提供保障(判定和实施一个判定)。这些策略的应用取决于 AC 系统的准则(包括访问控制所需的数量、用户数、域的大小和数量等)。在 OSI 访问控制框架(ISO/IEC 10181 -3)中包含了这些策略,但在那里并不是按照强制性访问控制(MAC)或者选择性访问控制(DAC)来叙述的,而是强调基于规则的策略和基于身份的策略之间的区别。因此,为了实用起见,基于身份的策略(由用户选择的策略)等同于选择性策略,基于规则的策略等同于强制性的策略。

2. 6. 1 基于标签的访问控制

基于标签的访问控制使用访问者和目标受限的 ACI,这个 ACI 以安全标签来限制访问者和目标。该标签被用来进行 AC 的判定,因此允许数据在实体之间安全地传递。当多个访问者访问多个目标并要求 AC 的过程粒度(course granularity)时,这种方案是最方便的。基于标签的方法能够用来控制一个安全域中数据的流向,或者提供安全域之间的 AC。

一个安全标签可作为目标 ACI 去保护另一个目标。访问规则定义了在给定的访问者的安全标签和赋予目标的安全标签下所允许的访问权限。如果当前的安全策略要求 ACI 维持这个安全标签,并被用于目标ACI,则能够控制所有的目标内外的数据流。

体系结构中还有其它的基于标签的方案,但融合了其它的传送 ACI 的方法。基于规则的 AC 是一种用标签来识别目标的基于标签的方案,但它采用 X. 509 证书去识别访问者和相关的特权及支持策略。

基于规则的访问控制（RBAC）策略依赖于能够用算法表示的策略。基于规则的 AC 使用受限访问者和受限目标的 ACI 去传送由管理策略所建立的规则。对于 MISSI 而言，受限访问者 ACI 在 X.509 证书中传送，目标 ACI 在安全标签中传送。基于规则的策略的一个例子是按照国家安全标准来区分信息的级别，如绝密、机密、秘密。如果两个实体是同一分区的成员且二者都允许持有机密信息，则允许他们通信，因为他们的“MISSI 组件”遵守相同的国家安全规则。

基于规则的访问控制（RBAC）有两类：基于分区规则的访问控制（PRBAC），它以一种在整个分区（区域）中一致的策略为基础，这种策略和适合的规则几乎不可变，允许把它们分配给大量的实体。基于本地规则的访问控制（LRBAC）以适用于较少实体的规则的的策略为基础，LRBAC 满足实体数目少而又频繁变换策略的场合。例如，也许有这样一种规则：“红方”和“绿方”的成员仅能与他们内部群体中的成员通信，而“蓝方”的成员却能与“红方”和“绿方”的成员通信。这些规则适用于“本地”。本地应用这些规则的原因是：有关的策略经常变化，在本地非常容易控制。“本地”这个术语给出了正确的含义，但并不意味者代表成员实体必须被集中在一个地方，它们可以广泛地分布在各地。

2.6.2 基于目录(list)的访问控制

用目录去识别限定目标的 ACI 和限定访问者的 ACI 的访问控制是大家所熟悉的基于目录的访问控制。AC 目录(ACL)是一些项目的集合(或序列)，每一项有两个字段：访问者限定符和操作限定符。访问者限定符用来识别具有某种操作限定符的访问者的身份；类似地，操作限定符描述各种操作或操作的类型（在某次访问请求时），即对于相应的访问者的限定符而言是允许还是拒绝。基于目录的 AC 被当作访问者和操作限定符的目录加以管理，正如限定目标的 ACI 和单个的、分组的角色标签被当作限定访问者的 ACI 加以管理一样。

基于目录的AC可用在要求细粒度的AC的系统中,在少量访问者(或几组访问者)的地方,以及以每个目标而不是以每个访问者为基础进行AC管理的地方,它是最好的。在目标总数为动态的而访问者总数相对固定的地方,这种AC分类是很方便的。

基于角色访问控制是基于目录的AC一种形式,这时AC的判定取决于你在给定域被认可的的特权。这些特权依据你在那个域中作为用户的角色,并用一种基于目录的格式来表示。

基于身份访问控制(IBAC)以一种明显地适用于个人、主机,或一群个体或主机实体的策略为基础。是否允许访问一个目标只取决于身份或访问者的ACI。

2.6.3 基于性能(capability)访问控制

基于性能的访问控制根据限定访问者的ACI(一种性能)进行操作,它定义了一组允许的操作,这些操作可按目标的标识集合进行。限定访问者的ACI是一些性能的集合,它有两种主要成份:目标或目标组的名称、目标授权的运行目录。因此,按访问者执行AC管理,并提供一个域,该域包含访问少数目标的很多用户(或用户群)。

基于性能访问控制也考虑到限定目标的ACI,这个ACI由一些项目的集合组成,每个项目有两个部份:安全域机构的标识符(SDA)和安全域机构所认可的操作。因此它允许访问者的SDA撤回对目标的访问权。

2.6.4 基于上下文的访问控制(Context - Based Access Control)

基于上下文的AC以所执行的访问请求的上下文获得的信息为依据。从底层服务接口或者从本地管理接口可获得这些信息。依据限定访问者或限定目标的ACI对AC加以管理,控制表是一些项目的集合(或序列),每个项目有两个字段,即上下文限定符和操作限定符。上下文限定符是可施加操作限定符的上下文的一序列条件(如时间、路径、区域),每个上下文的条件都分别与一个真或假的语句相关连。操作限