铁路计算机应用
RAILWAY COMPUTER APPLICATION

基于标记技术的强制访问控制模型设计与应用

朱　涛，董　鹏，朱　贺，齐　胜

Mandatory access control model based on marking technology

ZHU Tao, DONG Peng, ZHU He, and QI Sheng

引用本文:
朱涛, 董鹏, 朱贺, 等. 基于标记技术的强制访问控制模型设计与应用[J]. 铁路计算机应用, 2022, 31(1): 55–60.
ZHU Tao, DONG Peng, ZHU He, et al. Mandatory access control model based on marking technology[J]. Railway Computer Application, 2022, 31(1): 55-60.

在线阅读 View online: http://tljsjyy.xml-journal.net/2022/I1/55

文章编号：1005-8451（2022）01-0055-06

基于标记技术的强制访问控制模型设计与应用

朱　涛[1]，董　鹏[2]，朱　贺[2]，齐　胜[2]
（1. 中国铁路信息科技集团有限公司　研发和建设处，北京　100844；
2. 中铁信（北京）网络技术研究院有限公司　网络安全研究室，北京　100044）

摘　要：为了增强铁路应用在新型计算基础设施环境下的网络安全防护能力，根据《信息安全技术 网络安全等级保护基本要求》，在铁路现有的网络架构基础上，设计铁路网络空间安全体系架构，并提出适用于该体系架构的强制访问控制模型。依据该模型，利用标记技术可以实现相同网络空间相同域、相同网络空间不同域和不同网络空间之间的强制访问，并与可信操作系统、数据交换平台和数据交换总线协同工作，能够实现对访问操作的管控，保证数据安全交换，提升铁路网络的安全防护能力。

关键词：等级保护；主体；客体；标记技术；强制访问控制；铁路网络空间
中图分类号：U29 : TP393　**文献标识码：**A　**DOI：**10.3969/j.issn.1005-8451.2022.01.09

Mandatory access control model based on marking technology

ZHU Tao[1], DONG Peng[2], ZHU He[2], QI Sheng[2]
(1. R&D and Construction Department，China Railway Information Technology Group Co. Ltd., Beijing　100844，China；2. Network Security Research Office, China Railway Information (Beijing) Network Technology Research Institute Co. Ltd., Beijing　100044, China)

Abstract: In order to enhance the network security protection ability of railway applications in the new type computing infrastructure environment, according to the basic requirements for network security level protection of information security technology, based on the existing railway network architecture, this paper designed the railway cyberspace security system architecture, and put forward the mandatory access control model suitable for the system architecture based on marking technology. According to this model, the marking technology could be used to implement the forced access between the same domain in the same cyberspace, different domains in the same cyberspace and different cyberspace, and work together with trusted operating system, data exchange platform and data exchange bus, so as to implement the control of access operation, ensure data security exchange and improve the security protection ability of railway computing platform.

Keywords: classified protection；subject；object；marking technology；mandatory access control；railway cyberspace

以云计算为代表的新型计算环境大部分是基于高速网络访问并可共享访问，按需分配的计算模式[1]。自提出以来，云计算已进入稳定发展的阶段。但是，云计算的大规模应用使安全事故频发，出现了诸如横向扩展、访问混乱、账户劫持等问题[2]。铁路业务系统经过长期的分散发展，一直以业务或者应用为中心进行安全防护和建设，产生了许多“碎片化”“区域化”网络，因而网络安全的防护设计在整体上不够全面，易出现“单兵作战”的情况，降低铁路业务系统的整体防护能力[3]。尤其在应对新型网络威胁下，铁路网络安全由于主动防御能力欠佳，联防联控防护能力较弱，导致在云计算环境下的安全事件频发。

按照《网络安全等级保护 2.0》系列标准的要求，在三级及以上的信息系统要求在安全区域网络、安全区域边界、安全计算等各个层面实施强制访问控制，通过对重要主体和客体设置安全标记的方式，控制主体对有安全标记信息资源的访问[4]。访问控制技术可以通过授权信息，对资源访问操作进行控制，实现对信息资源的保护[5]，从而有效阻止非法接入和

收稿日期：2021-05-27
基金项目：中国国家铁路集团有限公司科技研究开发计划重大课题（K2019S001）
作者简介：朱　涛，正高级工程师；董　鹏，高级工程师。

非法入侵，保证信息资源的合法使用。

本文设计基于标记技术的强制访问控制模型（简称：访问模型），以两个安全要求为设计原则：

（1）只有经过认证并授权的主体可以发出访问或者执行请求；

（2）只有正确的访问或者执行请求才可以到达客体资源，实现了铁路业务系统在云计算环境下的纵深防御、多级安全和细粒度访问控制和防护。

1 铁路网络安全架构

铁路网络现已覆盖中国国家铁路集团有限公司（简称：国铁集团）、18 个铁路局集团公司和 5 000 多个基层站段，在纵向上分为国铁集团级、铁路局集团公司级（简称：铁路局级）和站段级三级网络[6]，在横向上在国铁集团和铁路局集团公司形成外部服务网、内部服务网和安全生产网三网分离的架构，如图 1 所示。外部服务网承载面向社会大众，提供服务的系统。内部服务网承载面向铁路内部人员，提供一般性服务的系统。安全生产网承载关系到铁路运输生产的系统。另外，根据安全生产需要，铁路网络建设了专用业务生产网络，如列车运行控制专网、列车调度指挥专网、客票系统专网、资金专网、公安专网等。

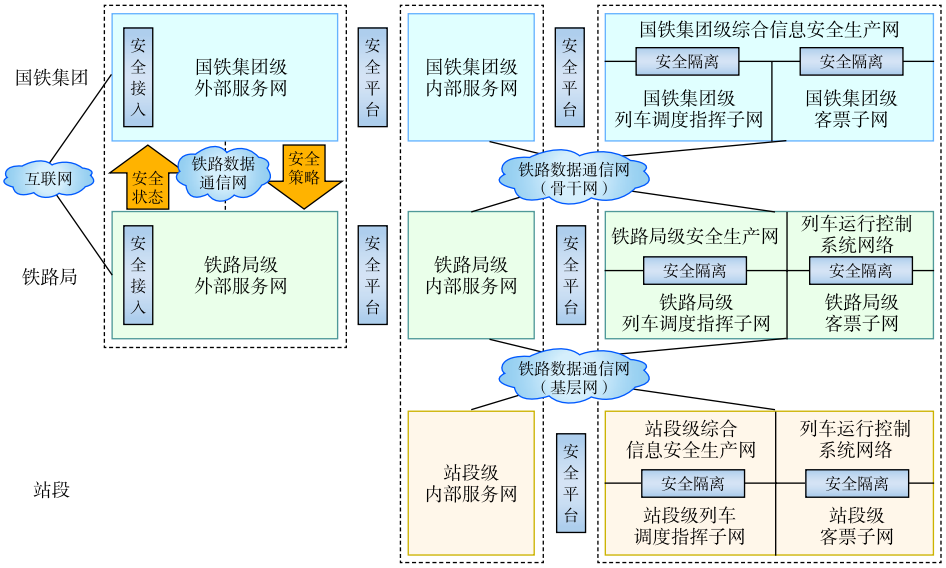

图1 铁路网络架构

2 模型设计

2.1 铁路网络空间安全体系架构设计

按照国家相关管理部门的要求，进一步优化铁路网络安全的体系架构，本文在既有的铁路网络架构基础上，设计了铁路网络空间安全体系架构，如图 2 所示。铁路网络空间安全体系对应于现有的铁路网络架构，将铁路信息分为服务网络空间、管理网络空间和生产网络空间。

（1）服务网络空间在物理上由互联网和外部服务网构成，主要部署对外服务和外网应用，以及外网终端。

（2）管理网络空间基于内部服务网，主要部署应用服务资源和内网终端。

（3）生产网络空间基于铁路业务的各个生产网，合并构成新的用于生产服务的网络空间，由生产设备构成。

铁路网络空间安全体系架构在密码技术和可信计算的基础上，以“一个中心三重防护”作为总体思路，进行安全体系架构设计。

“一个中心”即安全管理中心[7]。作为统一管理调度平台，安全管理中心对策略对象统一进行建立、维护、下发、跟踪、收集，实现完整的智能策略调度闭环管理。安全管理中心由可信策略管理模块、访问关系管理模块、客体策略管理模块和主体策略

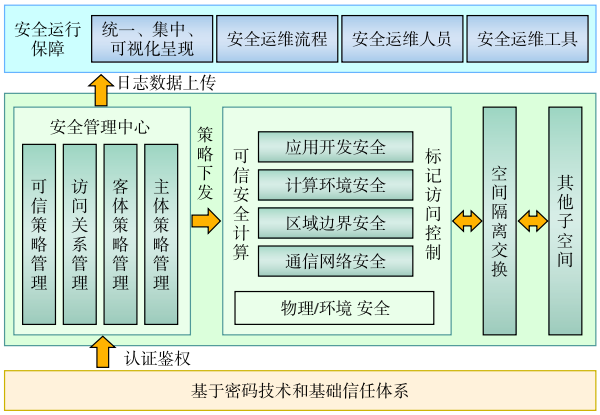

图2　铁路网络空间安全体系架构

管理模块组成。

“三重防护”即计算环境安全、区域边界安全和通信网络安全。该体系通过标记强制访问控制技术和可信安全计算，在物理环境安全的基础上不仅可以满足三重防护的要求，还可以实现应用开发安全。标记强制访问控制技术通过每一次访问操作进行管控，可确保访问操作安全可控。可信安全计算技术通过网络准入控制和程序白名单机制，确保访问过程安全可信。

网络空间的子空间之间通过安全隔离交换设备进行数据的安全交换，并将收集的威胁信息、边界网络和终端的日志数据上传到态势感知系统进行智能化关联分析，将全网的安全态势可视化展现。

2.2　访问模型

网络空间 4 要素为载体、主体、操作和资源，其中，载体是部署在网络空间的物理设备；主体泛指各种应用、程序等；操作指主体对资源的访问过程；资源又称为客体，一般为文件、数据库等。在不同网络空间，仅有限资源可以跨越网络空间。在各网络空间安全域之间采用有限的安全数据交换，实现空间之间的信息有限共享，铁路计算平台安全方案是以资源为核心的防护模型，空间安全域之间仅交互有限资源，空间安全域内需要确保有限访问。铁路网络空间的安全域划分如图 3 所示。每个网络子空间内部划分为不同的安全域：服务网络空间和管理网络空间划分为服务器域和终端域；生产网络空间划分为管理域、设备域，实现不同安全域之间的相互隔离和分层防护。

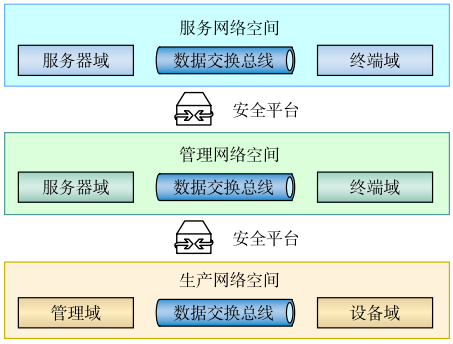

图3　铁路网络空间内安全域划分

基于标记技术的可信访问模型的建立可以确保访问过程中每个主客体的操作都是可信的。铁路网络空间内的访问需求主要有 3 种访问模型：（1）主体对相同空间、相同域内的客体进行访问；（2）主体对相同空间、不同域内的客体进行访问；（3）主体对不同空间、不同域内的客体进行访问。

第 1 种访问模型如图 4 所示。主体和客体不仅在相同的空间，而且也在相同的域内。首先，操作系统或安全模块根据进程的签名信息和安全配置策略文件信息，生成主体标记信息。主体发出携带该标记信息的访问请求，该请求可以通过代理实现对客体的安全访问。代理提供数据传输接口，通过对标记信息识别判断是否可以传递主体的访问请求给对应客体单元。客体对象受资源保护单元保护，资源保护单元收到来自主体的访问请求后，根据请求中所携带的标记信息进行判断，给予本次访问对应的客体操作权限。

第 2 种访问模型如图 5 所示。主体和客体虽然都在同一空间，但是需要跨越不同的安全域（域 1、域 2）进行传输。操作系统或安全模块根据安全配置策略文件信息，结合进程的签名信息生成主体标记信息。主体发出的访问请求中携带该标记信息，该请求可以通过代理实现对客体的安全访问。代理提供数据传输接口，通过对标记信息识别判断是否可以传递该请求给客体所在的域。到达客体域后，代理通过对标记识别判断是否可以传递该请求给对应客体单元。客体对象受资源保护单元保护，资源保

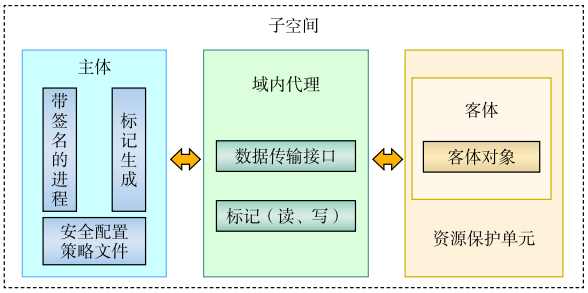

图4　第 1 种访问控制模型

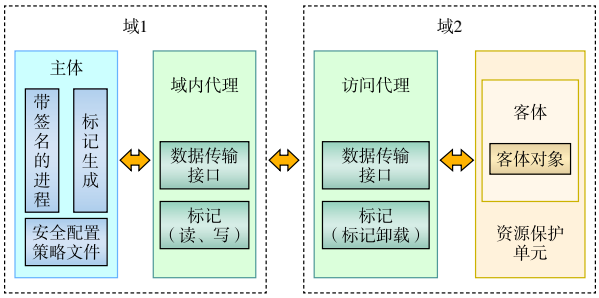

图5　第 2 种访问控制模型

护单元收到来自主体的访问请求后，根据请求中所携带的标记信息进行判断，给予本次访问对应的客体操作权限。

第 3 种访问模型如图 6 所示。主体不仅要跨越不同域，还要跨越不同空间。此时主体的访问请求不仅需要域内代理和访问代理，同时需要数据交换平台进行数据摆渡。操作系统或安全模块根据安全配置策略文件信息，结合进程的签名信息生成主体标记信息。主体发出的访问请求中携带该标记信息，该请求可以通过代理实现对客体的安全访问。代理提供数据传输接口，通过对标记信息识别判断是否可以传递该请求给客体所在的网络空间，在网络空间边界处数据交换平台通过对标记进行识别判断，实现数据的准入控制。在客体空间内，代理通过对标记信息识别判断是否可以传递该请求给对应客体单元。客体对象受资源保护单元保护，资源保护单元收到来自主体的访问请求后，根据请求中所携带的标记信息进行判断，给予本次访问对应的客体操作权限。

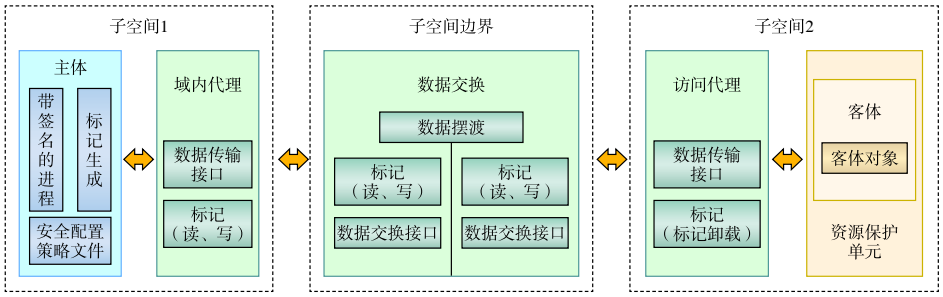

图6　第 3 种访问控制模型

3　模型应用

3.1　系统构成

基于访问模型的系统由部署在服务器或终端计算节点内的可信操作系统或安全模块、部署在云虚拟机内的安全数据交换总线和部署在不同网络空间边界的网络安全数据交换系统构成。该系统可以对每一次主客体的访问操作进行管理，将主体标记—操作标记—客体标记为每次访问会话的标识依据，以对空间内的每次访问进行准确管控。

（1）数据交换系统

数据交换系统与网络隔离技术、标记强制访问技术、准入控制技术和数据加密技术相结合，在不同的区域边界部署性能不同的数据交换系统，以保证数据的机密性和完整性，防止病毒、恶意程序、非法授权访问跨越不同安全域[8]。数据交换系统还具有添加和去除标记信息的功能，是标记强制访问的核心系统。

（2）数据交换总线

数据交换总线运行在支持标记技术的操作系统上，提供数据传输接口，通过对标记信息识别判断，控制数据流向，实现同一子空间的不同应用之间，

以及不同子空间之间的数据安全交换。数据交换总线还设置了数据缓存区，通过直接读取缓存区中的数据提高运行效率。

（3）可信操作系统

可信操作系统可以实现操作系统之上的可信，而在操作系统之前启动的程序就无法进行访问[9]，只有经过安全模块验证的、带有正确标记信息的进程主体才可以在操作系统中运行，发出操作请求；没有标记信息或者标记信息错误的请求则会被抛弃。可信操作系统还会建立主客体和对应操作的访问控制矩阵，按照控制矩阵确认对每个访问操作进行控制，实现强约束条件下的受控访问。

3.2　数据传输

数据传输分为以下两种情况。

（1）应用若访问同一个网络子空间的数据资源，其数据传输如图 7 所示。

图7　同一个网络子空间的数据传输示意

① 应用（主体）调用安全模块给访问请求添加标记信息，完成标记的初始化。

②安全模块将带有标记信息的报文发送到数据交换总线，由数据交换总线依据报文信息的目标地址，将访问请求传输到被访问端的安全模块。

③安全模块依据访问控制矩阵判断操作请求的合理化，请求按照访问操作矩阵的规定对资源进行有限访问。

（2）应用的访问请求若要跨越不同的网络子空间，其数据传输如图 8 所示。

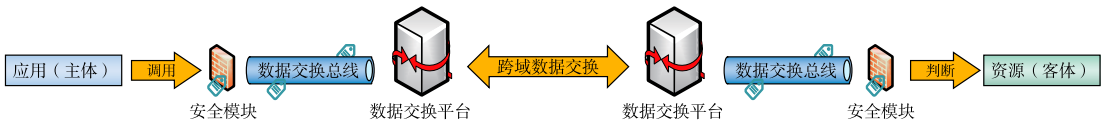

图8　跨越网络子空间数据传输示意

① 应用（主体）调用安全模块，给访问请求添加标记信息，完成标记的初始化。

②安全模块将带有标记的报文发送到数据交换总线，数据交换总线依据报文信息的目标地址，将数据报文发送至数据交换平台。

③数据交换平台对标记信息进行检查，核实能否向下传输。核实之后，当前数据交换平台将报文发送至下一个网络子空间的数据安全平台。

④目标端的数据交换平台会重新添加标记信息，对数据报文进行重新组装，然后发送至数据交换总线。

⑤数据交换总线将报文发送至安全模块，安全模块对标记信息识别判断后进行资源访问。

4　关键技术

标记技术是铁路计算平台安全方案实现强制访问控制的关键技术，由安全模块生成标记信息。标记信息是操作系统、网络控制设备对主客体进行标记和强制访问控制的依据，包括安全等级、数据基本属性、安全机制等信息。主体是主动发起动作的实体，一般指进程；客体是主体发起动作的对象，一般指文档、图像等数据。在铁路网络空间内利用标记技术对客体进行保护，对空间内的操作进行管控，仅有空间内允许的资源可以通过隔离设备穿越空间；同时，建立主体、资源和对应操作的访问控制矩阵，利用控制矩阵对每次操作进行访问控制，对应的主体只进行固定的操作，完成在强约束条件下的受控访问。在输入/输出层部署管控模块，实现客体对主体访问操作的识别和认定，同时对资源进行加密保护，只有操作正确才可以透明地施加在资源上，非授权的访问则被禁止。

5　结束语

本文从铁路网络架构实际情况出发，结合网络安全的要求及发展，设计了铁路网络空间安全体系架构，为铁路各信息系统与生产系统的空间划分、

安全优化、访问防控等方面提供了基础研究保障。本文所提出的基于标记技术的强制访问控制模型可以对网络空间内每个访问进行控制，实现铁路网络空间内的端到端安全访问，实现了铁路网络内空间、区、域、端的基于一体化安全策略的安全访问控制模型。

参考文献

[1] 锁向荣，齐　胜，张悦斌，等. 铁路云平台细粒度访问控制方案研究 [J]. 铁路计算机应用，2021，30（4）：45-49.

[2] 纪　方，田海波，刘鹏宇. 铁路云计算安全标准研究与实践 [J]. 铁路计算机应用，2020，29（9）：42-46.

[3] 史天运. 铁路行业信息安全管理面临的挑战及对策探讨 [J]. 铁路计算机应用，2015，24（2）：1-4.

[4] 全国信息安全标准化技术委员会. 信息安全技术 网络安全等级保护基本要求：GB/T 22239-2019[S]. 北京：中国标准出版社，2019.

[5] 鲍连承，赵景波. 访问控制技术综述 [J]. 电气传动自动化，2006（4）：1-5,18.

[6] 吴　冲. 我国铁路信息化建设现状及发展方向 [J]. 物流工程与管理，2013，35（1）：82-84.

[7] 周泽岩. 基于铁路行业的新时代网络安全技术体系的研究 [C]//2020年第四届国际科技创新与教育发展学术会议论文集（卷一）. 香港：香港新世纪文化出版社有限公司，2020：3.

[8] 朱　贺，齐　胜，张悦斌. 安全隔离与信息交换技术研究 [J]. 通讯世界，2021，28（1）：105-106.

[9] 雷彦斌，朱　贺，齐　胜，等. 可信计算技术在铁路即时通讯系统建设中的应用 [J]. 通讯世界，2020，27（12）：3-4，7.

责任编辑　张晓芬