城市轨道交通云平台信息安全方案研究

刘琳
北京市地铁运营有限公司通信信号分公司

[摘　要]随着社会经济的快速发展城市化建设的不断加快，我国城市轨道交通行业也进入了上升时期。城市轨道是一个包含大量信号设备和运营数据的系统，需要一个性能优越的综合管理平台进行管理。文章根据城市轨道交通业务系统特点及云平台特点分析云平台信息安全需求，并对主要业务系统承载方案、云平台信息安全方案进行研究，制定城市轨道交通云平台信息安全体系框架，为城市轨道交通云平台信息安全体系的设计和建设提供参考。

[关键词]城市轨道交通；云平台；信息安全方案；研究
【DOI】10.12252/j.issn.2096-6261.2021.08.711

引言

当前，云计算在各个领域发展迅速，但在城市轨道交通领域起步较晚，各地控制中心仍基于传统的服务器运营模式，体系架构陈旧、技术落后、各业务系统之间存在信息“孤岛”，安全管控薄弱，CPU利用率低，耗费成本高，占有大量人工及用房面积，造成相当程度的资源浪费，不符合绿色低碳的技术理念。随着轨道交通技术的不断发展，伴随着大量数据的增加，也给设备扩展带来了一定的压力。伴随着云平台技术的引进，我国较发达的一、二线城市，都在积极地规划建设新型“智慧”城市。结合国家推进、政府响应以及城轨行业内部推动等方面的影响，轨道交通融合云平台的建设势在必行。

1 城市轨道交通云平台建设需求分析

①管理需求。城市轨道交通云平台的建设需要符合最新监管合规的各项要求，如网络安全法、网络安全等级保护基本要求、智慧城轨信息技术架构和信息安全规范等法律法规的要求。云平台需要满足三级等保要求，并为云上业务系统提供IaaS层的三级等保能力。云平台的安全体系建设参考等级保护三级基本要求，搭建符合业务运行基本安全需求的安全体系，争取做到既考虑安全实效，又兼顾投资成本，减少安全疏漏，避免贪大求全。适度安全：信息安全业界的基本原则之一就是没有绝对的安全，多少预算都无法保证云数据中心的绝对安全。随着云数据中心安全性的提高，需要的预算也越来越高，系统的性能和灵活程度就越低。安全体系建设的目标为适度安全，在合理的预算范围内，尽可能保证云数据中心免受外部用户和内部人员的非恶意安全威胁。前瞻性和可扩展性：云数据中心云平台建成后，将接受公安部的等级保护测评，安全体系的设计应具有前瞻性和扩展性，保证后续可以逐步扩充，接受测评时不会由于设计不合理导致返工和浪费。②业务需求。当前城市轨道交通业务系统拥有自己的独立的网络，城市轨道交通云平台及网络部署后，需要考虑部分业务上云、部分业务自有网络运行的混合运行模式以及混合运行模式下的安全防护。混合运行模式下，需要对各业务系统的纵向网络防护以及云平台自身及承载业务的防护分别设计。云平台需要为部署在多个安全域的业务系统定制协同一致的安全策略，提供基础平台的安全服务，以保证业务的完整性。基于平台云化的需求，信息安全需要考虑前瞻性，安全需要适应云平台的需求；安全服务化，具备敏捷、弹性能力；基于云平台承载的业务，持续提升云平台的安全服务能力。

2 城市轨道交通云平台信息安全方案设计

2.1云平台的服务模式

云平台的服务模式有三种：基础设施即服务（IaaS）：主要为用户提供虚拟机、网络连接、计算和存储等资源，用户可在平台上搭建自己所需的应用系统，或是运行大型专业软件，甚至可以按用户需求灵活地扩展或缩减存储容量，这大大缩减了网络、计算、存储及服务器等设备的开销。平台即服务（PaaS）：该服务建立在IaaS平台和硬件之上，服务商可以为用户提供更多服务，如完整的、可进行软件研发的环境和平台，包括开发的工具、语言、数据库以及Web服务器，用户只需要通过运行平台或互联网编程接口来部署应用环境。提高了平台上可利用资源数目，因此，PaaS的出现同时也促进了SaaS的发展。软件即服务（SaaS）：服务商可利用互联网浏览器为用户提供个性化服务系统，用户无须关注底层的管理，购买软件服务后，只需通过浏览器或者Web程序使用已部署在云平台上的应用，可以轻松管理企业，还可以根据需求定制软件，或自行组装、配置软件的各个模块，具有极大的灵活性和便捷性。

2.2轨道交通云管平台设计

轨道交通云平台管理平台通过设置统一入口，将轨道交通领域多个线路中心的资源整合，统一调度管理，并封装成标准的云服务业务。对内部轨道交通提供基础云服务，对外部轨道交通用户提供云服务。轨道交通云平台资源管理模块从逻辑层面来讲划分为四层，分为业务逻辑层、用户层、业务中间件层、数据层。用户层包括管理员访问服务和用户访问服务、CLI以及第三方外部应用服务；业务逻辑层主要包含资源、设备、运维、统一认证、系统5个管理、接口功能及异常、故障管理体系和全局安全管理；业务中间件层属于整个资源池的业务基础平台，所有的上层业务功能全都是基于业务中间件层构建设计完成，而且为上层应用模块提供相对

便捷的基础运行环境；数据层主要是对资源池系统各类数据提供存储管理，从而完成资源池数据的管理与存储工作。轨道交通云平台提供云安联动，实现虚拟机安全部署策略定制化设置及安全攻击阻断机制运行，保护业务系统免受外部攻击；提供云网联动，实现一键开通网络功能的便捷服务；与运维融合实现重启等相关联动，根据智能监控系统报警实现云主机资源重启联动功能；与数据中心融合提供基于大数据分析的功能以及经过数据中心建模后的相关轨道交通业务数据整理与服务。

2.3业务系统承载设计

城市轨道交通云平台的服务对象是业务系统，各业务系统通过骨干网的各级接入节点及数据中心节点连接云平台，使用云平台的计算、网络和存储资源。根据《智慧城轨信息技术架构及信息安全规范》规定，应遵循“系统自保、平台统保、边界防护、等保达标、安全确保”策略，以网络安全等级保护为基础，分级分类建立应用系统的安全保护措施。承载在云平台和自有网络运行的部分，都需要各业务系统管理者自行部署安全防护策略，安全责任也归属于业务系统管理者。对于承载在云平台上的业务系统，安全由应用系统自身安全机制和云平台的安全机制协同保障，根据各业务系统的安全诉求，云平台需要提供对应的安全能力，在各层级、各区域分别给予防护。承载在云平台上的各业务系统，应采用“网间分级隔离”策略。在云平台网络节点上采用路由+转发平面隔离，在云数据中心为各业务系统提供专属的虚拟网络（VPC）。VPC之间可以实现安全隔离，保证不同业务系统之间的安全隔离以及云平台与业务系统之间的安全隔离。如果业务系统之间通过云平台互通，应在云平台数据中心及骨干网的对应位置部署安全防护策略，对业务系统之间互访的流量进行防护，保证流量正常转发。

2.4安全设计

融合云平台安全体系建设涉及运维单位、业务部门、云平台提供方、应用系统厂商等多个项目参与方，由于各参与方对所管理的资源控制力度和所有权各不相同，因此需要建立安全共建、责任共管的模型来共同保障云平台系统的整体安全。轨道交通融合云平台系统安全框架可分为终端安全、网络安全、虚拟化安全、主机安全、应用安全和数据安全等几个层面，在满足各层面安全的基础上做到安全管理、安全服务和等保安全合规。①终端安全包括各种办公终端、监控终端及各类服务器的安全，所采用的安全措施包括部署防病毒软件、主机防火墙、主机入侵防护系统等一系列主机安全防护系统。②网络安全可以采用防火墙、入侵防御、AntiDDOS和VPN等一系列网络安全措施。③虚拟化安全由虚拟化平台自身实现各类安全加固措施，包括虚拟资源隔离、云平台安全加固、VDC、VPC和安全组等。④主机安全包括融合云平台针对各类服务器的安全防护措施，例如部署主机入侵防护、防病毒软件、软件白名单和终端管理软件等各类主机安全措施。⑤应用层安全涉及各类业务应用的安全，主要采用WAF和安全沙箱等技术。⑥数据安全是保障城轨业务安全运营的重点，应从数据隔离、访问控制等多个方面采取安全管理措施。对于融合云平台信息安全的设计，应保证系统安全合规、安全风险可控、安全责任明确。融合云平台和相关业务自上而下从安全管理、数据层、应用层、虚拟化、主机、网络、终端等几个层面考虑，满足等保3级的安全标准。

2.5云平台信息安全防护设计

根据《信息安全技术网络安全等级保护安全设计技术要求》（GB/T25070-2019）的要求，连接到云平台的业务应用程序系统将具有适当级别的信息安全保护系统，针对乘客服务、资源管理、媒体发布和其他业务的“系统自我保护”应用程序以及与资产管理有关的开发、管理、维护和付款应用程序。内部服务应用领域：主要用于项目管理、智能建筑模型、建筑单位的风险管理、日常维护、运营单位的管理和建设以及企业财务、合同和办公自动化系统。安全生产应用：主要运行生产应用系统，包括乘客信息系统、自动售检票系统、综合监控系统和集中报警系统。运营和维护应用程序域：完整的应用程序和工具，主要用于云平台管理、网络管理、应用程序管理和安全管理。它旨在基于虚拟机隔离、容器隔离和微服务安全开发框架原理，应用程序到应用程序隔离和安全数据交换以及云到端安全保护策略的集成设计。它使用云平台提供的微服务安全开发、体系结构和安全组件来实现安全机制，例如身份认证、权限管理、加密通信和安全存储。

结语

面对信息安全风险和加强防护意识的形势，城市轨道交通工程应依照等级保护规范打造针对城市轨道交通云平台的信息安全防御体系。本文从城市轨道交通云平台信息安全的需求分析入手，对云平台的设计原则、云上业务系统承载方案、云平台信息安全方案进行研究，制定了城市轨道交通云平台安全体系框架，有利于在城市轨道交通行业内建立统一标准，为城市轨道交通云平台信息安全体系的设计和建设提供指引。

参考文献

[1]赵庆安，戴克平，唐龙.城市轨道交通整体网络安全风险分析及应对策略[J].铁道通信信号，2021，57（3）：84-89.

[2]陈超群，陈勃，刘布麒，等.轨道交通网络信息安全防护系统研究与设计[J].电气技术，2020，21（2）：50-55.

[3]荣喜丰.云计算技术在计算机网络安全存储中的应用[J].电子技术与软件工程，2020（22）：251-252.

[4]黄龙，张博.城市轨道交通云平台建设方案分析[J].铁道通信信号，2020，56（9）：76-80.