文章编号：1005-8451（2015）09-0022-05

铁路移动办公系统安全防护方案的研究

蒋笑冰
（北京铁路局 北京铁路通信技术中心，北京 100038）

摘 要：本文综合分析铁路移动办公系统网络接入存在的安全风险，结合铁路信息安全技术架构特点，提出一种铁路移动办公系统网络安全接入方案。该方案针对铁路移动办公系统网络接入安全风险设计，并与铁路信息网络安全技术架构特点相适应，为铁路移动办公系统网络接入安全防护提供了一种新的方法。

关键词：铁路移动办公系统；网络安全；终端安全
中图分类号：U29：TP39 **文献标识码：**A

Security protection scheme for Railway Mobile Office Automation System

JIANG Xiaobing
(Beijing Railway Communication Technology Center, Beijing Railway Administration, Beijing 100038, China)

Abstract: After analyzing the security risk of network access for Railway Mobile Office Automation System and combining with the technique architecture of railway information security, this paper proposed a security scheme of network access for the System. This scheme was aimed at the security risk, adapted to the technique architecture of railway network security, which was provided a new approach to security protection of network access for the System.

Key words: Railway Mobile Office Automation System; network security; terminal security

随着智能终端应用的普及，移动办公的需求日益增多，建设一个铁路移动办公系统，支持随时随地的移动办公业务审批、信息快速查询、移动网络互动交流，以提高办公处理效率和办理灵活性非常必要。移动办公系统在满足办公人员便利的同时，也带来了诸多安全隐患，为此，本文提出一种铁路移动办公系统网络安全接入方案。

1 系统介绍

铁路现有办公系统始建于2002年，后续相继开发了机关办公网、电子邮件、公文流转、档案管理等多个子系统，在日常办公中发挥了一定作用。由于办公系统建设时间较早，存在建设理念不新、技术标准不统一、业务规范性不高、应用功能不能满足需要、硬件设备陈旧等诸多问题。目前电力等行业已经部分实现移动办公[1~3]，铁路亟待建设铁路移动办公系统，支持移动终端、实现移动办公。在无线网覆盖的地方，随时随地可以上网办公、参加会议。支持视频、短信、网络电话、微博、微信、即时通、邮件等多种通信方式，选择方便、快捷、直观、简洁的工作和通信方式，实现双人、成组、会议多媒体方式。移动办公接入铁路信息网络，实现应用系统间的互联互通与信息共享。

2 安全风险及需求分析

2.1 安全风险

2.1.1 数据泄密的安全风险

移动办公系统所涉及的部分数据比较重要和敏感。移动终端在通过网络访问这些数据时，如果有恶意程序在终端后台运行，可能在用户不知情的情况下对敏感数据做拦截、截图等非法操作；当终端连接互联网时，包含敏感信息的数据在用户不知的情况下可能被发送到互联网指定位置。

在移动办公过程中，用户可能会将企业敏感的信息文件存储到终端的本地磁盘中进行操作，导致这些敏感信息存在泄漏的风险。

2.1.2 网络环境的安全风险

移动终端有可能从任意地点、任意环境通过无线网或互联网访问移动办公系统，当数据在无线网或

收稿日期：2015-01-29
基金项目：中国铁路总公司科技研究开发课题（2015X009-I）。
作者简介：蒋笑冰，高级工程师。

互联网进行传输时，可能会遭受到各类攻击和窃听。接入终端在进行远程办公的过程中，如果还能继续访问互联网，就会造成互联网和企业网络交叉访问，带来严重的安全风险。

2.1.3 移动终端自身的安全风险

移动终端在提供用户便利的同时，由于其便携小巧，遗失、被盗被抢的风险大大增加，对终端存储的数据造成威胁。

由于用户终端接入网络的安全性未知，终端在上网或安装其他软件的过程中，容易感染病毒或被恶意植入木马，当用户通过终端进行移动办公的时候，这些病毒和木马可能会扩散到企业的内部网络中，从而带来巨大的安全隐患。

2.1.4 接入身份的安全风险

攻击者可能伪装、假冒成合法用户，通过网络接入到应用系统中，从而进行信息窃取、破坏和攻击等行为。

2.1.5 内外网信息交换的安全风险

数据大都存储在内网中，如果对来自互联网的访问未经有效防护，将带来内网数据被破坏的风险。

2.2 安全需求

移动办公系统的安全需求如下。

2.2.1 保证敏感信息的使用和存储安全

保证敏感数据在网络访问和存储中的完整性、机密性和不可否认性；保证未授权的其他应用不能调用办公系统的数据。在网络、终端、主机多个层面保证数据安全。

2.2.2 保证移动办公接入网络通道的安全

需要使用加密专用网络访问通道，保证数据在传输中的机密性。

2.2.3 保证终端的安全

通过多种技术手段提升终端安全性，制定终端安全策略，对终端的行为进行适当控制。加强终端病毒、木马防治。当移动终端丢失时，采用远程数据擦除等补救措施。

2.2.4 保证使用移动办公系统的用户均经过安全认证

需要在不同层次对用户进行身份认证，用户接入网络和用户访问移动办公系统时认证用户身份，保证只有经过认证的用户才能使用移动办公系统。

2.2.5 保证移动办公数据在内外网之间交换的安全

需要通过安全平台的代理机制和访问控制机制保证数据在内外网之间的安全交换。

2.2.6 保证移动应用的安全管理

为移动终端提供安全的应用软件，需要搭建面向内部的移动应用管理平台，对企业内部应用及公共应用进行发布、审核、更新和管理，并对企业移动应用进行病毒扫描、更新、删除等。

3 安全架构设计

通过对移动办公系统的风险分析，本方案的安全目标是保障在移动办公系统访问过程的整体安全性。结合安全需求分析，方案需要考虑的安全要点主要是敏感信息的保密性、网络接入的安全性、移动终端的安全性、接入人员身份的合法性、内外网数据交换的安全性以及移动应用软件的安全性。本方案分别从网络安全、终端安全、应用安全、主机安全和物理安全 5 个方面进行设计[4]。架构如图 1 所示。

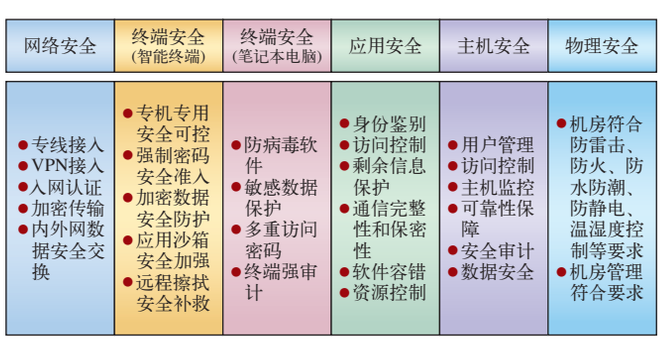

图1 安全架构

4 安全设计方案

4.1 网络安全

4.1.1 安全区域划分

根据移动办公系统的部署架构，该系统的安全区域分别是互联网区、外部服务网区、内部服务网区。安全边界分别是互联网 / 公网边界、内外网边界，对不同安全域边界采取相应的安全措施，重点保障边界接入安全。

4.1.2 网络接入边界安全

当用户希望在非办公室的环境中能够随时访问敏感业务和敏感数据时，可以采用安全性更高的无线移动虚拟拨号专用网络（VPDN）实现对用户的安

全接入和访问控制管理，如图 2 所示。

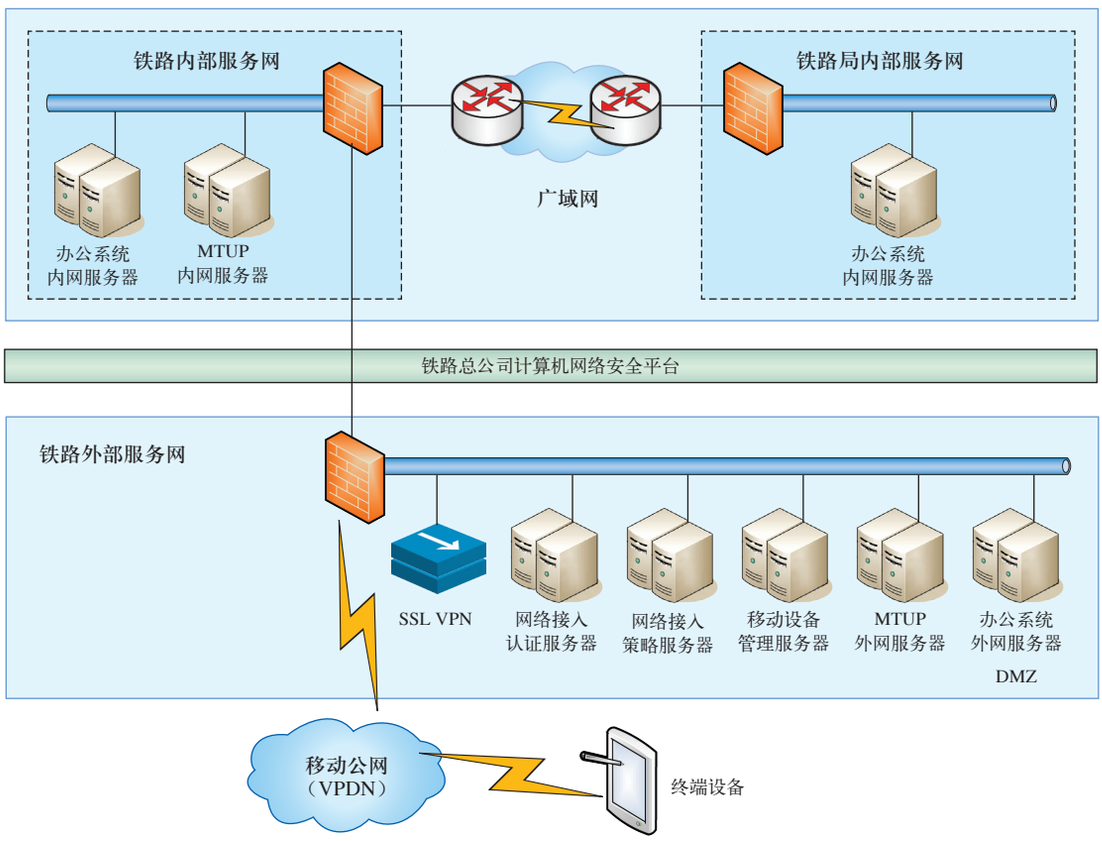

图2　移动办公安全接入

用户使用各类终端设备，通过移动公网接入铁路外部服务网。在铁路外部服务网部署 SSL VPN 设备、网络接入认证服务器、网络接入策略服务器、移动设备管理服务器，构成移动办公网安全平台。

内外部服务网边界主要通过既有网络安全平台访问控制系统实现边界划分。移动办公内外网信息交换网关通过与安全平台访问控制系统及安全隔离与信息交换设备的协同工作，实现内、外网边界数据的安全交换以及统一的访问控制，优化用户体验。

4.2　移动终端安全设计

根据移动终端的类型不同，移动终端安全设计分为笔记本电脑安全设计和智能终端安全设计。智能终端包括：智能手机、平板电脑、手持终端等。

4.2.1　笔记本电脑安全设计

（1）检测防病毒软件更新状态

联网计算机安装并运行防病毒产品和补丁升级产品，及时修补安全漏洞，定期实行病毒扫描、病毒特征码更新和软件补丁升级，接受病毒防治系统的集中控制。

（2）敏感信息保护

在进行远程办公时，用户访问内部网络的应用，可能会从应用获取一些内部文件到本地磁盘进行处理。这些文件可能含有敏感信息。由于接入终端在非办公时间可能连接互联网，这些存储在本地的信息具有极大的安全风险，容易造成敏感信息的泄漏。移动终端安全管理系统可提供文件保险箱功能，保证信息在本地存储的安全性。

（3）设定多重访问密码

笔记本电脑必须设定开机密码和锁屏密码，必须设置合理的自动锁屏时间，访问敏感数据的应用程序必须设定独立的访问密码。可通过移动终端安全管理系统策略进行检查和报警。

（4）终端强审计功能

当用户进行远程办公时，立刻启用录屏强审计措施，信息记录在本地，不能删除，回单位后可由审计人员提取。另外，对于文件保险箱的操作进行审计，记录文件保险箱向本地磁盘的文件操作。

4.2.2　智能终端安全设计

智能终端安全的解决方案主要从数据的敏感性、设备的移动性和便携性 3 个特性所带来的安全风险着重解决。可以通过在企业内部设置移动终端安全管理服务器，移动终端安装客户端的方式来解决移动终端上的众多安全问题，如图 3 所示。

（1）专机专用

图3　智能终端安全设计

为保证敏感数据的安全性，数据不被第三方程序监控和窃听，任何有权访问敏感数据的移动终端（需要访问办公网敏感数据的终端，或者对移动终端有明确要求，只能工作专用不能上互联网的终端），必须从技术上保证专机专用，使用定制终端，禁止安装第三方软件。

（2）安全准入

智能终端必须设定开机密码和锁屏密码，必须设置合理的自动锁屏时间，访问敏感数据的应用程序（APP）必须设定独立的访问密码。可通过移动终端安全管理系统策略进行检查和报警。

（3）加密数据

为避免非授权用户接触到智能终端后导致数据泄露，所有工作数据需加密，访问敏感数据的应用程序不得将敏感数据长时间驻留本地。敏感数据不落地，强制用户在线模式下打开敏感数据，保持对敏感数据访问的在线监控；非敏感数据加密存储。

（4）应用沙箱

用户安装第三方程序可能为终端系统带来病毒和风险，必须有可控手段在用户安装第三方程序之后仍能对终端系统进行保护。通过移动终端安全管理系统启用应用级沙箱，监控和管理应用程序之间互相调用的行为，并针对可疑的病毒行为进行处置和报警。

（5）远程擦拭

一旦终端设备丢失，可从管理端对终端设备进行有条件的数据擦拭。可通过移动终端安全管理系统的远程擦除数据功能实现。

4.3　应用安全设计

4.3.1　身份鉴别

移动办公系统严格限制非法人员的使用，保证只有经过授权的人员才可以访问应用系统，采用的措施为：统一用户身份管理和统一认证与授权管理。在移动终端的操作入口提供专用的登录模块对登录用户进行身份识别。如果登录失败，结束当前会话并自动退出；多次登录不成功，锁定该用户帐号，以限制非法登录。

4.3.2　访问控制

移动办公系统提供访问控制功能，依据安全策略控制用户对系统功能和数据的访问。系统通过权限配置限制每个用户的访问权限，严格限制默认帐户的访问权限，为不同调度岗位制定其承担任务所需的最小权限，确保应用访问安全。

4.3.3　剩余信息保护

移动办公系统在完成一次对数据库访问后，及时清除此次访问中操作会话记录占用的系统内存、硬盘等存储空间，防止被恶意利用。

4.3.4　数据的完整性、保密性和不可抵赖性

移动办公系统与其他系统间通信使用数字证书。所有的通信过程发送前都必须使用数字证书对数据进行安全校验和签名。接收端在接收到数据后，使用对应的数字证书对签名进行验证，保证了通信过程中数据的完整性。对于敏感信息，在通信过程中对相关字段进行加密。

4.3.5　软件容错

移动办公系统提供数据有效性检验功能，保证通过平板输入或通过通信接口输入的数据格式或长度符合系统设定要求。

4.3.6　资源控制

为保证移动终端在使用过程中的应用和数据安全，应用系统通信双方在一段时间内如果一方未作任何响应，另一方将自动结束会话，系统退出。移动办公系统设置最大并发会话连接数并进行限制。

4.4　主机安全设计

4.4.1　用户管理

对登录服务器操作系统和数据库的用户，都会为其创建独立的帐户，并且分配到相应的用户组，设置相应的登录路径和操作权限。过期帐户，将会及时在系统中删除。

4.4.2　访问控制

不同身份用户，将分配不同的读写权限，并且仅授予其最小访问权限。远程登录服务器，仅允许加密的连接方式如 SSH，禁止 Telnet 登录。此外，root

用户无法直接登录，必须通过普通帐号跳转。

4.4.3 主机监控

针对主机故障监控，采用自主研发的ITSM信息服务管理系统。该系统集监控和管理于一体，能够实时监控服务器、存储、网络设备、数据库、中间件和应用系统的状态，发现问题及时报警；同时以ITIL理念为指导，将事件管理、变更管理和维修管理融为一体，实现故障从发生到关闭全闭环管理，有效地提高了应用系统的安全性。

4.4.4 可靠性保障

服务器采用集群部署方式，当主用服务器出现故障时，应用可以自动切换至备用服务器上运行，实现应用访问不中断，有效地提高了系统的可靠性和可用性。

4.4.5 安全审计

所有服务器均采用单点登录系统（堡垒机）进行管理。每个运维人员都会为其在堡垒机上创建一个唯一账户。运维人员只有先登录堡垒机，然后才能跳转到被管的服务器上进行各种维护操作，无法直接登录机器。该系统能够完整地记录下所有登录用户的操作内容，便于日后审计。

4.5 数据安全

数据是企业的重要资产，保证数据的安全至关重要。移动办公系统的数据安全保障方案主要通过以下技术实现。

4.5.1 集中式数据库管理系统

应用系统中重要的数据都是通过数据库管理系统来集中管理。数据库系统部署在高可用的小型机上，由专业的数据库管理员进行维护和管理，数据访问都遵循严格的访问控制机制，有效地确保了数据的安全性和一致性。

4.5.2 双磁盘阵列架构

数据的存储采用双磁盘阵列架构，即所有数据都同时存入两台磁盘阵列中，数据保存两份，当有一台存储出现故障无法访问时，另一台存储可以支撑应用正常运行，不会出现应用访问中断或数据丢失。

4.5.3 数据备份机制

数据库的数据都会被定期备份到磁带库中，用于数据的恢复和长期保留。备份数据库时，通过制定合理的增量及全备份策略，将数据库数据备份至虚拟磁带库中，当发生数据丢失或数据库异常情况时，可以通过备份管理软件将丢失的数据从虚拟磁带库恢复出来。

4.6 物理安全设计

移动办公系统设备部署的机房要求专门人员7×24 h值守、监控、巡视。机房各关键地点均有摄像头进行实时监控。机房符合防雷击、防火、防水防潮、防静电、温湿度控制的要求。采用不间断供电系统（UPS），达到等级保护对供电系统的要求。设备采用双路供电。进行电磁防护，对密码机等关键设备和磁介质实施电磁屏蔽。

5 结束语

本文根据铁路信息安全技术架构特点，提出了一种铁路移动办公系统网络安全接入方案。该方案针对铁路移动办公系统网络接入安全风险设计，为铁路移动办公系统网络接入安全防护提供了一种新的方法。

参考文献：

[1] 赵永彬，韦　明，李　巍．电力企业移动办公系统的研究与设计[J]. 电力信息化，2011，9（4）.

[2] 唐全艺，蒲　江，赵　进，周　旋．安全移动办公平台技术研究[J]. 信息安全与技术，2013，4（5）.

[3] 时长江，张柏青，赵　谦，郑　雯．基于智能网络与虚拟化计算的移动办公系统信息安全的研究与应用[J]. 网络安全技术与应用 2014（1）.

[4] 中华人民共和国国家标准 .GB/T22239-2008，信息安全技术－信息系统安全等级保护基本要求[S]. 北京：中国标准出版社，2008.

责任编辑　王　浩