



基于安全管控平台的“金库模式”分析及应用

宁建创, 谭 彬, 梁业裕

(中国移动通信集团广西壮族自治区有限公司网络运营中心 南宁 530022)

摘 要: 为降低高权限账号被滥用引起违规操作和客户信息泄露的风险, 借鉴银行金库管理中开关库房必须由两名管库员在场共同进行的方式, 以多人制衡的手段对高权限的使用进行监督和控制。通过对广西移动网络运营中心“金库模式”的各种应用场景的调查和分析, 对“金库模式”的触发模式、授权模式和工作效率优化进行了分析和实现设计。并在网运中心的语音交换网元、WAP、信令监测等系统进行了成功的实施和应用, 敏感数据查询量显著下降, 有效遏制了权限滥用的情况, 降低了客户敏感信息泄露的风险。

关键词: 金库管理; 应用场景; 触发模式; 授权模式

doi: 10.3969/j.issn.1000-0801.2013.06.029

Treasury Pattern Analysis and Application Based on Security Control Platform

Ning Jianchuang, Tan Bin, Liang Yeyu

(Network Operations Center, China Mobile Group Guangxi Co., Ltd., Nanning 530022, China)

Abstract: In order to reduce illegal operations and customer information disclosure of risk caused by the high privilege account abuse, drawing lessons from the way of the bank vault management in warehouse that must switch consist of two warehouse keepers who jointly conduct the warehouse, high authority for supervision and control was used in many means of checks and balances. Through the investigation and analysis of various application scenarios for Guangxi mobile network operation center treasury management, trigger mode, authorization model and working efficiency optimization of treasury management were analyzed, designed and implemented. And it was successfully implemented and applied in the systems such as voice switching network, WAP and signaling monitoring in network operation center. The results show the query sensitive data volume decrease significantly, and it can effectively curb the abuse of authority of the customer and reduce the risks of disclosure of sensitive information.

Key words: treasury management, application scenarios, trigger mode, approval mode

1 引言

通过获取用户通话记录、用户通话位置信息锁定使用者的位置, 这些在电影大片中才会看到的情节已成为触手可及的现实。在 2010 年 12 月北京市朝阳区法院审理的一起“私家侦探”敲诈勒索案中, 根据检方指控, 这些“私家侦探”非法获取了用户的通话记录和位置信息。这些个人信

息源自某些电信运营商。

这些安全事件很多都与 IT 支撑系统的信息泄露和人员违规操作有关, 由于内部威胁比外部威胁更难发现, 且企业往往对内部人员疏于防范, 导致内部信息安全漏洞百出。“金库模式”在电信运维上的研究和实践, 借鉴了银行业金库管理的成熟管理思维, 并从技术手段上提供了支撑, 对降低 IT 支撑系统的违规业务操作和信息泄露风险

意义重大。

2 现有业务系统存在的信息安全风险

2.1 信息安全的外部威胁和内部威胁

目前,网络信息安全面临的威胁有来自外部攻击的威胁,也有来自内部员工滥用职权的威胁。常见外部的威胁有拒绝服务攻击、信息嗅探、木马、病毒等;而内部员工的威胁主要体现在内部用户或者是曾经的内部用户违反安全规定要求,利用系统脆弱点进行非法的篡改、窥探、越权等行为。

根据 Verizon 公布的 2010 年数据外泄调查报告显示,在所有的数据外泄事件中,48%的事件由内部人员造成,而公司却往往容易忽略来自内部的威胁,信息安全保护措施一般是“防外不防内”。公司的安全策略侧重于保护其信息系统和资产不受外部的入侵者和黑客攻击,几乎所有的系统已经实施了保护其边界的安全工具,包括防火墙、入侵检测、反病毒、反垃圾邮件、反间谍软件和其他工具。而针对内部威胁的安全手段则比较缺乏,大多仅依靠系统自身的鉴权机制。由于内部人员对系统的运作、结构熟悉,导致非法行为不易被发觉,而且内部人员最容易接触敏感信息,危害的往往是公司最核心的数据、资源等,所以急需建立应对内部威胁的技术手段及管理模式。

2.2 现有业务系统的敏感信息情况

网运中心负责移动通信网络运行维护管理工作,其交换网网元设备(包括移动交换中心(mobile switching center, MSC)漫游位置寄存器(vistor location register, VLR)、媒体网关(media gateway, MGW)、归属位置寄存器(home location register, HLR)、无线应用协议网关(wireless application protocol gateway, WAPGW)、充值中心(voucher center, VC))、管理支撑系统上存储了客户的各种敏感信息,包括客户位置信息、通信记录、上网记录等,具体见表 1。

对涉及客户高价值信息的系统资源和应用资源,部分操作人员(内部员工或者系统厂商人员)可能受利益驱使违规获取、篡改相关信息。这些敏感信息的泄露,侵犯了用户个人隐私,并可能被黑色产业链用于商业目的或者恶意使用,对企业形象也会造成负面影响。

3 业务系统维护操作模式

3.1 传统的分散维护模式

传统维护模式示意如图 1 所示。

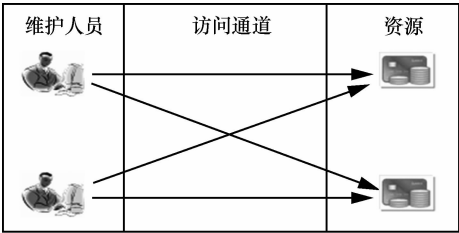


图 1 传统维护模式示意

在传统维护模式下,各个业务系统分散操作,各个维护人员直接登录设备进行操作,主要存在以下信息安全风险。

- 自然人与账号无法对应。由于可能存在账号共用、账号盗用、标识不明确等问题,导致账号与自然无法一一对应,出现信息安全事件时找不到对应责任人。
- 用户操作行为无法有效审计。因网元设备类型不同而日志格式不同以及日志功能完善程度不同,如较多设备无法记录操作日志,则会影响日志审计的完整性、可靠性和可行性。
- 对维护人员无法进行事中控制。由于维护人员拥有的账号权限在事先已经授权,授权后对使用人员是否滥用权限则无法控制,只能靠管理制度进行约束,一旦碰上流氓管理员或管理员准备离职的情况,在利益或报复心理的驱动下,则很可能会发生较大的信息安全问题。

3.2 通过管控平台的集中维护模式

通过管控平台的集中维护模式示意如图 2 所示。

目前,中国移动通信有限公司广西分公司网运中心通过建设安全管控平台(4A 系统),实现了用户生命周期管理、资源从账号管理、集中授权管理、集中接入、单点登录和日志审计管理。大大降低了账号口令管理方面的风险,确保用户权限最小化,通过集中的操作维护通道,将自然人与设备账号一一对应并记录操作日志,对潜在违规用户形成了有效威慑。

通过管控平台的集中维护模式解决了传统维护模式

表 1 敏感数据分布情况

系统	MSC/VLR/ MGW	HLR	WAP 网关	VC	信令监测系统
敏感信息	客户位置信息	客户位置信息	上网记录	充值卡信息	客户位置信息通信记录

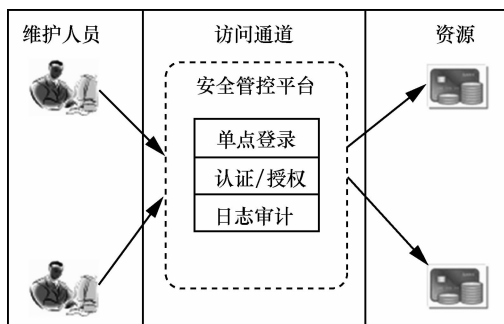


图2 通过管控平台的集中维护模式示意

中存在的自然人与账号无法对应以及用户操作行为无法有效审计的问题,是防范内部威胁的有效手段,但对维护人员无法进行事中控制的问题仍未能有效解决。

3.3 应用“金库模式”的集中维护模式

“金库模式”是一种“双人操作”或“多人操作”模式,对于涉及到高价值信息、敏感信息的高风险操作,强制要求必须由两个或两个以上有相应权限的员工共同协作完成操作,通过相互监督、利益制约确保关键操作的安全性。金库模式场景过程示意如图3所示。

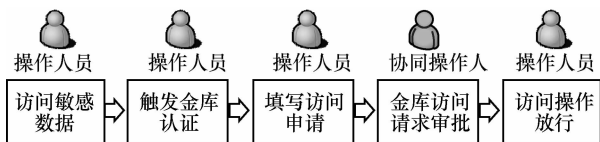


图3 “金库模式”场景过程示意

“金库模式”技术实现是在操作人员对敏感数据进行访问的过程中,增加了金库认证触发、申请和审批的环节,通过协调操作人的监督和制衡左右,在技术上保证一个人不可能独自完成高敏感操作。“金库模式”实现了对掌握高权限的人员的“事中控制”,也遏制了滥用权限行为的发生,是应对内部安全威胁的一种有效手段。

由于“金库模式”在用户访问操作过程中增加了协作制衡措施——即敏感操作审批环节,必然对现有运维工作的效率有所影响。因此,在“金库模式”应用获得安全性目标的同时,需要确保不影响正常运维工作的开展,并兼顾访问操作的效率。

金库管理维护模式示意如图4所示。

为了降低账号权限滥用、信息泄漏的内部风险,仅靠事后的稽核或日志审计是不够的,加强“事中控制”非常必要。而“金库模式”通过登录敏感系统或进行敏感操作时触发金库审批,需要审批人同意才可继续进行登录或操作。“金库模式”多人制衡的方式对高权限的使用进行了监督和控制,

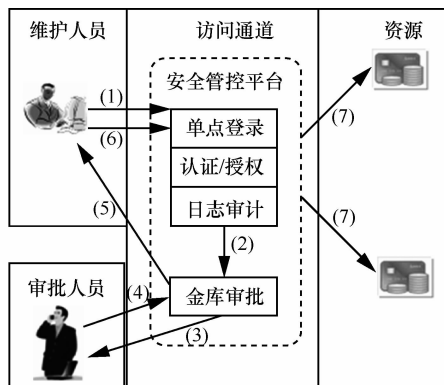


图4 金库管理维护模式示意

避免由于高权限账号被滥用而引起违规操作产生的严重影响。因此引入“金库模式”能够增强信息安全监管的“事中控制”能力,弥补了现有维护模式对“事中控制”的不足。

4 “金库模式”功能设计及实现

安全管控平台提供了集中的维护通道,只需要在通道上进行控制就能达到金库管理的目标,且能够大大降低“金库模式”的实现难度,因此本文把“金库模式”作为安全管控平台的一个独立功能模块进行设计实现。从图3中可以看到,“金库模式”场景过程中有两个关键的节点。

- “金库模式”触发:即在什么情况(如登录资源、执行敏感操作)下触发金库模式。
- 金库授权审批:即协同操作人(审批人)在不同的工作状态下,如何确保审批工作不影响运维工作的开展和效率。

4.1 金库触发模式设计

“金库模式”的触发可以在以下两个环节实现。

- 从账号登录环节:在具有敏感操作权限的从账号登录时,触发金库审批。
- 敏感操作执行环节:在执行具体敏感操作或者菜单时,触发金库审批。

基于上述场景的分析,金库触发模式分为基于账号登录触发和基于业务操作触发两种。

4.1.1 基于账号登录触发

基于账号登录触发方式是指当拥有敏感操作权限的账号通过安全管控平台登录时,触发金库审批。

此触发方式容易实现,不需要对资源进行改造,只需要对单点登录过程做少量改造即可实现金库触发。但触发的粒度较粗,在用户登录后,其具体执行的敏感操作过程不受控制。

为了降低不必要的金库认证触发量,对于支持基于特定操作授权的网元设备或者应用系统,仅将敏感操作权限(如位置信息查询操作权限)赋予个别特权账号,特权账号在安全管控平台单点登录时触发金库审批。

4.1.2 基于业务操作触发

基于业务操作(命令)的触发方式是指当用户对敏感信息进行高风险操作时,触发“金库模式”。这是一种细粒度的触发模式,只在用户执行敏感操作时触发,操作过程完全受控。

针对不同的客户端访问方式,主要分为如下两种类型。

(1)基于图形界面访问触发

对通过图形界面访问敏感数据的操作,通过进行应用系统改造,在每个敏感操作菜单/按钮增加“金库模式”控制点。当对应敏感操作的菜单或按钮被点击时,触发金库审批。

(2)基于命令行访问触发

对通过命令行访问敏感数据的操作,在安全管控平台的堡垒主机中增加“金库模式”控制点,提供指令鉴权功能。当敏感指令执行时,触发金库审批。

4.1.3 金库触发模式实现

通过对基于从账号登录触发和基于业务操作触发两种模式的分析,其优缺点对比分析见表2。

基于账号登录触发实现流程如图5所示。

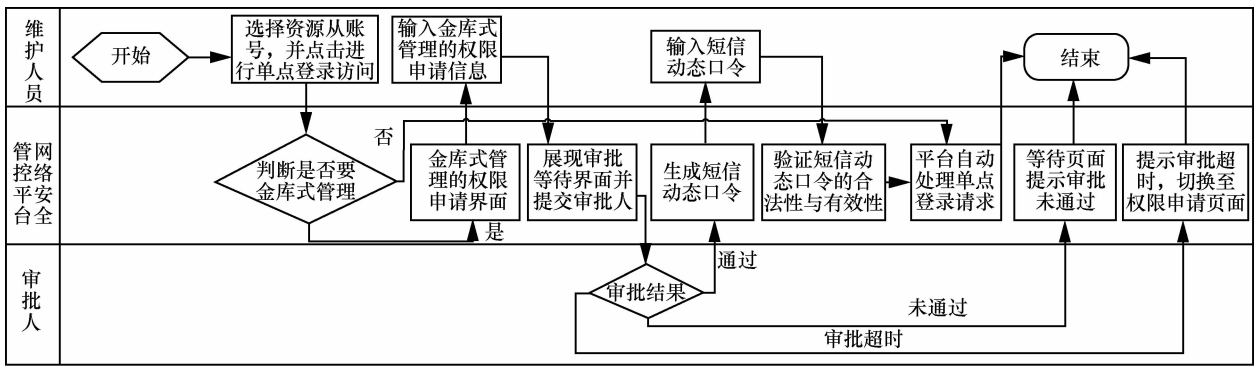


图5 基于账号登录触发金库

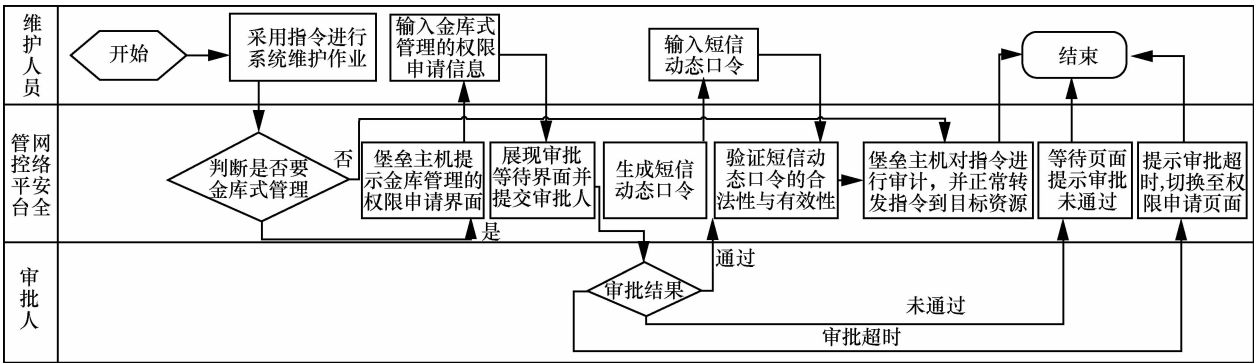


图6 基于业务操作(命令)触发金库

表2 金库触发模式分析对比

触发模式	改造量	实现难度	触发粒度	触发量
基于账号登录触发	小	小	粗	较实际操作量偏大
基于业务操作触发	大	大	细	与实际操作量一致

基于业务操作(命令)触发流程如图6所示。

4.2 金库授权模式设计

根据协同操作人的不同工作状态,金库模式授权方式分为人工授权和自动授权两种方式。

4.2.1 人工授权模式分析

根据金库模式应用场景分析,人工授权模式细分为如下两种授权模式。

(1)现场授权

现场授权模式需要协同操作人员在现场,通过现场输入主账号密码、插入硬件证书、提供当前动态令牌码或按指纹等完成实时授权。其中,操作人员与协同操作人员的对应关系需要在4A的金库管理模块上维护,并由4A提供主账号密码认证鉴权服务或相应其他强认证服务。

现场授权模式适合用于客服人员的应用场景,客服人员的协同操作人员可以是操作人员主管领导、值班经理、班组长、营业厅班长或其他授权协同人员。现场授权模式



的使用流程设计如图 7 所示。

(2) 远程授权

远程授权采用短信方式,协同操作人员通过回复短信完成授权。“金库模式”触发后,安全管控平台向协同操作人员发送申请短信,短信内容包含操作员账号、操作类型、操作对象、操作原因等信息。授权人员回复审批结果后,安全管控平台根据审批结果反馈操作人员,操作人员根据审

核结果继续或终止本次操作。其中,操作人与协同操作人员的对应关系在安全管控平台金库管理模块中维护,安全管控平台认证中心提供授权码验证服务。

远程授权模式适合用于运维人员的应用场景,协同操作人员可以是专业系统管理员双人互为协同操作人,或者由专业系统管理员的直属领导担任协同操作人。

远程授权模式的使用流程设计如图 8 所示。

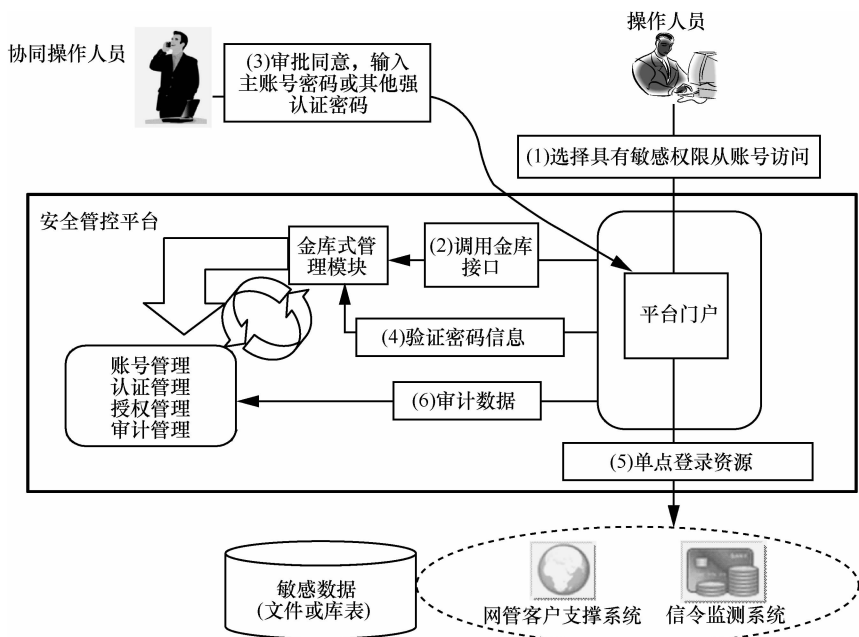


图 7 现场授权模式使用流程示意

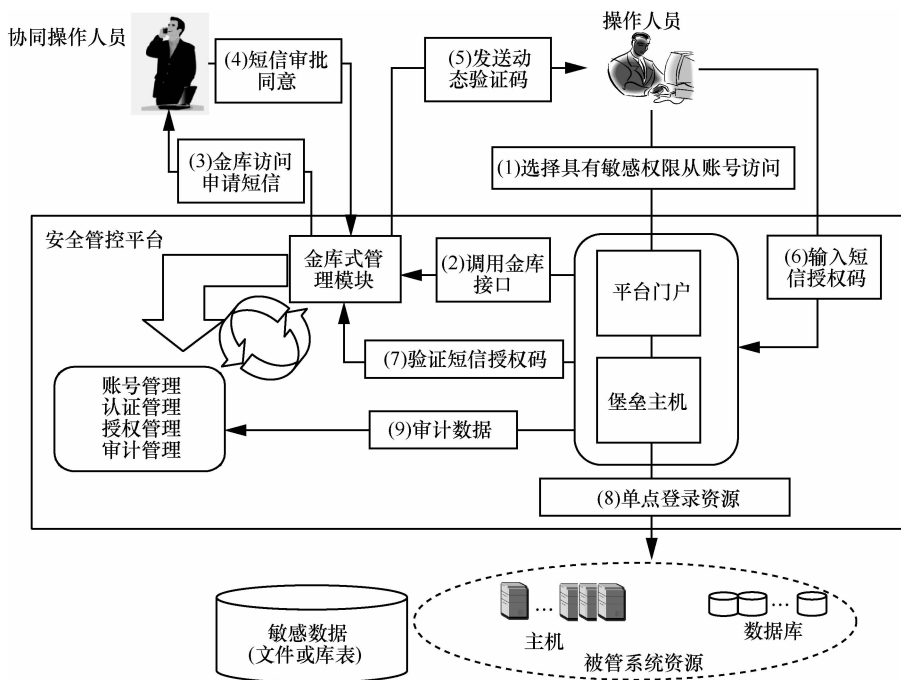


图 8 远程授权模式使用流程示意

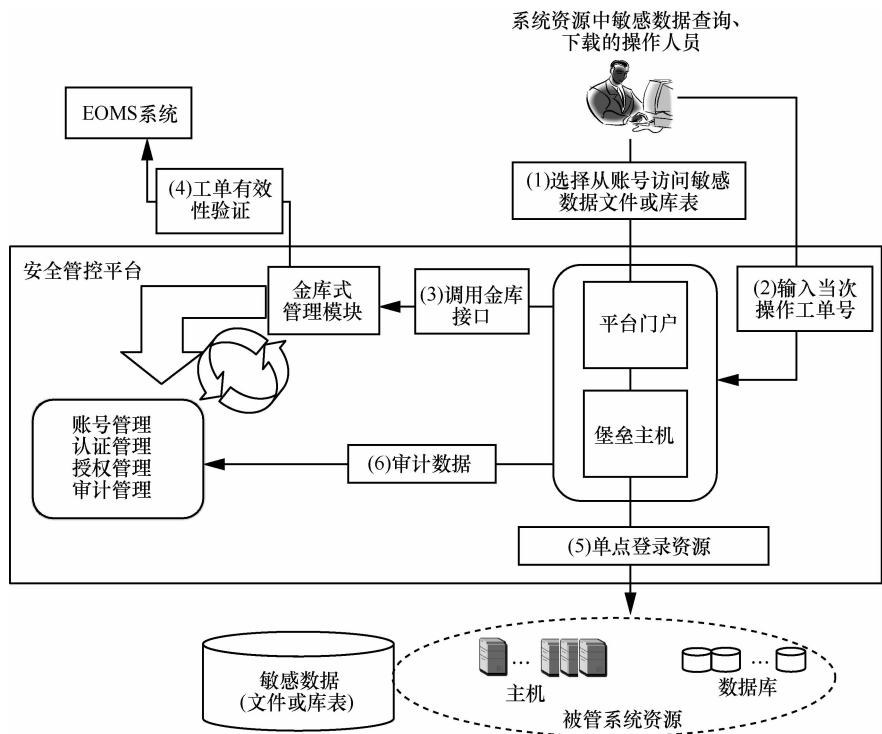


图 9 自动授权模式使用流程示意

4.2.2 自动授权模式

自动授权方式是指金库模式触发后,操作员输入本次操作的工单号,金库管理模块自动与工单系统进行联动,调用工单系统的查询接口,并根据返回信息解析、存储详细工单信息,包括操作人信息、访问时间范围等信息。根据比对结果,继续或终止本次操作。

自动授权模式的使用流程设计如图 9 所示。

4.2.3 金库授权模式比较

通过对人工授权模式和自动授权模式的分析,其优缺点对比分析见表 3。

表 3 金库授权模式分析对比

授权模式	是否涉及第三方改造	实现难度	准确度
人工授权	不涉及	低	高
自动授权	涉及 EOMS 改造	较大	较低

综合实现效果和技术实现难度,金库授权模式采用人工授权方式,同时因应不同的场景采用不同的人工授权方式。两种人工授权模式具体介绍如下。

- 现场授权模式:协同操作人员在现场通过现场输入主账号密码完成实时授权,适用于客服人员的应用场景。
- 远程授权模式:协同操作人员通过回复短信完成授权,适用于运维人员的应用场景。

5 “金库模式”应用效果

聚焦关键系统、高风险操作和高价值信息,通过金库管理模块的部署和推广实施,把如下系统敏感资源的访问纳入金库管理范围。

- MSC/VLR/MGW、HLR、WAP 网关、VC、MISC:共 2 991 个敏感权限从账号;
- 信令监测系统:118 个敏感权限从账号;
- 网络安全管控平台:5 个敏感权限从账号。

通过金库管理,每个敏感账号进行敏感操作前都需要审批人进行审批,实现了“事中控制”,并将每次审批记录详细记录,易于进行日志审计。

随着“金库模式”的推广应用,目前每周金库审批数达到 200 次/周,敏感数据查询量下降 46%,有效抑制了权限滥用的情况。具体各个业务系统敏感信息的月度查询量在“金库模式”应用前后的变化如图 10 所示。

备注:应用前的访问量为取样自“金库模式”应用前 1 个月的查询量;应用后的访问量为取样自“金库模式”应用后 1 个月的查询量。

6 结束语

本文分析了现有维护模式在“事中控制”方面的不足,

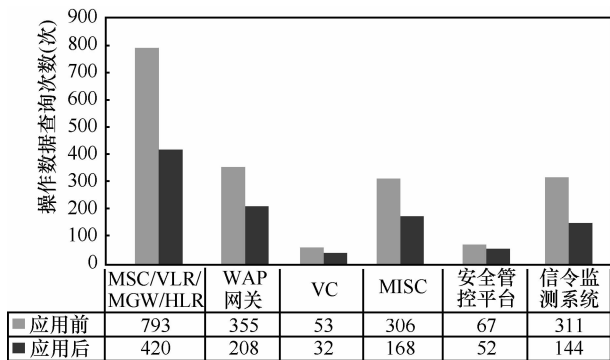


图 10 “金库模式”实施前后敏感数据查询量对比

并结合网运中心的业务特点,设计了金库管理的触发模式

和授权模式,依托“金库模式”管理,以多人相互制衡的方式对高权限的使用进行监督和控制,使金库管理达到了“事中控制”,降低了敏感信息泄露风险,提高了信息安全管理水平。

参考文献

- 1 李京华,公磊.移动联通内部员工出卖用户信息催生侦探产业链.经济参考报,2010-12-31
- 2 工银发[1996]36号.中国工商银行金库管理规定,1996
- 3 贺东.计算机系统内部威胁检测技术研究. <http://www.doc88.com>, 2009

(收稿日期:2013-05-29)

(上接第 169 页)

参考文献

- 1 YD/T 1193.2-2002. 与承载无关的呼叫控制(BICC)规范——第 2 部分: BICC 的消息、参数的基本功能和格式, 2002
- 2 ITU-T Q.1902.2. Bearer Independent Call Control Protocol (CS2) and Signaling System No 7-ISDN User Part General Functions of Messages and Parameters, 1902
- 3 3GPP Q.1902.3. Bearer Independent Call Control Protocol (CS2) and Signaling System No 7-ISDN User Part Formats and Codes, 1902
- 4 3GPP Q.1902.4. Bearer Independent Call Control Protocol, Basic Call Procedures, 1902
- 5 3GPP Q.764. Signaling System No 7-ISDN User Part Signaling Procedures, 1999

- 6 3GPP TS 48.008. Mobile Switching Centre-Base Station System (MSC-BSS) Interface; Layer 3 Specification, 2012
- 7 3GPP TS 48.002. Base Station System-Mobile-Services Switching Centre (BSS-MSC) Interface; Interface Principles, 2012
- 8 3GPP TS 24.008 V4.2.0 (2001-03). Technical Specification 3rd Generation Partnership Project; Technical Specification Group Core Network; Mobile Radio Interface Layer 3 Specification; Core Network Protocols-Stage 3 (Release 4), 2001

[作者简介]

陈翠玲,女,中国移动通信集团福建有限公司网管中心交换室工程师,主要从事交换核心网的规划、优化以及维护工作。

(收稿日期:2013-05-30)

· 简讯 ·

2013 年 4 月通信业主要指标完成情况(二)

指标名称	单位	本月末到达	比上年末净增	本月净增
固定电话用户合计	万户	27 519.3	-296.0	-121.3
公用电话用户	万部	2 305.7	-41.4	-11.1
城市电话用户	万户	18 811.2	-82.2	-62.4
住宅电话用户	万户	10 855.0	-158.2	-58.4
农村电话用户	万户	8 708.1	-213.7	-58.9
住宅电话用户	万户	7 094.1	-214.7	-59.0
移动电话用户合计	万户	115 512.5	4 297.0	940.4
其中:3G 用户	万户	28 874.3	5 593.9	1 147.6
互联网拨号用户	万户	563.4	-6.4	-5.9
互联网宽带接入用户	万户	17 787.8	802.5	135.9
其中:xDSL 用户	万户	11 419.1	-472.0	-62.9
移动互联网用户	万户	80 765.1	4 328.6	-974.2
固定电话普及率	部/百人	20.5		
移动电话普及率	部/百人	84.9		

注:互联网宽带接入用户、xDSL 用户等指标自本月起统计调整,比上年末净增、本月净增按同比口径计算。

(来源:工业和信息化部运行局)