



电信运营商安全审计系统小概率关联分析技术探讨

郭 健, 沈 杰

(中国移动通信集团山西有限公司 太原 030000)

摘 要:通过分析电信运营商业务支撑系统安全审计软件关联分析技术的重要性和困难性,提出了小概率关联分析的解决思路,阐述了小概率关联分析模型的原理、设计方法、实现步骤和实际效果。

关键词:安全审计;关联分析;小概率分析

doi: 10.3969/j.issn.1000-0801.2013.04.026

Discussion on Small Probability Correlation Analysis Technique of Security Audit System for Telecom Operator

Guo Jian, Shen Jie

(China Mobile Group Shanxi Co., Ltd., Taiyuan 030000, China)

Abstract: The importance and difficulties of security audit software correlation analysis technique of business support system (BSS) for telecom operator was analyzed, and then solutions for small probability correlation analysis were proposed. Finally the model principle of small probability correlation analysis, design method, implementation steps and actual effects were described.

Key words: security audit, correlation analysis, small probability analysis

1 引言

安全审计是一种根据一定的安全策略记录,分析历史操作事件及数据,及时发现系统中存在的违规操作和安全漏洞的信息安全保护技术。电信运营商业务支撑系统的安全审计平台通过采集、记录、管理、分析用户对业务支撑系统高敏感度(非常重要和重要)数据的关键操作,对人员的登录过程、关键操作等行为进行审计和分析,最终建立并完善针对“自然人→资源”访问过程的完整审计管理,实现安全事件实时告警和安全事故责任追踪。

2 关联分析的重要性和困难性

在业务支撑系统中,安全审计系统通过有效的审计分析手段和方法,检查、发现并预警各种异常和违规行为。在

信息安全领域审计系统中,关联是指将系统中所有的事件,按照相关性综合到一起进行观察;分析是核心功能和关键技术。关联分析是指对网络或系统全局的安全事件数据进行自动、连续分析,通过特征对业务场景操作流的上下文进行关联,根据用户定义的、可配置的规则识别具有威胁、复杂的攻击模式,从而确定安全事件的真实性,对事件进行分级并对事件进行有效响应。关联分析是与实际业务操作贴合紧密并且具有一定智能程度的分析手段,可以用来提高安全审计的可靠性、效率以及可视化程度,并为安全管理和应急响应提供技术手段。如违规创建账号后,利用该账号执行业务操作的行为;又如将用户敏感数据导出为主机文件后,对该文件的下载行为等。

在关联分析中,关注的日志范围涉及业务日志的各个层面。山西省审计软件上线后,每天产生的日志量多



达 2 GB, 在这数量庞大的日志中进行关联分析变得非常困难。

(1) 分析性能很难有效保证

一次简单的关联就需要对海量日志中的每一条进行交叉遍历, 不仅分析耗时长, 对系统资源占用大, 而且容易出错。

(2) 分析策略很难制定

业务是不断发展的, 分析的策略也需要不断改变, 但审计管理员很难对每个系统的业务流程都足够熟悉, 这增加了审计落地的难度。需要研究一种智能关联分析技术解决以上问题。

3 小概率分析模型的原理

在实际使用审计系统过程中发现, 违规操作和异常行为只占海量日志中的很小部分。通过对这类小概率事件进行深入挖掘, 回溯此类事件的产生场景、操作过程和特征, 建立知识库, 形成系统自学习的智能分析体系。

小概率模型基于如下假设: 合法的日常操作是多数的, 非法的操作是少数的, 某种操作行为的数量非常少, 以至于低于某个阈值时, 就有可能是非法的。所以小概率分析模型可以找出数量低于特定阈值的操作行为。

在如上假设的基础上, 先统计过去发生的操作记录的执行次数。操作记录由操作(operation)、参数(option)、对象(object)三者组合而成, 简称 3O。每次操作就是 operation 与 option 和/或 object 的任意组合, 即把统计结果与事先给定的违规阈值(illegal threshold)进行比较, 如果发生次数小于等于该阈值, 则认为该操作记录是一条疑似违规记录, 把这条疑似违规操作放入疑似违规操作表 sus_violation_record 中, 这个阶段称为“查找”。

得到“疑似违规操作记录库”后, 用每个操作对应的 session ID(一次会话的唯一标识)回溯在此操作之前所有相关的操作集合, 如所在 session 里所有的操作记录、user 在这给定时间段内的操作记录、所在 IP 主机的操作记录等。这样就得到了若干疑似违规操作流, 这个阶段称为“回溯”。

得到疑似违规操作流后, 对于不在违规操作库中的记录, 需要由安全专家确认是否为真正的违规操作。如果是, 则保存到违规操作表 violation_record 中; 如果不是, 则丢弃。这个阶段称为“确认”。

如果疑似违规操作已在表 violation_record 中, 则自动增

加其发生次数; 对于不在表 violation_record 中的记录, 用户确认的添加到表中, 没确认的丢弃, 这个过程称为“修改”。

小概率分析模型的执行过程由查找、回溯、确认、修改 4 个阶段组成。

4 小概率分析服务程序的组成

小概率分析是软件系统的一种自学习行为, 需要用户事先设定关联分析策略及违规阈值和回溯时间范围, 在知识库建立的初始阶段需要管理员参与完成分析和知识积累。小概率分析服务程序分为 4 个子模块: 统计、回溯、确认、监控。

(1) 统计

统计指定的时间段内日志中所有操作发生的次数, 并从小到大进行排序, 然后根据管理员指定的关联分析策略中的阈值筛选出疑似违规操作, 最后将疑似违规操作的具体信息保存到疑似违规数据表中。

(2) 回溯

得到疑似违规操作库后, 由管理员判断是否需要回溯。根据该疑似违规操作对应的时间、用户名等字段进行回溯, 回溯结束后得到若干个违规操作流。如假设违规阈值是 3, 操作 create user(创建用户)的发生次数是 2, 则 create user 操作为疑似违规操作, 用户对该操作进行回溯得到两个操作流, 然后进入操作流确认模块。

(3) 确认

确认工作需要经验丰富的业务系统管理员参与完成, 管理员根据经验判断操作流是否为违规的操作过程。确认结束后得到两类操作流: 一类是违规操作流, 另一类是安全操作流。在确认过程中, 完整的操作流有可能会很长, 特别是设定的回溯时间段比较长时, 需要对日志流进行归并处理, 或者过滤掉安全的操作, 如 'cd ./' 和 'ls', 再展现给用户进行确认, 从而减少了用户参与的难度, 提高了操作流的质量。

(4) 监控

使用违规操作流对用户的操作过程进行监控, 用违规操作库中的操作流对用户的操作过程进行实时匹配。匹配程度比较高便认为用户正在进行危险的操作, 生成相关的告警信息。

5 小概率分析模型设计

小概率分析模型的实现步骤分为 4 个阶段: 查找、回

溯、确认、修改。下面就第一次运行和例行运行两种情况通过“以脚本方式导出 DB2 数据库表到主机文件”为例,介绍小概率分析模型的设计过程。

5.1 查找

(1)第一次查找

分析审计数据库中的所有操作记录,首先从表中取出一条记录详情 (30),对 30 进行预处理 (去掉 operation、option、object 三者之间多余的空格),用表 map 保存统计结果,用 30 做这条记录的主键,记录发生次数,并在表 operation_session 中记录主键及每一次的执行所在的 user_session_ID。对于不存在的主键,添加到表 map 中,并将发生次数置 1,并在表 operation_session 中记录主键及每一次执行所在的 user_session_ID。得到所有操作记录的统计结果后,发生次数小于阈值的操作被认为是疑似违规操作,把这些疑似违规操作放入表 violation_record 中。

为了避免查找过程的发生日期重叠,需要记录下本次查找所跨越的时间范围。因为操作日志表名一般以日期命名,查找结束后,将查找的第一个与最后一个表的表名作为起始时间戳和结束时间戳,以此来标识该次查找跨越的时间范围,下一次查找只能从上次查找结束时间戳的下一个表开始查找。

统计得到疑似违规操作表后,循环遍历所有操作记录进行回溯。

(2)例行性查找

系统例行每天查找一次,即当天查找昨天的日志记录,称为例行查找。例行查找过程中对操作记录进行统计,方法与系统第一次运行时统计过程一样,唯一不同之处是过滤疑似违规操作时参考例行查找阈值。利用例行查找阈值过滤得到疑似违规操作表,紧接着对疑似违规操作表进行回溯。

5.2 回溯

遍历疑似违规操作表,读取一条疑似违规操作 A,取得与记录 A 对应的所有 user_session_ID;因为统计的是一段时间内的操作,重复操作每一次执行时对应的 user_session_ID 不同,为方便回溯,记录下每次执行时记录 A 所在的 user_session_ID;对每一个 user_session_ID 做一次回溯。如对于 A_session_ID_1,查找到与 A_session_ID_1 对应的相关信息 (如 user name、IP、date and time),利用这些相关的信息进行回溯。

回溯原则如下所述。

(1)第一次回溯

在查找阶段所对应的操作记录中进行回溯,分析 A_session_ID_1 的所有操作,寻找该用户在 A 之前 (包含记录 A)所有的操作。

(2)例行性回溯

在例行查找所对应的操作记录内,回溯 A_session_ID_1 对应的 user,分析该用户在 A 之前 (包含 A)执行的所有操作。

重复回溯完记录 A 对应的所有 user_session_ID 后,记录 A 回溯结束,可以得到一个记录所对应的若干个操作流。接着遍历回溯下一条记录 B。回溯遍历结束后,便得到了疑似违规操作流。将所有的疑似违规操作流保存到表 T_NEED_CONFIREDD_****_**_** 中,供管理员做进一步确认。

5.3 确认

第一次确认和例行性确认的过程相同,都是逐行分析表 T_NEED_CONFIREDD_****_**_**。例如,需要管理员确认的操作流见表 1。

表 1 需要管理员确认的操作流

session_ID	operate_ID	operate_record
19497	1262237169814	su ipd
19497	1262237169819	ipd
19497	1262237169826	cd d/db2home/mk
19497	1262237169829	cd proghome
19497	1262237169844	cd bin
19497	1262237169865	ls E*
19497	1262237169882	Execstepsql cd ../log

5.4 修改

疑似违规操作经确认后成为违规操作,进入表 violation_record 中。表 violation_record 中的操作经确认为非违规操作,则从表 violation_record 中剔除。

6 小概率关联分析模型技术特点和上线使用效果

- 安全审计系统小概率分析模型技术具有以下特点。
- 不仅提高了关联分析的准确性,而且审计分析的内容与山西省实际业务紧密贴合。
 - 建立了智能的自学习系统和完善的知识库,审计管理员不需要进行大量的策略配置工作,也不需要每一个业务都非常熟悉。



- 提高了审计系统关联分析的效率,使审计工作实时化、常态化。

安全审计系统小概率分析模型上线使用一段时间后,初步建立了分析知识库,审计管理员配置策略的工作强度大大降低,系统能自动进行常用的关联分析,包括只查询不办理、金库场景等,审计内容与日常业务生产贴合更紧密。

例如,针对只查询不办理场景,能够深入分析、核实、查证各种异常与违规操作的行为。包括应用资源的客户资源查询、业务关键操作等,包括缴费(充值)管理、异地缴费业务、开/过户、订购变更、营业停/复机、积分兑换、补/换卡等内容。审计工作不完全依赖于 CRM 管理员,审计管理员也可以通过审计系统对相关业务操作进行直观的管理,比如,对于一手机号在非正常工作时间进行业务查询后,第二天又进行了补/换卡操作,审计系统在 30 min 内就能产生告警信息,并且告警信息准确不需要经过 CRM 管理员和审计管理员反复确认,也不会对审计系统的性能造成太大影响。而在此功能没有上线前,因为需要审计的操作数据量很大,在审计中发现违规操作十分困难;同时,审计系统需要定期执行计划任务,核查时间依赖于任务的触发周期,实时性很难保证。

总之,应用小概率分析模型技术极大地提高了安全审计系统的智能关联分析功能,有利于安全事件的实时告警和安全事故的责任追踪,提高了 IT 安全管理水平和效率。

参考文献

- 1 中国移动通信集团公司. 中国移动业务支撑网 4A 安全技术规范 2.0, 2010
- 2 中国移动通信集团公司. 中国移动业务支撑网数据安全管理办法, 2011
- 3 刘必雄, 杨泽明, 吴焕等. 基于集群的多源日志综合审计系统. 计算机应用, 2008, 28(2)
- 4 邓小榕, 陈龙, 王国胤. 安全审计数据的综合审计分析方法. 重庆邮电学院学报(自然科学版), 2005, 17(5)
- 5 韩正平, 蔡凤娟, 许榕生. 网络安全信息关联分析技术与应用. 计算机应用研究, 2006(10)

[作者简介]

郭健, 女, 中国移动通信集团山西有限公司工程师, 主要研究方向为支撑网。

沈杰, 男, 中国移动通信集团山西有限公司工程师, 主要研究方向为支撑网。

(收稿日期: 2013-03-15)

(上接第 136 页)

机下沉覆盖, 实现快速宽带接入和业务控制能力; 提升 CMNet 城域网汇聚层端口汇聚, 实现快速转发; 渐进式推进核心路由器集群或新建核心节点, 优化路由性能; 优化 WLAN AP 承载方案, 节约传输资源, 进而降低城域网综合造价。紧密结合 OTN 等光传输技术, 实现超宽带条件下的快速光层调度。优化方案对提升 CMNet 网络性能、提高宽带业务的竞争能力具有重要意义。方案中还有一些需要深入研究和细化的问题, 如 QoS 实施、IPv6 部署、VPN 实施、LTE 条件下是否进行第二 IP 城域网平面的建设等, 这些课题是下一步的研究方向。

参考文献

- 1 Broadband Forum MR-185. Next Generation Broadband Access White Paper. <http://www.broadband-forum.org>, 2009
- 2 赵慧玲, 徐向辉. 智能管道构建思路探讨. 电信科学, 2011 (3): 7~11
- 3 蔡康, 唐宏. 超宽带城域网架构设计思路 and 关键技术浅析. 电信科学, 2012 (1): 1~6
- 4 彭巍, 唐宏. IP 数据网与光网融合的超宽带网络发展演进. 电

信科学, 2012 (1): 7~11

- 5 倪作廷, 王红梅. IP 网络建设中的传输承载模式研究. 邮电设计技术, 2012 (4): 13~17

[作者简介]



姜全泽, 男, 硕士, 华信邮电咨询设计研究院有限公司工程师, 主要研究方向为移动 IP 网络等。

来志远, 男, 硕士, 中国移动通信集团北京有限公司工程师, 主要研究方向为移动 IP 网络等。

陈方荣, 男, 学士, 华信邮电咨询设计研究院有限公司工程师, 主要研究方向为移动传送网络等。

(收稿日期: 2013-03-15)