基于ITIL模型的动态信任管理研究

沈 思 韩 普 苏新宁

(南京大学信息管理系 南京 210093)

摘 要 ITIL的可信运行框架为信任管理提供了良好的上下文环境,可根据网络行为来实现动态的安全监控。现有的动态信任管理研究主要关注P2P、网格等环境,针对信息化中广泛使用的ITIL模型的改进较少。基于真实的ITIL平台行为监控数据,提出了一种结合行为监控上下文环境的ITIL动态信任管理方法。通过监控上下文环境,计算ITIL中业务随着运行时间变化的信任度改变,并引入IOWA算子进行信任度评估和预测,随后通过计算告警信息中频繁时间段序列来提高信任预测的准确性。通过实例分析表明,该方法可以帮助实现网络故障分析,以及ITIL平台下的服务资源优化。

关键词 ITIL,信任管理,动态访问控制,运维监控

中图法分类号 TP301.6,TP309 **文献标识码** A

Dynamic Trust Management Research Based on ITIL Model

SHEN Si HAN Pu SU Xin-ning

(Department of Information Management, Nanjing University, Nanjing 210093, China)

Abstract The trust running framework of ITIL platform can provide a good context environment for dynamic trust management. Most researches on dynamic access control focus on models of P2P or of grid platform, and few models are used in ITIL platform. We proposed a framework to evaluate the trust of ITIL service based on the monitor performance in ITIL context environment. We calculated the trust value of ITIL service, and used IOWA calculator to help the evaluation and forecast of trust value of ITIL service in different time period. We also mined the frequent sequence in alarm log to improve the accuracy of forecast. Example analysis shows that our method has a good effect on fault analysis and resources optimization under ITIL platform.

Keywords ITIL, Trust management, Dynamic access control, Operation monitor

1 引言

网络监控,是指对网络的运行状态进行监测和控制,使其能够有效、可靠、安全、经济地提供服务。当前,传统的"事后处理"监控方式无法适应大规模和复杂网络的需要。ITIL(Information Technology Infrastructure Library)[1]服务管理标准库,旨在利用信息和通信技术等基础设施,根据业务信息设计、规划和实施IT服务,并在服务的每个环节记录系统中业务相关事件的完整信息,以达到根据不同业务流程动态分配系统资源的目的。ITIL中指定的安全运营管理标准,用于统一管理来自不同安全组件的事件信息,将诸如防火墙、入侵检测系统、身份认证系统等信息安全技术工具和产品纳入到管理平台框架,以解决ITIL服务的安全问题。

ITIL服务的安全问题,不仅包括外部威胁的入侵检测,还包括业务对系统资源的不合理利用造成的安全隐患,以及因此造成的系统运行环境不可信问题。基于身份的认证和权限分配[2],虽可以防范来自系统外部的安全威胁,却无法抵御来自系统内部的安全风险。针对该问题,M. Blaze[3]提出了"信任管理"(trust management)概念。他通过定义描述系统安全场景的策略文件,以及限定关键性操作的信任关系,来实现系统内资源访问控制的授权问题。Policy Maker[4]、Keynote[5]等工具在不同平台下实现了M. Blaze的模型。然而,M. Blaze的模型存在如下两方面的缺陷:一方面,用基于形式化的方法来验证信任关系,应用开发人员需编制复杂格式的安全策略;另一方面,复杂的、动态的信任关系的认证,又需要耗费大量的资源和计算时间。Marsh[6]提出的动态信任管理模型,强调利用信任上下文环境来进行信任计算的技术,更符合开放环境中复杂信任关系表达和计算的需要。该模型需要大量收集和信任关系相关的信息,以作为不同量化输入计算信任关系的相关因素。然后,通过动态的监督和调整计算信任值的变化,设计出针对不同网络环境的信任管理策略。模型在不同环境下的的应用包括用于普适计算的PTM(Pervaive Trust Management)[7]模型、用于网格计算的fuzzy-trust模型[8]和用于P2P计算的EigenTrust模型[9]。国内方面,李小勇[10]提出了一种用于大规模分布式环境的动态信任模型。然而,网络安全环境的多边性和不确定性,阻碍了网络环境实

到稿日期:2011-07-02 返修日期:2011-10-10 本文受863计划项目(2011AA01A206)资助。

沈 思(1983—),女,博士生,助教,主要研究方向为数据挖掘、网络安全,E-mail:sszcgfss@gmail.com;韩 普(1983—),男,博士生,主要研究方向为信息处理、语言学;苏新宁(1955—),男,硕士,博士生导师,主要研究方向为信息处理与检索、知识管理、电子政务等。

时、动态的信任数据采集，设有 FTM 模型实现了原型系统。

目前提出的各种信任模型中，在一个环境下非常适用、合理的信任模型，在另外一个环境下其效率则可能变得低下，甚至导致评估结果的不准确和错误，如 EigenTrust 模型的推荐矩阵法在大规模网络中模型计算效率非常低下。因此，构造信任模型必须考虑应用环境的类型、特点，以及应用环境的规模，才能切实提高应用环境的信任度，使信任评估的结果更加合理准确。同时，基于 ITIL 平台的信任模型研究较少。一方面，国内外的研究更多在 ITIL 各领域平台的建设上[11-14]，关于 ITIL 安全服务领域如何实施仍然没有具体的规范。现有的、成熟的网络安全运营产品又缺乏统一的标准，如 CA 公司的 eTrust 系统[15]关注系统静态日志中系统风险的关联分析，而李小勇[10]更关注系统中网络实体动态行为的监控。另一方面，ITIL 标准要求建设的平台记录完整的系统行为信息，因此可以使用动态信任管理模型来研究 ITIL 平台下的安全问题，同时业务流的动态变化也为系统内部安全监控带来了一系列挑战。

本文基于金智科技提供的 iMAN-IT 运维管理系统作为 ITIL 平台，分析并计算平台中不同业务在资源和设备使用过程中的信任度变化，随后利用序列数据挖掘算法和 IOWA 算子，评估和预测不同时间段业务信任度的动态变化情况。最后提出了基于 ITIL 的访问控制模型，并以网络故障场景为例，验证该模型在动态的业务监控中的良好效果。

2 基于动态信任管理模型的 ITIL 业务监控

通常，信任管理模型主要考虑身份验证和行为验证两方面内容。基于身份的信任，主要关注请求者身份凭证与资源提供者访问策略的一致性检测，又称为客观信任。基于行为的信任通过观察业务实体的行为来决定业务实体的信任度，也称为主观信任。ITIL 标准设计用户登录完成身份验证，在行为验证方面没有统一的标准。根据文献[16]的规范，定义业务行为信任度考察指标如下。

定义 1(直接信任度，Direct Trust Degree，DTD) 本文通过分析 ITIL 安全运营管理记录，量化地计算某业务在一系列计算资源和设备上的信任值变化。

定义 2(间接信任度(Indirect Trust Degree，ITD) 本文通过分析 ITIL 安全事件记录以及告警日志，间接地度量业务信任度的负面变化情况。

定义 3(总体信任度，Overall Trust Degree，OTD) 本文通过计算在某时间段某业务流于某设备的总体评价，来监控和预测该业务对系统整体信任环境的改变情况，其值是通过直接信任度与间接信任度加权得到的。

2.1 直接信任度的采集与计算

ITIL 规范中，安全服务级别协议(SLA)按照规范格式记录了安全服务的内容、时间、关键性能指标、监控等标准。可以基于该标准考察一系列用于监控业务行为的网络性能指标。

内存和 CPU 使用率：通过对内存和 CPU 利用率的监测，可以最大限度地发现潜在的病毒危险。正常使用情况下，内存利用率和 CPU 利用率不会超过某一固定数值，而当有病毒发作等情况出现时，内存利用率和 CPU 利用率可能会升到很高的数值，如超过 90%。

网络端口和消息传送：对网络端口的监测可以发现非法任务引入木马程序后开发的非法端口。但是仅靠端口号是不能确保做出正确判断的，还需配合依附于该端口的进程行为综合判断。

网络流量：拒绝服务攻击和蠕虫病毒发作都会导致网络流量急剧上升。例如当发现某个计算任务非常大量地向外发送相同内容的包，则需要阻止该业务服务的执行，并向相关监测模块提交告警报告。

存储消耗：由于计算代理对于每一个提交业务均分配一定存储空间，业务异常往往会消耗大量的存储空间和进行频繁的 I/O 读写。针对存储消耗的监控和异常判断可以弥补网络流量故障的延时性。

表 1 列出了当前 ITIL 平台中常用设备采集监控的性能参数指标。其中，根据设备运行方式的不同，用主动和被动测量两种方式获取监控数据。

表 1 安全服务中网络性能列表

监控标准 / 设备类型	关键性能指标				测量方式
	CPU 使用率	内存	网络流量	I/O	
服务器			√	√	主动测量
路由器			√		链路检测
交换机	√	√	√		流量检测
主机	√	√			SNMP 轮询

主动测量利用安全工具在所选定的网络端点间进行参数获取，也是一般网络管理员分析网络故障的主要方法。被动测量主要以 SNMP 协议、链路检测、流量检测 3 种方式，周期性地轮询被动监测设备并采集信息。这些信息不仅能够判断网络性能和状态，也符合直接信任度的定义计算要求。基于表 1，定义业务 T 在 t 时刻在设备 d 上的直接信任度为：

$$DTD(T,d,t)=\sum_{i=1}^{n}x_i(t)\times W_i,\ i=1,2,\cdots,n \tag{1}$$

式中，$x_i(t)=(x_{i1},x_{i2},\cdots,x_{in})$ 是设备 d 在 t 时刻的 n 组采样性能指标，W_i 是各指标在监控中所占阈值，且 $\sum_{i-1}^{n}W_i=1$。

例如，中央交换机主要功能是负责包的存储转发，因此设置重要监控指标网络流量阈值最大，可设为 0.5，而内存使用率、CPU 使用率在交换机中重要程度基本相同，阈值可分别设置为 0.25。

以表 2 中的中央交换机 A-centerswitch 性能指标为例，通过式(1)计算业务的直接信任度为：

DTD(A-centerswitch，5/2/2012/00:03)=0.2*0.25+0.57*0.25+34.084*0.5=17.1192

表 2 A-centerswitch 性能指标

CPU 平均使用率	内存使用率	平均吞吐量	采集时间
0.2	0.579999994	34.12377455	2012-2-5 00:03

然而，不同设备的性能指标取值为一定范围内的物理量纲值或者百分比数据，为了正确地按照时间戳顺序计算信任度，需要对原始性能指标进行规范化处理。假设在 t 时刻需要监控业务 i 在 m 组设备上的行为，分别计算业务 i 在各设备中的直接信任度 DTD，得到如下 mXn 阶特征矩阵为：

$$\begin{bmatrix} x_{11}(t),x_{12}(t),\cdots,x_{1n}(t) \\ x_{21}(t),x_{22}(t),\cdots,x_{2n}(t) \\ \cdots\cdots\cdots \\ x_{m1}(t),x_{m2}(t),\cdots,x_{mn}(t) \end{bmatrix} \tag{2}$$

式中，$x_j(t)=(x_{j1}(t),x_{j2}(t),\cdots,x_{jm}(t))$表示 t 时刻设备 j 上对应的表 1 所采集的网络监控指标。若某指标此时不在设备 j 的监控范围内，则用当前监控指标组的平均值代替。利用式(3)对上述矩阵进行规范化处理，最终得到在信任度空间定义的[0,1]范围内并沿着正向递增分布的设备-性能矩阵。

$$b_{ij}=\begin{cases}x_{ij}, x_j \text{ 服从正态分布时}\\ (x_{ij}-\max\limits_{1\leqslant j\leqslant n}\{x_{ij}\})/(\max\limits_{1\leqslant j\leqslant n}\{x_{ij}\}-\min\limits_{1\leqslant j\leqslant n}\{x_{ij}\}), \text{其他}\end{cases} \tag{3}$$

中央交换机 A-centerswitch 在不同时间段对应的网络性能参数列表如图 1 所示，归一化处理后对应的业务 i 的直接信任度值如图 2 所示。

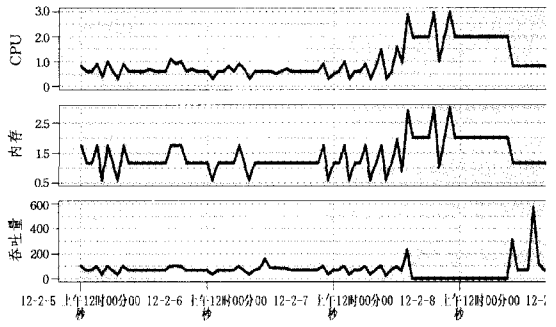

图 1　A-centerswitch 交换机监控指标

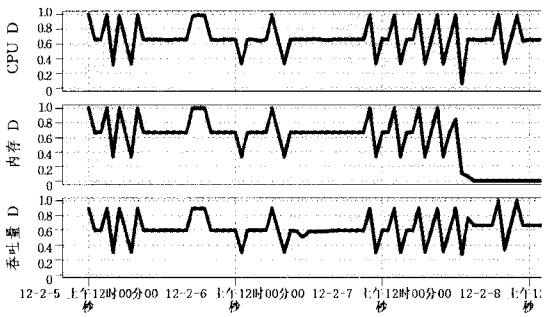

图 2　A-centerswitch 直接信任度变化趋势

从图中可以看出，该设备虽然在 7/2/2012/0:00 监控时指标值没有明显变化，但直接信任度却在该时间点明显降低，同样的趋势发生在 7/2/2012/12:00 前后，下文将详细地分析原因。同时，从总体趋势图可以看出，监控指标变化度越小，则直接信任度值越高，表明该业务运行越稳定。

2.2　基于序列数据分析的信任计算

ITIL 安全事件管理规范，要求监控一切导致或可能导致违背安全运营的方针、服务中断或服务质量下降的有害事件，通过事件管理记录和跟踪所有安全事件或服务请求，并提供相关的问题管理的信息。因此，可以根据事件管理记录来推算业务在设备上的间接信任度，并查找和预测可能降低系统环境安全的业务流。

ITIL 安全事件管理中，根据业务之间的逻辑关系，将相关设备的告警信息生成事件，上报给服务台负责并处理，最后将处理结果反馈给安全事件管理模块。因此在其告警日志中记录着时间连续的、基于设备参数监控的海量信息，为基于动态访问控制模型及计算业务的间接信任度，提供了良好的上下文环境。定义业务 T 于 t 时刻在设备 d 上的间接信任度如式(4)所示。

$$ITD(T,d,t)=(x_1,x_2,\cdots,x_i,\cdots,x_q)\times\gamma_i, i=1,2,\cdots,q \tag{4}$$

式中，$(x_1,x_2,\cdots,x_i,\cdots,x_q)$表示设备中产生了告警信息的关键性能指标，$\gamma_i$ 综合考察了该告警指标的重要程度，一般用 γ_i＝告警次数/告警级别来计算。

告警日志中广泛应用串行 WINEPI[17] 算法，即基于不同长度的时间窗口，根据关联规则算法，按照长度从短到大的顺序，找出告警信息中的频繁情景。该算法需多次扫描日志文件逐步递推地计算频繁情景，直接应用于 ITIL 平台将大量占用计算资源，影响系统性能指标采集的准确性。因此在计算间接信任度时，同时结合 Sagar 提出的一次内存扫描发现频繁关联规则的方法[18] 得到时间段$[t_s,t_e]$下按照时间先后排列的告警关联序列。

根据 iMAN-IT 运维管理系统 5min 一次的系统性能采集周期，分别计算时间段$[t_s,t_e]$中告警事件总次数 N，某一性能指标的告警次数 ec，用 $ec*N/100$ 作为频繁序列情景的置信度，并找出置信度较高的告警时间段。

试考察业务流{考勤，监控}于 7/2/2012/9:00 至 7/2/2012/17:00 时间段，在对应运行设备 Quidway123 和 A-centerswitch 中的监控指标变化情况，如图 3 所示。

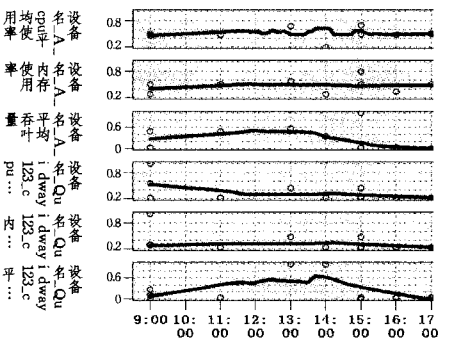

图 3　考勤 & 监控业务流设备监控表

表 3 是根据本文方法计算所得的业务流频繁序列。从表 3 可以看出，虽然(CPU,MEMORY,TRAFFIC)关联规则表明，负责运行考勤业务的中央交换机 A-centerswitch 于14:30 产生 TRAFFIC 严重告警，导致网络流量急剧下降，之前该设备的 CPU 和内存监控值均无异常。然而，从图 3 可以看出，负责监控业务的 Quidway123 设备早在 11:00 左右 CPU 和内存值已急剧降低，同时 12:00 后该设备网络流量激增。结合图 3 和表 3 综合考虑，该业务流{考勤，监控}可能随着执行时间的变化，将不安全因素在两设备间传递。同时，服务台中记录的故障检修记录验证了上述关联，该故障的检修描述如下：网络管理员通过主动测量分析两设备端口 IP 包收发情况，发现 Quidway123 设备因事故造成端口自链接后的流量异常增长，频繁收发包导致了 CPU 和内存满负载。同时，Quidway123 设备与 A-centerswitch 有 IP 包收发业务，一段时间后，间接地导致了 A-centerswitch 的瘫痪。

表 3　考勤 & 监控业务流频繁序列分析结果

业务	设备	情景序列	发生时间	置信度
考勤	A	(CPU,MEMORY,TRAFFIC)	[14:00,14:30]	70
监控	Q	(CPU,MEMORY)	[11:00.11:30]	70
监控	Q	(TRAFFIC)	[12:00,14:00]	75

因此，改良式(4)，定义业务 T 在$[t_{i-1},t_i]$时刻在设备 d

上的间接信任度 ITD 如式(5)所示。

$$ITD(T,d,t_i)=\sum_{i=1}^{m}\left(\frac{t_e-\max\{t_{i-1},t_s\}}{t_i-t_{i-1}}ITD(\Phi_i,d,t_i)\right) \quad (5)$$

式中,$[t_s,t_e]\subset[t_{i-1},t_i]$。$[t_s,t_e]$用于调整对业务间接信任度值变化的影响。如某告警时间持续越长,即使该告警重要级别不高,根据式(5),也将对当前系统信任环境造成重要影响,从而符合了实际场景的事实。

图 4 以业务流{考勤,监控}为例,计算了该业务流在对应设备上的总体信任度。从图 4 可以看出,相关业务 Φ 的信任度变化对当前业务的间接信任度计算有重要影响。

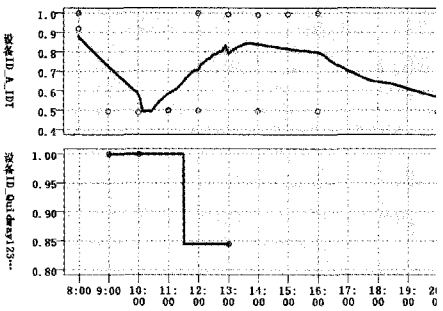

图 4 业务流{考勤,监控}总体信任度变化趋势

2.3 信任的评估和预测

根据 Marsh[6] 的动态信任管理定义,信任度的值随着环境和时间动态变化,并且离当前较近时间段的信任度值的降低,比更早时间段信任度值的降低,对当前系统安全性影响更大。OWA 算子是常用的预测算子,然而该算子在计算中没有考虑时间维度信息。Fuller 提出的 IOWA 算子[19] 保留了 OWA 算子有效集结数据的优点,同时增加了按照时间变化的数据集的预测问题。IOWA 算子将随时间变化的数据集表示为二维数组$\langle v_1,a_1\rangle\langle v_2,a_2\rangle\cdots\langle v_m,a_m\rangle$。随后定义函数 $\Gamma(\langle v_1,a_1\rangle\langle v_2,a_2\rangle,\cdots,\langle v_m,a_m\rangle)=\sum_{i=1}^{m}\omega_i^* a_{v\text{-}index}(i)$计算序列 $v_1,v_2,v_3,\cdots,v_m$ 按从大到小顺序排列后,对应 $a_1,a_2,a_3,\cdots,a_m$ 的有序加权平均值。

求解 IOWA 算子问题,即找出满足条件 $\omega_i^*\geqslant 0,\sum_{i=1}^{m}\omega_i^*=1,i=1,2,\cdots,m$ 的系数向量矩阵 $\omega_i^*=(\omega_1^*,\omega_2^*,\cdots,\omega_m^*)^{\mathrm{T}}$。

利用 IOWA 算子,将 ITIL 平台下按照式(1)计算,按照监控指标采集时间排列的业务直接信任序列表示为$\langle t_1,DTD(T_1,d,t_1)\rangle,\langle t_2,DTD(T_2,d,t_2)\rangle,\cdots,\langle t_n,DTD(T_n,d,t_n)\rangle$同时,将利用式(5)计算得到的业务间接信任度用作求解 IOWA 算子权值的参考因子。利用式(6)来求解权值向量。

$$\omega_i=\omega_{i-1}(1+(t_i-t_{i-1})*(1-ITD(T,d,t_i))) \quad (6)$$

最终根据 IOWA 算子预测 t_{n+1}时刻业务 i 的总体信任度为$(t_{n+1},OTD(T_{n+1},d,t_{n+1}))$。

本方法避免了计算 IOWA 算子时,常用的权值系数计算方法无法适应 ITIL 平台计算环境变化,导致的预先设置离散度 α 无法确定的缺陷。同时,又在 IOWA 算子预测中加入了间接信任度 $ITD(T,d,ti_i)$的负反馈作用,充分利用上下文环境丰富的时间信息计算业务总体信任度的变化。

3 基于 ITIL 的动态信任管理模型结构

根据上述业务信任度计算方法,在现有的 iMAN-IT 运维管理系统基础上,追加了仲裁器和行为评估中心模块,用于计算系统中每个业务在运行过程中对系统信任环境产生的影响。所设计的 ITIL 模型的动态信任管理模型如图 5 所示。该系统通过 Agent 代理实时采集各类设备的性能参数指标,主要模块设计功能描述如下:

行为数据收集器:主要利用 IT 运维平台的 Agent 自动获取常用设备的性能监控参数(CPU、交换区、内存、单个磁盘 IO、系统 I/O、适配器 IO、网络 IO、文件系统)。

资产状态监控:根据设备种类的不同(服务器、路由器、交换机、Web 服务设备、邮件服务设备以及数据),分类监控每一类别设备的分布情况。

业务监控:根据用户定义的业务逻辑图,监控该业务下的所有设备的相关告警和事件。具体业务监控包括业务名称、业务状态(可达、不可达、告警、严重告警)、业务优先级、业务创建时间、当前无故障运行时间、可用性等。

告警监控/事件监控:主要监控业务运行过程中重要的设备的告警信息,事件监控根据业务监控中指定的规则来判定告警级别和告警时间,交仲裁器判定行为的可信程度。

仲裁器:接收行为数据收集器和本地规则库的信息,并进行规则匹配并判断业务行为的合法性。对于仲裁为非法的行为,需要报告行为评估中心处理。

行为评估中心:根据监控的历史告警记录和事件日志等上下文信息,来进行业务行为的动态评估,将信任评估的结果用于更新 ITIL 平台上业务服务与应用的信任度等级,实现内部环境中对计算资源的约束访问。业务中执行了任何非法行为都会导致信任度的降低。

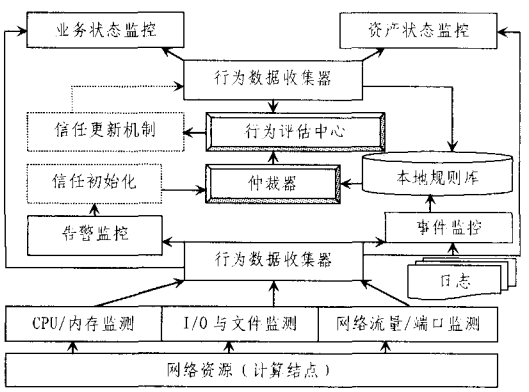

图 5 基于 ITIL 模型的动态信任管理模型

4 实验与结果分析

实验用于监控上下班时间段系统环境安全的业务流{考勤,监控},在 2012 年 2 月 5 至 2012 年 2 月 7 日时间段,总体信任度变化为例,来说明本文算法在故障排除中的作用。图 6 反映了该业务流的数据传递情况。从图 6 可以看出,服务器 A-centerswitch 和 Quidway123 分别负责考勤和监控业务,设备主机 31.242 负责保存相关数据。考勤业务的所有消息收发均须通过中央交换机 A-centerswitch 来完成。

根据本文提出的动态信任管理模型,分别计算考勤和监控在不同时间段的总体信任度值 OTD。考勤业务 OTD 值的变化如图 7 所示,对比图 3 可以看出,在 2012 年 2 月 7 日的[11:00,12:30]时间段,该业务的 OTD 值有明显下降趋势,与相关设备 Quidway123 的信任度下降保持一致,更准确地定位出了一系列故障发生的真正原因,为故障排查提供了有力

的参考。

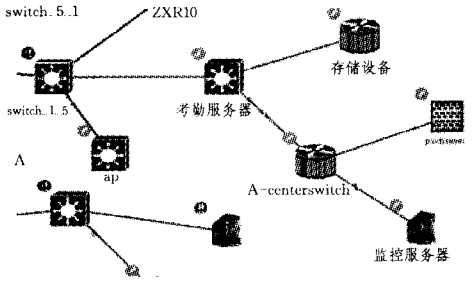

图 6 上下班场景业务逻辑图

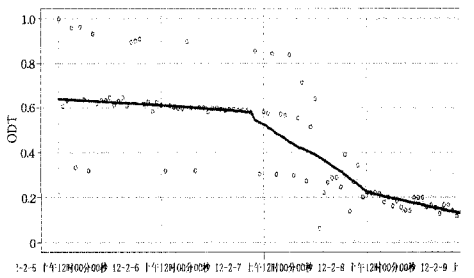

图 7 考勤业务的总体信任度变化趋势图

结束语 本文根据 ITIL 平台特点，提出了一种根据动态管理模型理论计算业务信任值的方法，并将信任值的变化用于监控系统内部的安全环境。在此基础上，结合现有的 ITIL 平台开发环境，建立了基于 ITIL 平台的动态访问控制模型，实现了针对业务的行为验证。该模型以 ITIL 标准中安全服务级别协议(SLA)和安全事件管理规范，为上下文环境的信任相关因素，动态地计算和变更计算资源的信任值，以期减少由于设备安全动态变化造成的网络服务可信性损失。下一步工作将集中探讨 ITIL 下信任数据存储、规模与效率等问题。

参 考 文 献

[1] Clifford D, van Bon J. Implementing ISO/IEC 20000 Certification: The Roadmap. ITSM Library[S]. Van Haren Publishing, 2008

[2] 张明德. 身份认证可信度研究[J]. 计算机科学, 2011, 38(11): 43-47

[3] Blaze M, Feigenbaum J, Lacy J. Decentraliezed trust management[C]//Bale J, Dinolt G, eds. Proceedings of the 17th Symposium on Security and Privacy. Washington: IEEE Computer Society Press, 1996: 164-173

[4] Policy Maker[EB/OL]. www. polimap. com/

[5] Keynote [EB/OL]. www. keynotesecurity. com/

[6] Marsh S P. Formalizing trust as a computational comcept [D]. Stirling: University of Stirling, 1994, http://www. nr. no/~abile/Papers/TR133. pdf

[7] Almenárez F. PTM: A pervasive trust management model for dynamic open environments[C]//Workshop on Pervasive. 2004

[8] Nefti S. A fuzzy trust model for e-commerce[C]//E-Commerce Technology. 2005

[9] Sepandar D K. The EigenTrust algorithm for reputation management in P2P networks[C]//Proceeding WWW '03 Proceedings of the 12th international conference on World Wide Web

[10] 李小勇. 大规模分布式环境下动态信任模型研究[J]. 软件学报, 2007, 18(6): 1510-1521

[11] 赛迪网. TSM: 中国银行广东省分行 IT 服务管理案例[EB/OL]. http://industry. eeidnet. eom/art/19/20040402/99965_1. html, 2004-04

[12] 王华. 上海西门子移动通信有限公司实施 IT 服务管理的策略研究[D]. 上海: 上海交通大学, 2008

[13] 张孜. 基于 ITIL 理念的交通信息设施运维管理系统设计与实践[J]. 交通运输系统工程与信息, 2011(4): 41-45

[14] 刘海峰. 基于 ITIL 体系的安全服务级别管理研究[J]. 计算机工程与设计, 2007(4): 780-784

[15] ca 公司. eTrust TM Security Management[EB/OL]. http://www3. ca. com/solutions/Solution. aspx? ID=271

[16] 桂小林. 网格技术导论[M]. 北京: 北京邮电大学出版社

[17] Peng N, Yun C, Reeves D S. Analyzing Intensive Intrusion Alerts via Correlation[C]// Proc of the 5th International Symposium on Recent Advance in Intrusion Detection. Zurich, Switzerland, 2002

[18] Savla S, chakravarthy S. An efficient single pass approach to frequent episode discovery in sequence data[C]//IET 4th International Conference. 2008

[19] Fuller R, Majlender P. An analytic approach for obtaining maximal entropy OWA operator weights[J]. Fuzzy Sets and Systems, 2001(1): 53-57

[20] 石贵民, 林宏基. 基于旁路的网络流量监控模式[J]. 重庆理工大学学报: 自然科学版, 2011, 25(9): 63-69

(上接第 56 页)

[9] Golden C, Cartridge T. Computer Chip Usage and the Impact on the After market[J]. Static Control Components, 2002: 36-46

[10] Chang K-H, Markov I L, Bertacco V. Fixing Design Errors with Counter-examples and Resynthesis[J]. IEEE Trans. on Computer-Aided Design, 2008, 27(1): 184-188

[11] King S T, Tucek J, Cozzie A, et al. Designing and implementing malicious hardware [EB/OL]. http://www. usenix. org/event/leet08/tech/full_papers/king /king. pdf, 2009-04-11

[12] Banga M, Chandrasekhar M, Lei Fang, et al. Guided test generation for isolation and detection of embedded Trojans[C]//Proc of the 18th ACM Great Lakes Symposium on VLSI. 2008: 363-366

[13] Agarwal D, Baktir S, Karakoyunlu D, et al. Trojan detection using IC fingerprinting[C]//Proc of IEEE Symp on Security and Privacy. 2007: 20-23

[14] Chakraborty R S, Wolf F, Papachristou C, et al. Towards trojan-free trusted ics: Problem analysis and detection scheme[C]//Proc of design, automation and test conference. 2008: 1362-1365

[15] Sanno B. Detecting Hardware Trojans[EB/OL]. http://www. crypto. rub. de/imperia/md/content/seminare/itsss09/benjamin_sanno. semembsec_termpaper_20090723_final. pdf. 2009-07-22

[16] Friedenberg J. Mind as a Black Box[M]. Sage Publications, 2006: 85-88

[17] 唐策善, 李龙澎, 黄刘生. 数据结构—用 C 语言描述[M]. 北京: 高等教育出版社, 2006: 125