

基于定量安全风险评估模型的网络安全管理平台

孙 强

(牡丹江师范学院 计算机科学与技术系, 黑龙江 牡丹江 157012)

摘 要: 分析了当前主要网络安全产品的局限性, 阐述了建设网络安全管理平台的必要性, 在此基础上介绍了一种基于定量安全风险评估模型的网络安全管理平台; 讨论了系统架构、定量安全风险模型和系统安全机制等系统实现中的关键技术问题及其解决方法。

关键词: 网络安全; 信息安全; 安全管理; 安全风险评估模型

中图分类号: TP309

文献标识码: A

文章编号: 1000-7180(2010)05-0070-04

Network Security Management Platform Based on Quantitative Security Risk Assessment Model

SUN Qiang

(Department of Computer Science and Technology, Mudanjiang Teachers College, Mudanjiang 157012, China)

Abstract: The limitations of main network security products at present are analyzed in this paper. Meanwhile, the necessity of establishing network security management platform is also explained, on the basis of which network security management platform based on quantitative security risk assessment model is introduced. Besides, the key technological problems and the corresponding solutions are discussed in the implementation of the system architecture, quantitative security risk assessment model and the security mechanism of system.

Key words: network security; information security; security management; security risk assessment model

1 引言

随着网络和信息技术的蓬勃发展和广泛应用, 越来越多的职能性专用网和信息系统的规模在不断扩大, 随之而来的安全管理问题也日渐繁杂。因为要想保障基于大型网络和信息系统之上的业务正常运转, 必须综合考虑应对各种问题, 包括: 设备故障、黑客入侵、信息外漏、病毒传播等。然而无论是传统意义上的网管系统, 还是各类安全技术产品, 都只能解决局部问题; 此外各类安全产品之间缺乏互操作性, 很难做到协同调度、统一管理, 无法保证整个网络和信息系统在安全策略上的完整性和安全措施上的一致性。在这种情况下, 不仅会加重网络和安全管理人员的负担, 更会使网络和信息系统的动态安全性无法得到保证, 大大增加整个系统的维护费用^[1]。

为了理清网络安全建设的发展思路, 为网络安全管理提供有效的技术手段, 人们在多年网络建设和管理的基础上, 提出以全网设备和用户信息管理为基础的, 集各类网络产品管理为一体的信息网络安全管理平台的设想, 最终实现网络安全管理信息分级管理, 全网实时监控, 达到加强网络安全统一管理, 确保网络安全畅通的目的, 最终提出网络安全管理平台(Security Management Platform, SMP)管理软件^[2]。网络安全管理平台的目的是保护有可能被侵犯或破坏的机密信息不受外来非法操作者的控制, 也就是实现信息的机密性(Confidential)、完整性(Integrity)和可用性(Availability), 即 CIA 这三个方面的安全目标^[3]。但 CIA 本身排除了其他一些重要的方面和需要考虑的地方。文中介绍了系统架构、定量安全风险模型和系统安全机制等系统实现中的关

键技术问题及其解决方法,最后给出该系统的特点和进一步研究工作的方向。

2 系统的总体架构

系统的设计主要采用面向对象的设计方法,使用了J2EE技术,基于MVC框架进行设计。J2EE提供了一个企业级的计算模型和运行环境用于开发和部署多层体系结构的应用。它通过提供企业计算环境所必需的各种服务,使得部署在J2EE平台上的多层应用可以实现高可用性、安全性、可扩展性和可靠性。系统总体架构如图1所示,是一个实现该系统的四层结构。

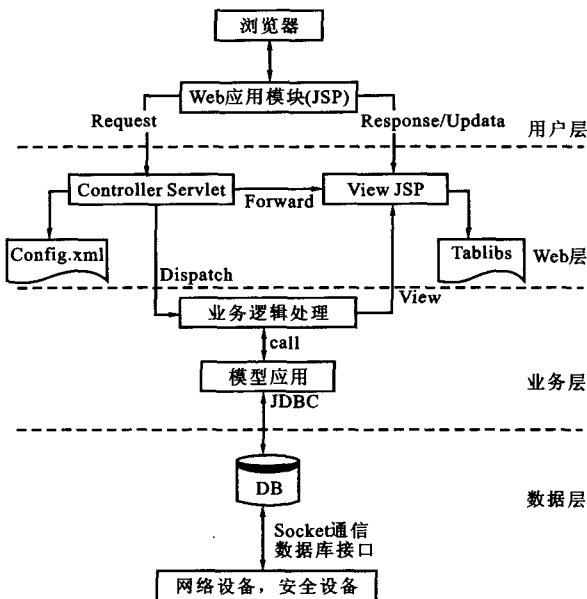


图1 SMP安全管理系统的总体架构

用户层:也就是客户端层,用来与用户交互,并把来自系统的信息显示给用户,在该层用户可以输入和更新数据;

Web层:该层包含J2EE Web组件,包括了JSP和Servlet。该层主要用来处理客户请求,调用相应的逻辑模块,并把结果以动态网页形式返回到客户端。该层生成Web页面和Web页面中的动态内容,该动态内容通常从数据库获得,并且在表示层能够把客户端传来的Web页面包含的请求打包。使用Struts框架来构建此层。Struts框架中的ActionServlet描述如何处理HTTP请求,如何产生应答,在系统中可以使用它们来传递动态内容。

业务层:这一层负责处理应用的核心业务逻辑。业务组件通常被实现为运行在EJB容器内的EJB组件,EJB容器提供组件生命周期、管理持久性、事务和资源分配等。该层是开发中最重要的部分,在

该系统中很多复杂的业务逻辑使用EJB来实现,并且将一些常用的功能也以EJB组件的形式实现。

数据层:负责数据管理,完成数据采集,该系统采用ORACLE数据库,数据库中的数据主要包括:资产数据信息、漏洞信息数据、威胁信息数据、风险信息数据、事件信息数据、工单信息数据、安全知识策略数据和系统支持信息。在设计中,尽量把动作和业务逻辑同数据层分离开,为了确保数据完整性和一致性,在数据库中包含了一定的约束,例如not null约束和外键约束等。

3 定量安全风险评估模型

3.1 基本要素描述

基于风险要素的风险计算模型是以ISO13335-1中的核心安全风险模型为基础进行系统建模的。基本要素为资产价值、威胁、漏洞、风险。各要素的相互关系如图2所示模型。

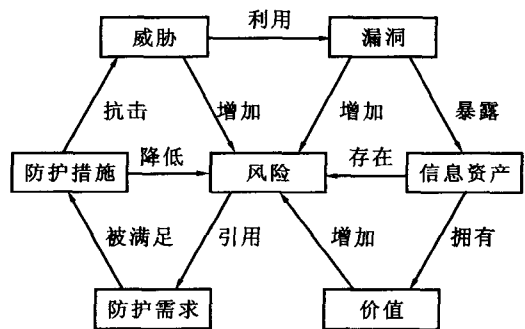


图2 安全风险模型各种要素的相互关系

(1) 资产价值是指在评估范围内的资产的自身价值和资产在系统内重要性的统一值。

(2) 威胁是指信息资产的安全可能受到的侵害,因为目前不可能实现事件和漏洞的精确对应,所以采用威胁来关联攻击行为(事件)和漏洞,定量的风险评估计算模型知识库自身定义的威胁由服务人员根据事件类和漏洞来建立^[4]。

(3) 漏洞本身是无害的,是被威胁利用来影响资产的一个必要条件,定量风险评估计算模型知识库自身定义了具体漏洞,包括扫描器的漏洞和人工评估的具体漏洞。

(4) 风险是指某个时间范围内企业的安全状况。风险是在考虑事件发生的可能性及其可能造成的影响下,漏洞被威胁所利用后在资产上所产生的实际负面影响。风险是威胁可能性和威胁影响性的函数^[5]。风险的函数关系为

风险 = F(资产价值、漏洞值、威胁影响值、威胁可能性)

3.2 量化的信息安全风险评估计算方法

资产价值不仅仅为自身的价值,而是它在信息系统中的价值,与资产的机密性、完整性和可用性有关.具体计算公式为

$$A_R = \log_2 \frac{2^C + 2^I + 2^A}{3} \quad (1)$$

式中, A_R 表示资产的价值, C 表示资产的机密性值, I 表示资产的完整性值, A 表示资产可用性值.

漏洞值 V 是漏洞的一个属性,具体参见量化的风险评估计算方法知识库中的安全漏洞库.威胁影响值分为影响初始值和影响资产值.影响初始值 T_L 是根据统计和经验判断某个威胁可能造成的影响的大小,固化在系统知识库中.

影响资产值指威胁发生后对特定属性(C 、 I 、 A)造成的影响,由三个权重(C 权重、 I 权重、 A 权重)构成影响资产权重数组,此数组中 CIA 权重分别与资产的 CIA 值相乘后求和除以 3,再开平方根得到影响资产值.威胁影响值则可以分为威胁初始影响值和威胁影响资产值两部分,可以由式(2) 计算出来.

$$T_S = \frac{T_L + T_A}{2} \quad (2)$$

式中, T_S 表示威胁对资产或者业务系统的影响性, T_L 表示威胁初始影响值, T_A 表示威胁影响资产值即威胁影响资产值,计算公式为

$$T_A = \sqrt{\frac{T_{CA} \times C + T_{IA} \times I + T_{AA} \times A}{3}} \quad (3)$$

式中, T_{CA} 表示威胁针对资产机密性的权重, T_{IA} 表示威胁针对资产完整性的权重, T_{AA} 表示威胁针对资产可用性的权重, C 表示资产的机密性值, I 表示资产的完整性值, A 表示资产的可用性值.

威胁可能性的判断可以确定某安全对象(资产)上是否面临某个威胁以及这个威胁发生的可能性有多大.威胁可能性的计算包括三个参数:固定经验值、发生条件值和发生次数值.威胁的固定经验值是国际组织长期统计的结果,固化在系统子知识库中,只能在知识库升级时修改.发生条件值的赋予根据具体的应用环境来确定,初始值为固定经验值,在此基础上调整.

最后根据威胁、漏洞、资产都会增加风险值,得到风险值计算公式.首先通过式(4) 计算出风险中漏洞所能利用威胁的数值:

$$T = \sqrt{T_P \times T_S} \quad (4)$$

式中, T 表示风险中漏洞所能利用威胁的数值, T_P 表示风险中漏洞所能利用威胁产生的可能性, T_S 表

示风险中漏洞所能利用威胁产生的严重程度,也就是影响值.再利用前几节介绍的资产价值、漏洞值和风险中漏洞所能利用威胁的数值,使用式(5) 计算出最终的风险值.

$$R_R = A_R \times V \times T \quad (5)$$

式中, R_R 表示该风险的风险值, T 表示风险中漏洞所能利用威胁的数值, V 表示风险中漏洞所能利用威胁的数值(漏洞值), A_R 表示资产的价值.

根据定量风险评估计算模型的计算,得出了每个风险的具体数值,我们可以根据这个风险值对风险进行等级划分.参考国家标准,定义严重程度为 4 级,如表 1 所示.

表 1 风险严重程度及其描述

风险严重程度	描述及相应对策
告知 [0,25]	正常网络状态,没有显著的网络攻击,只存在零星攻击.网络大多数情况下都处在此状态.此时保持普通安全策略.
预警 [25,70]	有一些严重漏洞发布或网络攻击事件有增多迹象.此时需对网络和主机进行安全评估、安全升级,以及进行必要的监控.
报警 [70,100]	某些严重漏洞或威胁正被攻击者利用来进行大规模攻击,网络攻击事件显著增加.此时需要立刻采取防御措施.
紧急 [100,125]	网络安全态势非常严峻,对全球互联网造成严重影响.此时需要与其他网络协作采取防御措施.

4 系统的安全机制

安全管理平台自身的安全可靠对被管理系统的正常运行至关重要,因为安全管理系统中存储着重要的安全信息和强有力的管理工具^[6].基于 B/S 结构的安全管理平台给安全管理带来了新的不安全因素,因为 Web 应用的平台独立性和地理无关性使得任何人、从任何地方都可能访问安全管理系统.为此,我们必须利用安全设备和安全技术来保证安全管理平台的自身安全.

由于整个安全管理平台是一个包括 Web 服务器、数据库、数据引擎等部分组成的大系统,不可能部署在一台主机上.我们首先部署相关的防火墙、路由器和网关等网络安全设备,对安全管理平台的外围进行安全性管理;对于安全管理平台内部的数据传输和存储我们使用了以下的安全技术:基于 UA 的用户认证、DES 数据加密存储、自定义的数据加密报文传输、基于 SSL 协议数据保密传

输、基于用户组和访问控制链表的访问控制,各种机制之间的关系如图3所示。

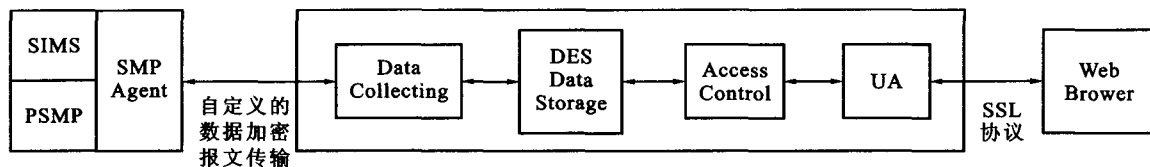


图3 系统安全机制

在图3中我们将安全管理平台逻辑上分为两部分:用大矩形框出部分作为系统的内部;负责数据采集的SMP数据代理和用户的Web浏览器是系统仅有的两个对外的接口,称为系统的外部,这两个外部接口也是整个安全管理平台自身安全防护的关键。在SMP数据代理与SMP数据传输时使用了自定义的数据加密报文,这个自定义加密报文采用MD5算法进行信息摘要,来认证数据源的可靠性和数据完整性,防止了假冒和篡改类型的攻击;使用IDEA算法进行信息和摘要的加密,防止了重要数据信息的泄密^[7]。

Web浏览器是安全管理平台唯一的对外访问点,系统对用户的认证是由Web服务器完成的,由于用户名/口令认证机制的众所周知的弱点,我们在浏览器与服务器之间使用了安全套接字协议SSL,利用SSL基于公开密钥的证书来认证系统用户。为此,我们维护一个独立的CA(certification authority)为SMP的每个用户签发证书。除了认证以外,SSL还保证了浏览器与服务器之间数据传输的保密性与完整性。同时在SMP软件中用户按照角色的不同分成不同的用户组,每个用户组中的用户具有不同的权限,只有具备足够权限的用户才能执行相应的操作(如读、修改、增加或删除),并且不同用户组对应不同的被管对象(即系统中的安全设备和网络设备),对被管对象的操作可用以下三元组来表示:

〈用户组,所属的被管对象,操作权限〉

当一个用户想对一个被管对象进行某个操作时,系统先查找用户所在的用户组,然后再查找该用户组是否有管理这个对象的资格,最后再查看系统访问控制表,来检索用户对该对象的操作权限来决定是否可以此种操作。

在SMP内部为了防止了关键数据的泄密,对于采集来的敏感信息,使用了DES加密算法加密之后存储在数据库中。

5 结束语

随着集成技术的发展以及网络安全产品接口的国际标准化工作的深入,网络安全管理平台也必将成为未来网络安全的综合解决方案。文中所研究的安全管理平台已经应用到实际的环境中,基本达到了预期的要求。但是所触及的仅仅是系统的一小部分,实现资产、漏洞、风险、事件之间的关联及数据汇聚和挖掘分析工作还做得不够。下一步工作的目标是以安全管理平台数据为基础,实现高层次的业务相关分析功能和安全设备配置管理功能,实现对安全管理的自动化、智能化和统一化。

参考文献:

- [1] 孙强,陈伟,王东红. 信息安全管理:全球最佳实务与实施指南[M]. 北京:清华大学出版社,2004:56-72.
- [2] 孙强,郭江鸿,王慧. 基于消息通信的安全管理系统的设计与实现[J]. 计算机工程与应用,2006,30(10):134-139.
- [3] ISO/IEC TR13335-1 Guide-lines for the management of IT security, part1: concepts and models for IT security [EB/OL]. [2004-11-19]. <http://www.din.de/ni/sc27>.
- [4] 冯登国,张阳,张玉清. 信息安全风险评估综述[J]. 通信学报,2004,25(7):10-18.
- [5] 高寅生. 安全漏洞库设计与实现[J]. 微电子学与计算机,2007,24(3):99-101.
- [6] 于璐,吴振强. 基于免疫的自适应安全模型[J]. 微电子学与计算机,2009,26(1):113-117.
- [7] 段海新. 基于Web和数据库的网络管理系统的设计与实现[J]. 软件学报,2000,11(4):468-472.

作者简介:

孙强 男,(1979-),博士.研究方向为信息安全和电子设计自动化等。