第 34 卷 第 2 期 计 算 机 工 程 2008 年 1 月
Vol.34 No.2 Compute Egineering January 2008
·安全技术· 文章编号：1000—3428(2008)02—0135—03 文献标识码：A 中图分类号：TP393

一种信息安全综合管理模型

赖 滇
(信号盲处理国防科技重点实验室，成都 610041)

摘 要：为有效解决目前信息安全资源的协同工作问题，降低系统的漏报率和误报率，该文提出了一种信息安全综合管理模型，。该模型使用开放式接口，实现了不同类型资源的统一管理，实现了设施与信息两级数据融合。采用分级、树状层次结构，有良好的可扩展性。具有设计模块化、应用灵活多变、管理可视化等特点。

关键词：综合管理；协同；融合

Integrative Management Model of Information Security

LAI Dian
(National Defence Key Laboratory of Blind Processing of Signals, Chengdu 610041)

【Abstract】 This paper proposes an Integrative Management Model of Information Security(IMMIS). The model solves the existent cooperation problems of information security resources. The model achieves low false alarm rate and false positive rate. It uses open interfaces to manage various resources, realizes instrument data and information data fusion. Adopting hierarchy and tree structure, the model is expansible. The modularization design makes the application of the model flexible. To users, the management is visual.

【Key words】 integrative management; cooperation; fusion

1 概述

信息安全事件的特点是突发性、多样性和不可预知性。这些特点决定了防御比攻击复杂得多，需要防御方掌握全面的信息安全理论与应用，甚至要求防御方本身也具有攻击的能力和经验，更重要的是充分利用和整合各类信息安全资源，统一管理、协同工作来应对安全事件。信息安全资源包括确保信息系统安全的一切资源，如人力、物力、产品、技术、服务、政策等。目前，因为各类信息安全资源管理复杂性较高，安全本身又具有“木桶效应”[1]，所以如何降低安全管理难度、提高安全管理效率已经成为信息安全保障中急需解决的重要问题。

信息安全管理模型多种多样。20 世纪 90 年代初期，C/S或B/S模型成为主流[1-2]。C/S或B/S将数据统一存储在数据服务器上，有关的业务逻辑都在客户端实现，即所谓的“胖终端”。“胖终端”的缺点是：单一的服务器结构过于依赖供应商；数据存取受到限制；难以扩展到大规模广域网或Internet；难以管理客户端机群；信息内容和形式单一等。

随着应用需求的增长和 Internet/Intranet 的普及，3 层或 4 层体系模型代替了 C/S 或 B/S 模型。3 层或 4 层模型是把用户端的业务逻辑独立出来，并与数据库中的存储过程合并在一起，构成应用层，以提高计算能力，实现灵活性。这种结构中，用户端仅仅是图形用户界面(Graphical User Interfaces, GUI)，即所谓的“瘦终端”。“瘦终端”的主要缺点是：用户管理功能单一，往往只能管理一种或几种信息安全资源的一种或几种功能。

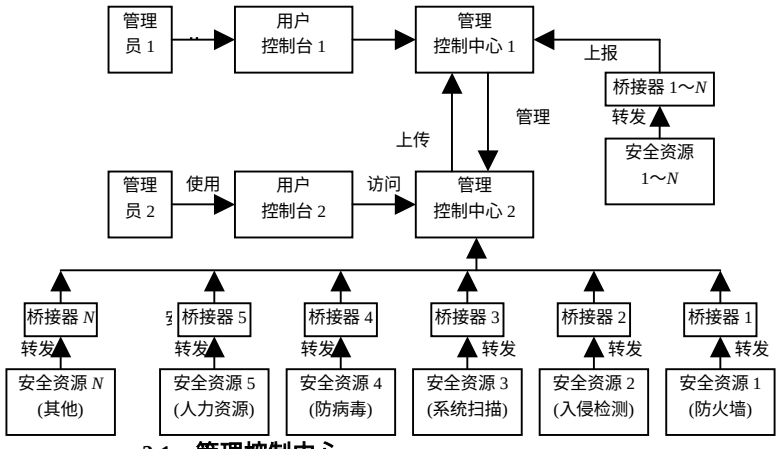
“胖终端”和“瘦终端”都没有解决的问题是：复杂分布式网络环境下如何有效地管理数量巨大、种类繁多的信息安全资源。

为此，本文提出了信息安全综合管理模型(Integrative Management Model of Information Security, IMMIS)。

2 信息安全综合管理模型

IMMIS 主要包括 3 个部分：管理控制中心，桥接器(bridge)，安全资源，如图 1 所示。安全资源通过桥接器与管理控制中心进行连接，实现信息交换，这些信息被管理控制中心处理或通过管理控制中心已经具备的上下级联功能汇总到上一级管理控制中心。

图 1 信息安全资源综合管理模型



2.1 管理控制中心

IMMIS 以管理控制中心为数据存储、处理、管理等功能的中心，建立多层面、分布式系统和集中式管理方式，实现高度集成、智能化管理，使多种信息安全资源信息共享、协

作者简介：赖 滇(1977－)，男，工程师、博士研究生，主研方向：信息安全

收稿日期：2007-01-20 **E-mail：**laidian@126.com

同工作。IMMIS 通过用户控制台为用户提供多角度的安全状况分析、报警、统计、报告等功能。

2.2 桥接器

桥接器以独立组件的方式运行(在 Windows 平台上一般是服务程序，在 Unix 平台上一般是守护进程)。桥接器的主要功能如下：

(1)建立安全资源与管理控制中心之间的通道

由于不同类型的安全资源的通信接口与协议有所不同，因此为保证管理控制中心的灵活性与可扩展性，即管理控制中心独立于安全资源，桥接器为各种安全资源与管理控制中心提供通用接口。桥接器向上与管理控制中心通信，向下与安全资源通信。一种类型的安全资源有一个桥接器与之对应。

(2)采集安全资源运行状态信息

按轮询或发布的方式采集安全资源运行状态信息：安全资源是否运行的状态信息；安全资源所在设备或计算机的 CPU 占用率、MEM 占用率；如果状态信息采用发布方式，发布的时间可配置或间隔不应该太长；提供安全资源位置配置参数，如地址、工作端口、认证信息等。

(3)采集安全资源报警、日志信息

提供报警、日志信息采集功能；能够解决重复采集问题，例如采集器重启后重复获取安全资源报警信息；安全资源发布的报警信息、日志信息应该具备可阅读性或者可被转换为可阅读信息。

管理控制中心、桥接器、安全资源三者之间的信息交互模式包括“拉”模式或“推”模式，分别如图 2、图 3 所示。

图 2 信息交互“拉”模式

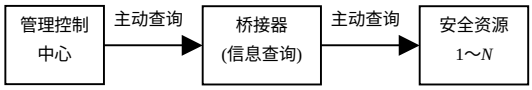
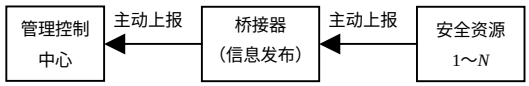


图 3 信息交互“推”模式



2.3 安全资源

安全资源包括确保信息系统安全的一切资源，如人力物力、安全产品、安全技术、安全服务、安全制度等。

3 IMMIS 相关技术

为达到复杂分布式网络环境下有效地管理数量巨大、种类繁多的信息安全资源的目的，IMMIS按以下准则设计：(1)采用标准的网络受管对象数据描述模型CIM(Common Information Model, 公共信息模型)[3]；(2)实现多种安全设施与信息的两级数据融合[4]，实现各类安全事件的集中分析与统一响应；(3)具有分级、树状的层次结构，实现多级分布式、可视化的管理模式，能够适应多级、跨地域的复杂网络环境；(4)融合事件关联和过滤处理、跨平台和跨系统操作的分布式中间件技术；(5)采用专家知识库和数据挖掘技术等。

3.1 CIM

IMMIS的主要通信协议是CIM over HTTP V1.0，该协议以HTTP为基础，以XML[5]为数据描述格式，规定了 22 个操作原语，具有很强的灵活性和扩充性，也可以顺利地加入符合简单对象访问协议(Simple Object Access Protocol, SOAP)协议的通信接口[6]。

CIM 是基于网络的企业管理(Web-Based Enterprise Management, WBEM)体系结构的核心组件[7]，是一个使用面向对象的基本概念来描述管理实体，如系统、软件、用户和网络等的概念信息模型。CIM定义了一个前后一致的模型，依据这个模型，网络设备、系统和应用程序能显示有关它们自己的信息，并使这些信息能被管理工具利用。CIM能描述诸如桌面软件和硬件配置、CPU封装块的序列号以及某个特殊路由器端口上的流量水平等信息。

3.2 DMS

IMMIS 的核心是数据处理服务器(Data Manager Server, DMS)，该服务器具有如下功能：保存并管理受管资源的 CIM 对象描述信息；初始化并调用与受管资源通信的代理程序(Providers)；将由受管资源传来的报警及日志信息统一保存在数据库中，以备统计分析和数据挖掘；另外，当跨级操作时(如上级 GUI 对下级某个受管资源进行操作时，上级和中级 DMS 将起到信息路由和转发的作用)，一个 DMS 可以同时被多个 GUI 连接，每个 GUI 都可以同时操作 DMS 可控制的受管资源。

GUI 和 DMS、上级 DMS 和下级 DMS 之间采用的是 Subscription/Filter/Indication(“订单/过滤/事件触发”)的机制。例如，GUI 与 DMS 建立连接后，下达关于网络入侵检测系统(Network Intrusion Detection System, NIDS)报警的订单，这样 DMS 只将 NIDS 的 Indication 传给该 GUI，而其他类型的事件在向该 GUI 传送前被过滤掉。

3.3 可视化技术

IMMIS 的 GUI 部分提供直观的系统网络拓扑图，实时显示整个系统的安全状况。用户可以便捷地对 DMS 进行管理配置和策略设定，查看各单元安全资源的报警信息、状态信息、日志信息以及处理结果，还可以根据历史记录和过滤条件，生成多种样式的统计及趋势分析报表。

在该功能的实现设计中，后台采用数据库，实现两种对应关系：(1)IP 地址和网络拓扑图的对应关系；(2)攻击行为等安全事件分类结果和安全警报信息在拓扑图上的显示方式，如设备对应图标闪烁显示的对应关系等。

3.4 事件关联处理技术

IMMIS 采用事件关联技术提高系统的效率和功能。黑客攻击现象的表现有时会同时产生大量事件，彼此似乎并不相关，事实上却由同一个攻击原因所致。另外，很多攻击行为从单独的安全事件中很难发觉，必须综合多种安全资源的事件信息进行分析才能得到准确的判断。

3.5 事件过滤技术

IMMIS 的任一环节被触动都会产生报警信息并自动进入响应流程，而一个安全事件有可能同时触动多个单元安全资源，同时产生多个安全事件报警信息，这些信息都会被发送到管理控制中心，容易造成信息“泛滥”，而使关键的信息淹没。

IMMIS 采用事件过滤技术解决这一问题。IMMIS 采用了 4 种安全事件过滤规则：存在过滤规则，频率过滤规则，间隔过滤规则，次数过滤规则。在实际应用情况中，过滤规则还会更加复杂，IMMIS 还可以在上述这些基本过滤规则的基础上，合成更复杂的过滤规则。

3.6 安全事件快速响应技术

事件响应是指系统对安全事件的自动响应和基于人工的应急响应。IMMIS 对事件响应包括由物力资源(主要是安全设备)实现的自动响应和由人力资源(主要是安全事件应急响应

人员)实施的人工响应两种方式。

物力资源的自动响应包括：报警，阻塞、阻断或切断连接，引入陷阱进行进一步研究，取证，反击，恢复等。

人力资源的人工响应包括：修复，调查取证，审计分析，扫描评估，事件处理等。这需要建立一支应急响应队伍或使用安全服务的方式建立应急响应机构，实现人工响应。

4 误报率和漏报率分析

评价信息安全防护模型的两个重要要素为“漏报率”和“误报率”[8]。“漏报”是指系统将异常的事件作为正常事件或没有发现异常事件从而导致这些事件被忽略。漏报事件太多可导致系统无法发现对系统的攻击行为。“误报”是指将正常的事件作为异常事件报告，即假警报。假警报不但会降低系统的效率，而且会降低管理人员对系统的信任度。如果“误报率”太高，可能掩盖一些重要的安全事件，甚至导致系统频繁响应而影响正常运行。

一个好的信息安全防护模型应该同时具有较低的“漏报率”和“误报率”。IMMIS 采用信息共享、集中处理、协同工作的方式有效降低了“漏报率”和“误报率”。

4.1 漏报率

设系统中的安全资源个数为 n，单个安全资源对应的漏报率为 $P_i\,(i=1,2,\cdots,n)$，系统漏报率为 P，则

(1)采用非综合管理模型

根据“木桶效应”，若某一个安全资源漏报，则系统漏报，此时，系统漏报率如下：

$$P'=P_m,\ P_m\in\{P_1,P_2,\cdots,P_n\}$$

(2)采用 IMMIS

由于 IMMIS 采用信息共享、集中处理、协同工作的方式，只有当所有安全资源都漏报时，系统产生漏报，此时，系统漏报率如下：

$$P''=\prod_{i=1}^{n}P_i=P_1\times P_2\times\cdots\times P_m\cdots\times P_n$$

(3) P'' 与 P' 比较

$$P'-P''=P_m-P_1\times P_2\times\cdots\times P_m\times\cdots\times P_n=$$

$$P_m(1-P_1\times P_2\times\cdots\times P_{m-1}\times P_{m+1}\cdots\times P_n)$$

由于 $0<P_i<1$，因此 $P_m\ (1-P_1\times P_2\times\cdots\times P_{m-1}\times P_{m+1}\cdots\times P_n)>0$，即 $P'>P''$。

此时，有如下结论：

1)IMMIS 能够降低漏报率；

2)当系统规模扩大，则安全资源个数 n 增大，$P_1\times P_2\times\cdots\times P_{m-1}\times P_{m+1}\times\cdots\times P_n$ 减小，$P_m\ (1-P_1\times P_2\times\cdots\times P_{m-1}\times P_{m+1}\times\cdots\times P_n)$增大，$P'-P''$ 增大，IMMIS 降低漏报率效果更明显。

4.2 误报率

设系统中的安全资源个数为 n，单个安全资源对应的误报率为 $P_i\,(i=1,2,\cdots,n)$，系统误报率为 P，则

(1)采用非综合管理模型

根据“木桶效应”，若某一个安全资源产生误报，则系统误报，此时系统误报率

$$P'=P_m,\ P_m\in\{P_1,P_2,\cdots,P_n\}$$

(2)采用 IMMIS

由于 IMMIS 采用信息共享、集中处理、协同工作的方式，假设当任意 l 个安全资源误报时(显然，$1<l\le n$)，系统产生漏报，此时，系统漏报率

$$P''=\prod_{j=1}^{l}P_j,\ \{P_1,P_2,\cdots,P_j\}\subseteq\{P_1,P_2,\cdots,P_n\}$$

(3) P'' 与 P' 的比较

由于单个安全资源的误报率与系统无关，因此可以合理假设 $P_m\in\{P_1,P_2,\cdots,P_j\}$，而 $1<l\le n$，P'' 至少有 2 项，因此：

$$P'-P''=P_m-P_1\times P_2\times\cdots\times P_m\times\cdots\times P_l=$$

$$P_m\ (1-P_1\times P_2\times\cdots\times P_{m-1}\times P_{m+1}\times\cdots\times P_l)$$

因 $0<P_i<1$，$P_m\ (1-P_1\times P_2\times\cdots\times P_{m-1}\times P_{m+1}\cdots\times P_l)>0$，即 $P'>P''$，此时，有如下结论：

(1)IMMIS 能够降低误报率；

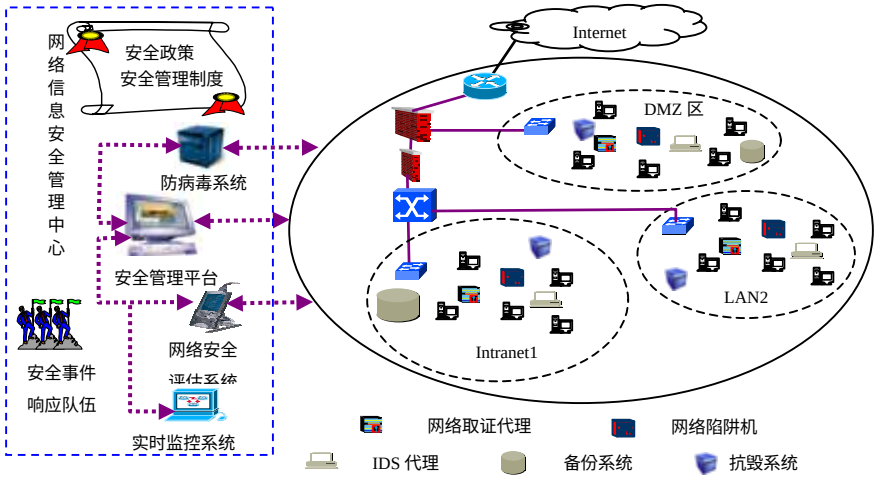
(2)当系统规模扩大，则安全资源个数 n 增大，$P_1\times P_2\times\cdots\times P_{m-1}\times P_{m+1}\times\cdots\times P_l$ 减小，$P_m\ (1-P_1\times P_2\times\cdots\times P_{m-1}\times P_{m+1}\times\cdots\times P_l)$增大，$P'-P''$ 增大，IMMIS 降低误报率效果更明显。

5 应用

5.1 典型应用

IMMIS 典型应用结构如图 4 所示。

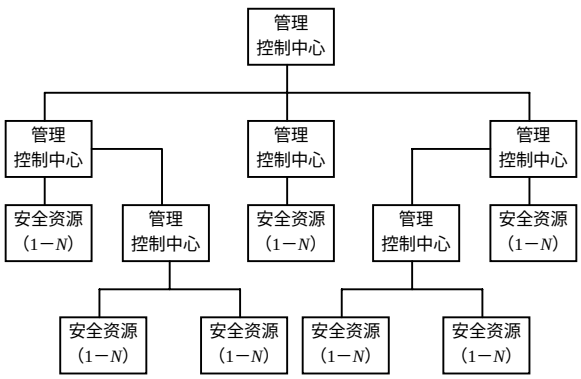
图 4 IMMIS 典型应用结构



5.2 分布式多级应用

IMMIS 分布式多级应用结构如图 5 所示。

图 5 IMMIS 分布式多级应用结构



对于结构比较复杂的网络，IMMIS 使用级联，以保障全

(下转第 150 页)