一种基于 CIM 的新安全管理平台*

钱 进[1], 刘 兵[2]
(1. 武汉大学计算机学院, 湖北 武汉 430072;
2. 北京中科网威信息技术有限公司, 北京 100011)

摘 要: 通过介绍 CIM (common information model, 通用信息模型) 的由来、原理和特点, 说明了在网络安全管理平台中采用 CIM 的优点和必要性, 在此基础上, 通过介绍 CIM 技术在中科网威安全管理平台中的成功应用案例, 进一步证明 CIM 在安全管理领域应用的可能性和意义。

关键词: 网络安全管理; CIM (通用信息模型); WBEM (基于万维网的企业管理); XML; UML; SNMP
中图分类号: TP393 文献标识码: A 文章编号: 0529-6579 (2003) S2-0156-04

随着网络应用的日益普及, 随着而来的安全管理问题也日渐繁杂, 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, 还是各类层出不穷的安全技术产品, 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, 无法保证整个网络策略上的完整性和行动上的一致性。这种局面不仅会加重网络管理人员的负担, 势必也会大大增加整个网络的维护费用。要解决上述问题, 首先面临的是“信息融合”的难题! 这里的“信息融合”是指: 能够以统一通用的数据描述格式保存所有受管设备的标识信息、工作状态和策略配置, 并能集中汇总这些设备产生的事件和日志信息。只有在“融合”的基础上, 我们才可能结合以往的经验和合理的技术, 在安全事故发生的前后, 对大量异类信息进行自动化的“去粗取精, 去伪存真”的关联性分析, 从而大幅度提高网管人员对安全事故的定位精度和响应速度! 提到网管领域的“通用协议和数据描述格式”, 我们首先会想到业界广泛使用 SNMP 和 MIB。然而, SNMP 及其改进版本都将精力集中在网络管理系统和它的代理之间的交互过程; 广域网环境下, 其平台的独立性和处理异类信息融合的能力就比较欠缺了。

1 CIM 的由来

关于 CIM (common information model), 必须先介绍一下 WBEM (Web-based enterprise management, 基于万维网的企业管理), 该技术最初是为了应对采用万维网 (WWW) 技术的分布式网络所提出的挑战, 由 Microsoft、Compaq、Cisco 等多家大公司联合提出的。1998 年 6 月, WBEM 的开发工作正式被移交给了 DMTF (distributed management task force, 分布式管理任务标准协会), 该技术目前的主要目标是: 推进网络、系统和应用的管理集成; 平台和管理环境的独立性; 随着网络扩容, 不断增强衡量机制; 以及降低网上客户的成本。

CIM 是 WBEM 体系结构的核心组件, 它使用面向对象的概念来描述现实世界中的被管理实体。CIM 最初的设计目的就是成为一种将不同管理系统上的信息结构化的一般方法, 因此, 来自不同网络或系统组件 (如 CMIP、SNMP 和 DMI 等) 的数据便能以一种标准的格式被进行描述和建立联系。

目前, 有许多公司支持 WBEM 和 CIM 标准, 其中包括: Intel, Microsoft, Cisco, Sun, IBM, Compaq, Dell, HP 等著名国际公司。此外, 该技术已被广泛应用在许多系统或技术中, 比较典型的包括: Cisco 的 Works2000 应用系统、Microsoft 的 WMI 服务, 以及 Sun 的 Jiro 体系结构[1-6]。

2 CIM 的原理

2.1 CIM 的组成

CIM 标准由 CIM 规范 (specification) 和 CIM 模型 (schema) 两部分构成。

CIM 规范用于形式上的描述, 它阐明了语言、命名、元模型和到其他管理模型 (如: SNMP 的 MIB) 的映射技术, 最新的版本为 2.2。

CIM 模型用于实际内容的描述, 它阐明了实际模型的具体内容, 从而提供了易于理解和扩展的系

* 收稿日期: 2003-05-02
作者简介: 钱进 (1973 年生), 男, 博士生; Email: ching73@163.com

统框架，并以此为基础开始组织与管理环境相关的可用信息。图 1 说明了 CIM 模型在概念上是如何层叠的。核心模型居中，它包含所有管理区域公共的类与关联，例如，所有可管理元素都是从一个名为 CIM_ManagedElement 的类继承而来的；外围的公共模型依次体现了更为具体的管理区域，这些区域的标准化工作分别由各个 DMTF 成员公司相关领域的专家组成的工作小组来负责，以保证公共模型的权威性和扩展性。CIM 模型最新的版本为 2.6。

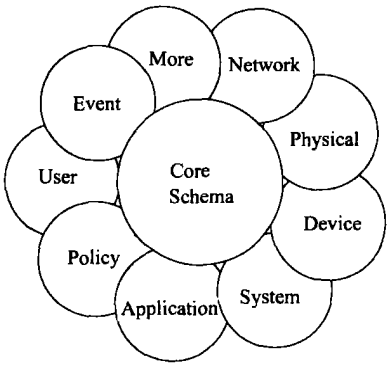

图 1　CIM 模型层次图

Fig. 1　CIM architecture overview

此外，DMTF 还发布了一个通信协议标准：CIM over HTTP V1.0。该协议以 HTTP 为基础，以 XML 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。

2.2　CIM 的定义形式

CIM 标准实际上提供了一个通用数据建模环境。它采用了类似对象设计图和称为 MOF (managed object format，受管对象格式) 中性语言的描述形式。在这一点上，CIM 建模环境中的 MOF 与 SNMP 中的 MIB、接口定义语言 (IDL) 很相似。

清单 1 给出一个 MOF 定义的示例，这些内容可以被 CIM 兼容系统中专用的编译器转换为 XML 格式。

```
// ==========================================================
// ManagedElement
// ==========================================================
    [Abstract, Description(
    " ManagedElement  is an abstract class that provides a common "
    " superclass(or top of the inheritance tree) for the "
    " non-association classes in the CIM Schema. " )]
    class CIM_Manag edElement
    {
    [MaxLen(64),Description(
      " The Caption property is a short textual description (one-
      " line string) of the object. " )]
    string Caption;
    [Description(
      " The Description property provides a textual description of "
      " the object. " )]
    string Description:
    };
```

清单 1　CIM-ManagedElement 类的 MOF 定义

图 2 给出一个用 UML 表示 CIM 核心模型的示例，图中 CIM 用“着色编码”的方式表达类结构和对象间的确切关系，如：蓝线表示继承、红线表示关联、绿线表示聚合。

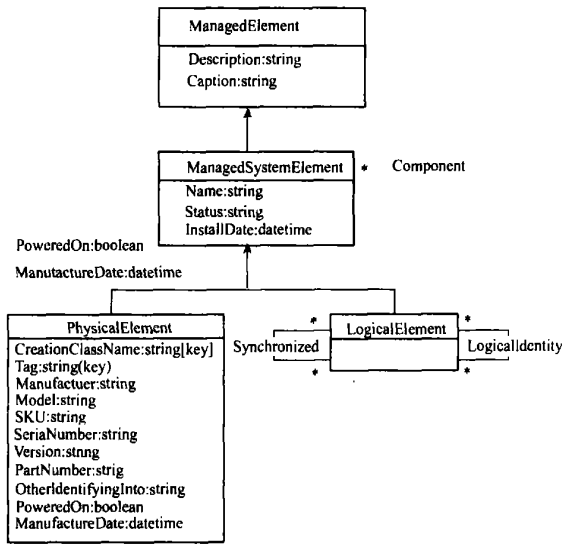

图 2　CIM 核心模型的示例

Fig. 2　The core model of CIM

2.3　应用 CIM 的步骤

应用 CIM 建模和构建系统的过程，接近地反映了 (类似于) 传统面向对象的先建模后编程的开发周期。一般按以下步骤进行：

(1) 用 CIM 为具体应用和实际环境建模，并根据类层次和类与类之间的关联产生 MOF；

(2) 为要求动态数据更新的类构建动态提供者 (Provider)；

(3) 将 MOF 导入 CIMOM (CIM 对象管理器)，并植入类实例要求的任意静态数据；

(4) 此后，便可以通过 CIMOM 的 API 管理系统中的受管对象。

2.4　CIM 的应用领域

以前的应用程序开发者不得不定义各种结构来存储管理信息，他们必须用不同的 API 处理不同来源的对象模型。CIM 利用 UML 和 XML 技术的优势克服了这些问题，它提供了一个统一的管理信息结构，为各种系统通过相同的系统来管理提供了基础。

CIM 的应用领域主要包括两方面：

(1) Manager (管理端) 到 Manager 的交互一作为描述分布式管理系统单元间交换管理信息的方法。

(2) Agent (代理) 到 Manager 的交互一作为来自桌面和服务器系统的管理信息源。

图 3 表明了在一个协议和应用都种类纷杂的大型网络环境中，CIM 能够利用自身的技术优势完全可以在各类综合管理应用系统中胜任“融合信息、统一数据格式”的角色。

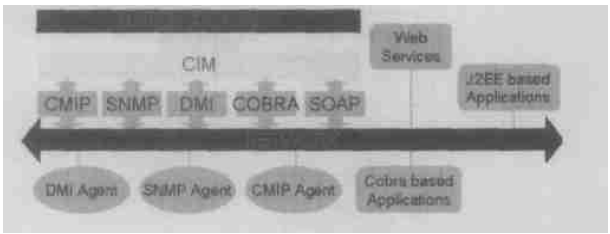

图 3 综合管理应用系统的逻辑架构

Fig. 3 Logical structure of application system of integrated management

3 CIM 在安全管理平台中的应用

众所周知，网络安全是一个“木桶”问题，单靠任何一种安全产品，都不可能做到真正意义上的安全。只有利用平台的综合特性，将各种安全手段汇集起来，实现关联性分析，提高对可疑事件的定位精度和响应速度，才能做到层层设防，处处拦截，迅速歼灭来犯之敌，从而将安全风险降到最低程度。

要建立安全管理平台，第一步就是要确定“统一的数据格式”标准。无疑，遵循业界认可的国际标准是保证与尽可能多厂商的安全产品兼容的最佳途径。尽管已经有一些标准化组织展开了相关的工作，例如：IETF 的入侵检测信息交换格式（intrusion detection message exchange format）和事件对象描述交换格式（incident object description and exchange format）。但令人遗憾的是，这些标准不仅尚处于草案状态，而且只涉及了网络安全的局部领域。

CIM 最初是为服务于网管系统而设计的，而安全管理又是网络管理中五大功能域之一。那么，我们能够将 CIM 应用于目前需要构建的安全管理平台中吗？一个典型的应用实例就是“网威安全管理平台”，该平台正是北京中科网威技术有限公司基于对上述问题的深刻认识，结合自身研发各类安全产品的丰富经验，在采用了 CIM 标准和先进的系统结构的基础上，成功推出的一款分布式网络安全管理平台。

该平台可以用来构建跨地域的多级分布式网络安全管理系统（拓扑示意图见图 4），它主要由：数据处理服务器（data handling server，以下简称 DHS）和用户管理控制台（console）组成，共同管理平台中的多种受管安全设备（如：防火墙、入侵检测系统等）。

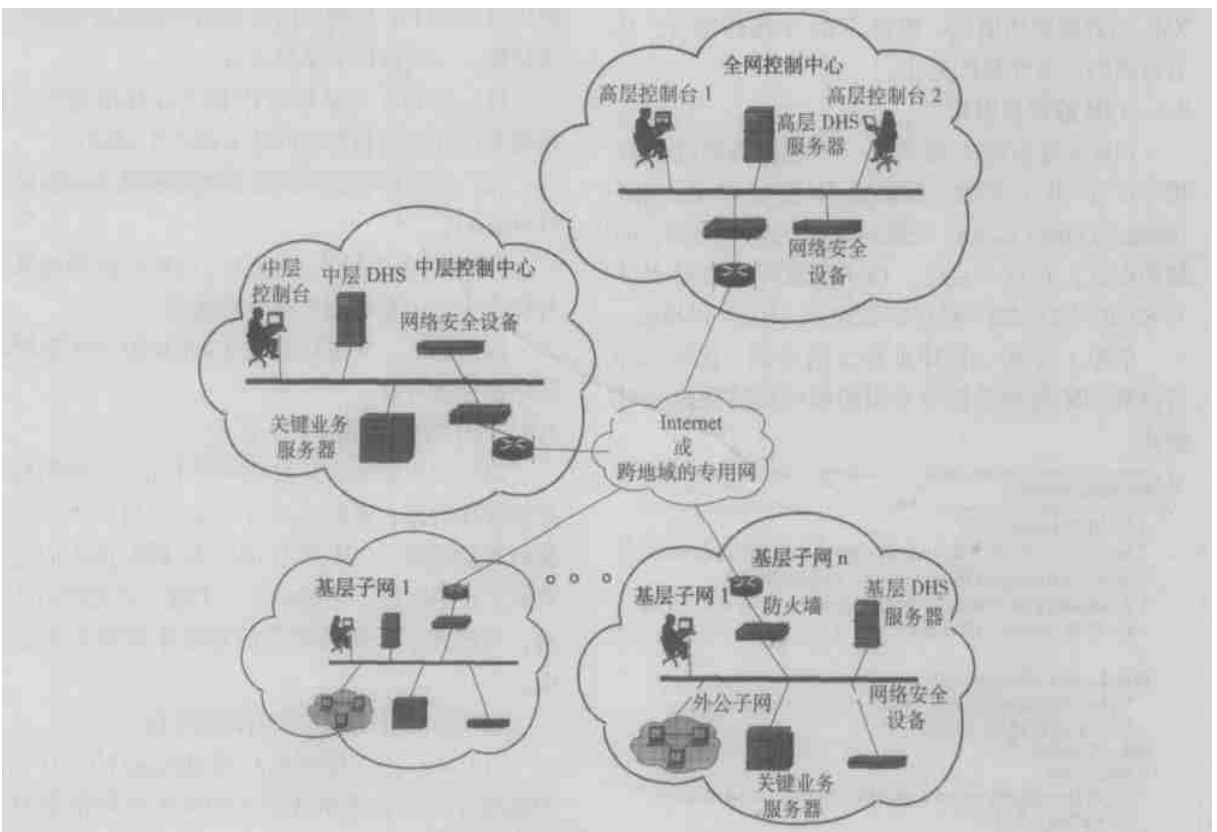

图 4 网威安全管理平台的典型拓扑示意图

Fig. 4 Typical topology of the Netpower Security management platform

整个平台的核心是 DHS（图 5），该服务器具有的如下功能：保存并管理受管设备的 CIM 对象描述信息；初始化并调用与受管设备通信的代理提供程序（providers）；将由受管设备传来的报警及日志信息统一保存在大型数据库（oralce 或 SQL server）中，以备统计分析和数据挖掘；另外，当跨级操作时（如高层 Console 对中层或基层的某个受管设备进行操作时，高层和中层 DHS 将起到信息路由和转发的作用）。一个 DHS 可以同时被多个 Console 连接，每个 Console 都可以同时操作 DHS 可控制的受管要素。Console 和 DHS、DHS 上下级之间采用的是“下订单/过滤器/事件触发”（Subscription/Filter/Indication）的机制，例如，Console 与 DHS 建立连接后，下了关于 NIDS 报警的订单，这样 DHS 只将 NIDS 的 Indication 传送给该 Console，而其他类型的事件在向该 Console 传送前将被过滤掉。

由于平台内部多处使用了插件（plugin）技术，使得系统模块间松散耦合，不仅便于部署，同时便于根据用户的实际需求进行快捷的二次开发。因此，该平台在客户的实际环境中应用过程中，收到了令人满意的反响。

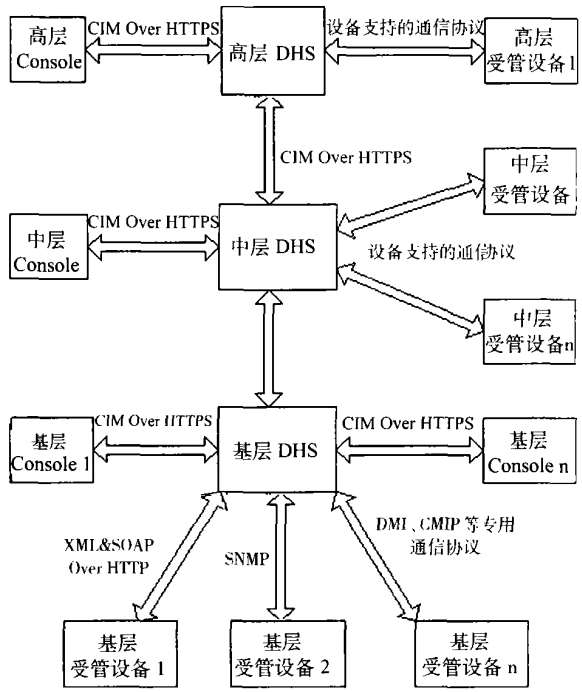

图 5　网威安全管理平台的系统逻辑图

Fig 5　Logical graph of system of the netpower security management platform

4　结　语

通过前面的介绍，可以看到 CIM 在“信息融合”方面具有天然的优势。但要将该技术的优势充分发挥出来，需要在现有 CIM 模型的基础上扩展出一套用于安全管理领域的标准模型。可以预见，随着 XML 逐渐成为国际网络环境中数据交换格式标准的同时，CIM 和其相关的技术标准由于其描述异类数据对象的包容性和扩展性，也将会被越来越多的网络安全管理平台所采用！

参考文献：

[1] CIM 标准 V2.2, DMTF 网站：http://www.dmtf.org/.
[2] XML 标准 W3C 网站：http://www.w3.org/XML/.
[3] UML 标准 Rational 网站：http://www.rational.com/uml/.
[4] MARK A, MILLER P E. 用 SNMP 管理互联网[M]. 第 3 版. 晏明峰等译. 北京：中国水利水电出版社.
[5] Jiro 技术体系结构 Sun 网站：http://www.sun.com/jiro/.
[6] WMI 技术体系结构 Microsoft 网站：http://www.microsoft.com/ntserver/management.

A New Security Management Platform Based CIM

QIAN Jin[1], *LIU Bing*[2]
(1. Department of Computer Science, Wuhan University, Wuhan 430072, China;
2. Beijing Netpower Technologies INC, Beijing 100011, China)

Abstract: Introducing the derivation, theory and characteristics of CIM, the article states the advantages and necessities of adopting CIM in network security management platform. Further more, some successful cases from Beijing Netpower Technologies INC's Security Management Platform supply a further proof of the possibility and meaning that CIM technology is adopted in security management field

Key words: Network security management; CIM; WBEM; XML; UML; SNMP