文章编号:1008-0570(2006)09-3-0128-03

统一通用入侵检测框架的研究与设计

Research and Design on Unified Common Intrusion Detection Framework

(广东建设职业技术学院)钟旺伟
Zhong,Wangwei

摘要:入侵检测是信息安全保障的关键技术之一,本文介绍了目前入侵检测系统中采用的两种通用模型:通用入侵检测框架(CIDF)和入侵检测信息交互格式(IDMEF),在技术上比较了两者的优势与不足,在集中 CIDF 和 IDMEF 优点的基础上,提出一种统一的通用入侵检测框架(UCIDF),用于构造统一的安全管理平台。

关键词:网络安全;入侵检测;入侵检测通用模型;入侵检测交互格式
中图分类号:TP393.08 文献标识码:A

Abstract:Intrusion detection is one of the critical techniques in information assurance. This paper introduces the general situation of the Intrusion Detection System and two kinds of common model used in Intrusion Detection System, including Common Intrusion Detection Framework (CIDF) and Intrusion Detection Message Exchange Format (IDMEF). After the compare between their advantages and disadvantages, one Unified Common Intrusion Detection Framework(UCIDF) is proposed in order to set up one security management platform.

Key words:Network Security,Intrusion Detection,CIDF,IDMEF

技术创新

1 引言

随着网络技术的飞速发展,网络环境变得越来越复杂,网络安全问题日益突出。因而,保障计算机系统、网络系统及整个信息基础设施的安全已成为刻不容缓的问题。目前传统被动防御的防火墙隔离技术已经无法满足对安全高度敏感的部门的需要,入侵检测技术由此应运而生,成为网络安全领域的一项重要技术,发挥着越来越重要的作用。

本文以入侵检测系统为研究对象,紧紧围绕如何增进网络安全系统管理的透明度和可用性这一目标,提出一种统一的通用入侵检测系统框架模型。该模型具有良好的可扩展性,可用于辅助全局网络安全系统的开发,改善网络安全管理的混乱状况,增进企业网络的安全程度,保护企业敏感信息的安全,对企业有非常重要的意义。

2 入侵检测系统介绍

2.1 入侵检测模型

入侵检测是对入侵行为的发觉并做出反应的过程。它通过从计算机网络或计算机系统中的若干关键点收集信息并对其进行分析,从中发现网络或系统中是否有违反安全策略的行为和被攻击的迹象。若有入侵行为发生,做出应急反应。进行入侵检测的软件与硬件的组合便是入侵检测系统 (Intrusion Detection System,简称 IDS)。与其他安全产品不同的是,入侵检测系统需要更多的智能,它必须将所得到的数据进行分析,并得出有用的结果。一个合格的入侵检测系统能够大大简化管理员的工作,保证网络安全的运行。

钟旺伟:硕士 讲师

2.2 入侵检测通用模型(CIDF)

为了使分布于网络中不同主机上的 IDS 能够相互通讯,交换检测数据和分析结果,以检测跨时间段的大范围攻击,提出了一个入侵检测系统(IDS)的通用模型(Common Intrusion Detection Framework, CIDF)。该模型将一个入侵检测系统分为 4 组件:(1) 事件产生器(Event generators):负责从整个计算环境中收集事件,并将这些事件转换成 GIDO 格式传送给其他组件。(2) 事件分析器(Event analyzers):负责分析从其他组件收到的 GIDO, 并将产生的分析结果传送给其他组件。(3) 响应单元(Response units):负责处理接收到的 GIDO,并根据分析结果做出反应,如切断网络连接、改变文件权限、简单报警等应急响应。(4) 事件数据库(Event databases):用来存储 GIDO,以备系统需要的时候查询和使用。

CIDF 模型将 IDS 需要分析的数据统称为事件,它既可以是网络中的数据包,也可以是从系统日志或其他途径得到的信息。以上 CIDF 模型中的 4 个组件代表的都是逻辑实体,组件之间采用统一入侵检测对象(General Intrusion Detection Object, GIDO)格式进行数据交换,其中的入侵检测对象(GIDO)是采用通用入侵描述语言 CISL 进行描述。

2.3 入侵检测交互格式(IDMEF)

互联网工程任务组 (IETF) 的入侵检测工作组

(IDWG)为了提高IDS产品、组件及与其他安全产品之间的互操作性,已经制定了入侵检测信息交换格式(IDMEF)、入侵检测交换协议(IDXP)和入侵报警(IAP)的标准,以便不同类型的入侵检测系统或者不同的检测组件之间能够进行更开放的互相通信。

IDMEF描述了表示入侵检测系统输出信息的数据模型,为不同检测组件之间所交换的各种警报信息,控制命令和配置信息等通讯数据提供了确定的标准表达方式。IDMEF模型中以警报信息Alert为核心,最精简的警报由分析单元(Analyzer)和分类(Classification)两个子类组成。分析单元(Analyzer)子类用于描述警报信息的来源,每个警报都只包含一个分析单元子类;而分类(Classification)子类则描述警报信息的类别及发现的攻击类别。此外,警报还指出产生警报事件的可能来源(Source)和警报事件的可能发送目标(Target)。

IDMEF模型具有很好的可扩充性,该模型的使用者既可以通过聚集的方法进行扩展,也可以通过增加子类的方法进行扩展。

2.4 两种方案的优缺点分析

CIDF模型侧重于描述入侵检测系统的框架,强调模型的通用性和组件之间的相互通讯能力。组件和组件之间通过交换GIDO对象进行通讯,因此CIDF允许不同类型的信息交换,如告警、事件、响应等。CIDF还强调组件的即插即用,并提供了UDP、可靠UDP和TCP三种底层通讯机制,能够很好地支持复杂的网络环境。CIDF的缺点在于没有简单易用的信息模型,其信息模型与CISL语法紧密结合在一起,而CISL是一种使用相对较少的通用信息描述语言。GIDO和CISL的组合既为CIDF带来了良好的通用性和灵活性,同时也带来了复杂性。这是CIDF难以推广的重要原因之一。

IDMEF模型侧重于警报信息数据格式的标准化,也就是说,跨系统的信息交换被局限在不同系统的分析单元和管理单元、管理单元和管理单元之间,信息交换的内容类型也局限于警报信息这一种,因此,IDMEF提供的功能是极其有限的。另外,由于IAP协议是一种基于TCP的类HTTP协议,对系统资源的要求比较高,并不适用于某些必须运行在只支持UDP协议的网络设备上的分析单元,从而限制了IDMEF的适用范围。

3 统一的通用入侵检测框架的设计

3.1 UCIDF模型

综合考虑CIDF模型和IDMEF模型各自的优点,本文在集中CIDF和IDMEF优点的基础上,提出一种新的统一通用入侵检测框架(简称UCIDF)。UCIDF的设计原则是尽量减少安全监测和管理对系统资源和网络资源的消耗,并尽量减少分析单元的复杂性,既要保持CIDF的强大功能和灵活性,又要达到IDMEF的简单性。该模型将一个安全监测管理系统分为两大部分:被监测的网络设备和中央管理系统,具体的模型设计结构如图3-1所示。

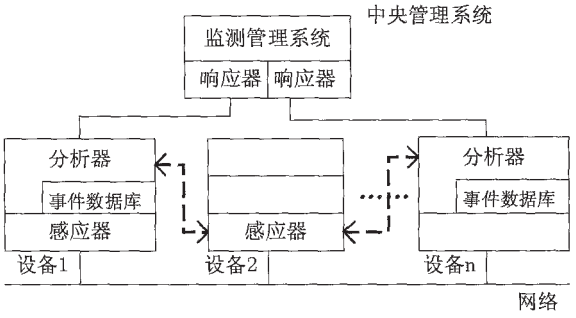

图3-1 UCIDF模型

(1)被监测的网络设备

被监测的网络设备包括硬件设备、感应器和分析器。

① 硬件设备:硬件设备是指与网络安全相关并可用于管理网络的节点,可以是路由器、交换机、网关或被监测的重要主机。可根据网络配置情况和检测需要情况来选择硬件设备。

② 感应器:感应器是一个相对独立的软件单元,可以运行在被监测的网络设备上,从而实现监测网络设备或网络的工作状态。它对应于CIDF中的事件产生器,数据来源既可以是网络中的原始数据包,也可以是来自主机的各种数据。在获取原始数据后,感应器对数据进行简单处理生成事件,然后送往分析器。可根据网络配置情况和检测需要情况安装在单独的一台主机上,也可以各自分布安装在一个网络的不同位置的硬件设备上。

③ 分析器:分析器是负责对感应器采样的事件进行记录和统一分析处理的软件单元。其中的分析方法可动态更换,并且多种算法并存。一个分析器可以对应多个感应器。分析器和感应器既可位于同一设备也可位于不同设备。在分析器中必须包含一个记录可疑事件的事件数据库,以供中央管理系统查询。

(2)中央管理系统

中央管理系统包括响应器和监测系统控制台。在一个被管理的网络中,必须有一个或一个以上的中央管理系统。

① 响应器:响应器对应于CIDF中的响应单元。响应器对确认入侵行为采取相应措施,如断开入侵者与系统的连接,甚至自动关闭系统与外部的连接,发出警报,给管理员发电子邮件,采用反攻击策略等。

② 监测系统控制台:监测系统控制台主要负责安全体系的配置、管理和数据综合功能。监测系统控制台是系统和用户交互的接口,通过它管理员可以管理和配置系统中的各个部件,可以查询各部件的运行情况。由于控制台是用户与入侵检测系统对话的桥梁,

所以要求其界面要友好，把它设计为一个基于 Windows 界面的程序较好。

3.2 UCIDF 实体设计

我们可以将实现 UCIDF 模型的各功能单元称为 UCIDF 实体，为了提高 UCIDF 实体的复用性，应该将 UCIDF 实体设计为具有层次的模块结构。每个实体均包括消息收发、消息处理和安全实施的协议层模块和若干个服务层的模块组成。不同的实体应该具有不同的服务层模块，从而可以提供不同的功能。中央管理系统单元具有命令产生模块和警报响应模块，分析器单元具有命令响应模块和警报产生模块。为了提供更多的服务，实体还可以包括一些其他的功能模块。实体的层次结构设计如图 3-2 所示。

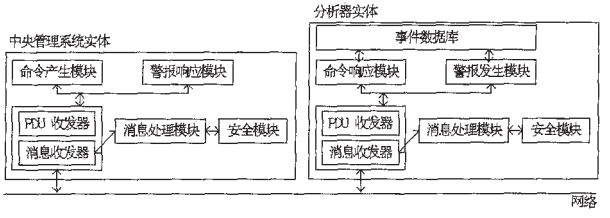

图 3-2 UCIDF 实体的层次结构图。

(1) 消息收发模块(Message Dispatcher Module)：主要功能是①向网络发送消息和从网络接收消息；②判断消息的格式，选择正确的消息处理模式；③提供服务层 PDU 的收发。

(2) 消息处理模块(Message Processor Module)：负责消息发送的准备工作以及从接收的消息中提取数据。

(3) 安全实施模块(Security Implement Module)：负责提供所需要的安全服务。安全实施模块可包含多个安全模式，不同的安全模式可采用不同的认证方法、加密解密方法等。

(4) 命令产生模块(Command Generator Module)：负责监视和处理管辖范围内的事件。

(5) 命令响应模块(Command Responsor Module)：负责提供事件信息。

(6) 警报产生模块(Alert Generator Module)：负责产生警报。

(7) 警报响应模块(Alert Responsor Module)：负责对警报做出反应。

该 UCIDF 模型的实体设计采用了层次结构的设计方式，不仅带来了良好的复用性，而且具有很好的开放性和扩展性。该实体的使用者既可以通过增加新的服务模块提供服务，而且还可以通过增加模块内的模式来适应和兼容新的技术。譬如安全实施模块内可以包含有多种安全模式，用户可选择任何一种，从而提供更多的安全选择。

3.3 UCIDF 的通讯协议设计

入侵检测信息交换格式(IDMEF)的 IAP 协议是不能符合通用性的要求，而 CIDF 采用传输磋商机制进行通讯又显得过于复杂。为了更好地支持 UCIDF 的设计，UCIDF 的通讯协议采用了基于 UDP 的 CIDF 消息机制，同时放弃了 CIDF 模型中原来的传输磋商机制。

采用 UDP 传输服务具有以下几个优点：

(1) UDP/IP 通讯服务能够为 UCIDF 提供路由、端到端校验、分片和重组以及媒介无关功能，使 UCIDF 能够在各种不同的网络平台上运行。

(2) 安全监测管理系统是网络保护的第一道防线，因此，系统本身必须具有在恶劣的网络状态下正常工作的能力。与 TCP 的工作模式比较，UDP 更能适应恶劣的网络。

(3) 如果采用无连接的传输协议，则应用层协议必须保证数据传输的可靠性。由于 UCIDF 采用请求响应的工作方式，超时重发的工作主要由中央管理系统或资源较多的分析器完成，被请求方不需实现这些功能，因此使用无连接协议的开销主要由中央管理系统承担。

(4) 因为 UDP/IP 是因特网的基本网络配置，且占用资源较少，所以 UDP/IP 为 UCIDF 带来通用性的保证。另外由于 UDP 是无连接的，因此它不会产生多余的通讯负载。

由此可知，若采用 CIDF 的传输磋商机制则增加了实体的复杂性和实体所消耗的系统资源，由于 UDP 比 TCP 更适合于提供 UCIDF 所需的通讯服务，因此，放弃 CIDF 的传输磋商机制而采用 UDP/IP 的单一传输机制来设计 UCIDF 通讯协议，是一项有价值的工作。

4 结论

总而言之，本文吸取了 CIDF 和 IDMEF 两个模型各自的优点，克服其缺点，提出了一种新的统一通用入侵检测框架 UCIDF，该模型既具有良好的易用性和可扩展性，也减少了安全监测和管理对系统资源和网络资源的消耗，是一种开发安全监测管理系统的有效手段。随着网络技术的发展、入侵检测系统标准化工作的深入，基于 CIDF 模型和 IDMEF 模型的统一通用入侵检测框架 UCIDF 在安全监测管理系统中必将得到广泛的应用。

本文作者创新点：本文以入侵检测系统为研究对象，在集中 CIDF 和 IDMEF 优点的基础上，提出一种统一的通用入侵检测框架 UCIDF。该模型具有良好的可扩展性，可用于辅助全局网络安全系统的开发，改善网络安全管理的混乱状况，增进企业网络的安全程度，保护企业敏感信息的安全，对企业的网络安全有非常重要的意义。

参考文献：

[1]王杰,王金磊.分布式入侵检测技术在网络控制系统中的应用[J].微计算机信息,2005, 7:90-92

[2]王士乾,李东生.一种分布式入侵检测 (下转第 81 页)

的,攻击者需要多次选择 ID_j,以使得 $H_1(ID_j) = H_1(ID_k)$,其中 ID_k 为代理签名者(真实签名者)的身份信息。但由散列函数的性质可知,这是不可能的。同时,由于代理签名私钥 $S_R = S_W + S_P H_1(W)$ 中包含有代理签名者的私钥信息,因而原始签名者也无法伪造代理环签名。所以,在我们提出的方案中,代理环签名是不可伪造的。

(3)可验证性。从代理环签名生成的过程来看,我们可以得到如下公式

$$\prod_{i=1}^{n} C_i = \prod_{i=1}^{n} e((P_O + P_i)P_{pub}, H_3(C_i)H_1(W))^{H_2(m\|L)} \times e(R_t, P)$$

$$= \prod_{i=1}^{n} e(P_i P_{pub}, H_3(C_i)H_1(W))^{H_2(m\|L)} e(P_O P_{pub}, C_t H_1(W))^{H_2(m\|L)} e(R_t, P)$$

$$= e(P_{pub}H_1(W), \sum_{i=1}^{n} H_3(C_i)P_i)^{H_2(m\|L)} e(P_O P_{pub}, H_1(W)\sum_{i=1}^{n} C_i)^{H_2(m\|L)} e(\sum_{i=1}^{n} R_i, P)$$

$$= e(P_{pub}H_1(W), \sum_{i=1}^{n} H_3(C_i)P_i)^{H_2(m\|L)} e(P_O P_{pub}, CH_1(W))^{H_2(m\|L)} e(R, P)$$

$$= e(P_{pub}H_1(W), CP_O + \sum_{i=1}^{n} H_3(C_i)P_i)^{H_2(m\|L)} e(R, P)$$

因而,代理环签名是可验证的。

(4) 不可否认性。由于代理签名私钥 $S_R=S_W+S_PH_1(W)$中包含有代理签名者的身份信息,所以他不能向原始签名者否认由其生成的有效代理环签名。

(5) 可鉴别性。由于代理签名者本人的公钥与代理签名公钥不同,因而任何人都可区别由代理签名者产生的代理环签名和正常环签名。

4.3 效率分析

在代理环签名生成过程中,本方案和 Zhang 提出的代理环签名方案计算量大致相当,但对于代理签名验证过程来说,本文提出的方案只须进行两次双线性对的运算,然而在 Zhang 的方案中要进行 2n 次运算。如果从计算复杂性的角度考虑,在本方案中,在签名生成过程中,双线性对、G_1 及 G_2 中的群乘法计算量都是 O(n),散列运算及 G_1 中的加法运算量都是 O(1)。对于签名验证过程,双线性对和散列运算的复杂性都是 O(1),然而在 Zhang 方案中,计算复杂性始终都是 O(n)。因而,与 Zhang 提出的代理环签名方案相比,我们的方案所需双线性对运算数目大大减少,计算效率更高。

5 结论

本文的技术创新点在于:指出了 Lang 等提出的代理环签名方案存在两大致命缺陷,从而使得该方案无法实现。同时,设计了一种高效的代理环签名方案,该方案克服了 Lang 方案中存在的问题,能够有效地防止原始签名者伪造代理环签名,较好地满足了代理环签名的安全需求。与 Zhang 提出的代理环签名方案相比,本文提出的方案将签名验证过程中所需的双线性对计算量由 O (n)降低到 O (1),因而执行效率更高。

参考文献:

[1]陈智罡,胡锡伟.基于椭圆曲线的多重盲签名方案[J].微计算机信息,2005,11:58-59

[2]Mambo M,Usuda K,Okamoto E.Proxy signature:Delegation of the power to sign messages. IEICE Trans. Fundamentals, September 1996, E79-A (9): 1338-1353

[3]Zhang Fangguo, Safavi-Naini Reihaneh, Lin Chih-Yin. New Proxy Signature, Proxy Blind Signature and Proxy Ring Signature Schemes from Bilinear Pairings. Cryptology ePrint Archive, Report 2003/104, pages 1-7

[4]Lang Weimin, Yang Zongkai, Cheng Wenqing, et al. A New ID-Based Proxy Ring Signature Scheme. Journal of Harbin Institute of Technology, 2004, 6 (2): 10-15

作者介绍:吕小红(1969-),男,湖北武汉人,武汉理工大学理学院讲师,研究方向为应用数学和信息安全;郎为民(1976-),男,河北馆陶人,华中科技大学电信系博士,通信指挥学院讲师,研究方向为传感器网络、下一代网络和信息安全;夏婧(1979.11-),女,湖北武汉人,华中师范大学数学系硕士生,研究方向为应用数学和信息安全

(430074 湖北武汉 武汉理工大学)吕小红

(430074 湖北武汉 华中科技大学电子与信息工程系)郎为民

(430010 湖北武汉 华中师范大学)夏婧

(Wuhan University of Technology, Wuhan, 430070, China)Lu, Xiaohong

(Department of Electronic and Information Engineering, HuaZhong University of Science and Technology, Wuhan, 430074, China)Lang,Weimin

(HuaZhong Normal University, Wuhan, 430079, China) Xia,Jing

通讯地址:(430010 武汉解放公园路 45# 通信指挥学院装备管理运用教研室)吕小红

(投稿日期:2006.1.25)(修稿日期:2006.2.27)

(上接第 130 页)

系统的设计 [J].太原理工大学学报,2004, (4):456-459

[3]唐屹.基于 CIDF 的入侵检测原型的设计与实现 [J].广州大学学报,2002,(3):35-38

[4]唐正军,李建华.入侵检测技术 [M].清华大学出版社,2004(4)

作者简介:钟旺伟(1976 年生),男,汉族,广东湛江人,讲师,硕士。主要研究方向:网络安全、计算机体系结构及计算机应用技术.E-mail:zhong_ww@163.com

Biography:Zhong Wangwei, Borned in 1976, Male, from Zhangjiang Guangdong, Prelector, Master. Majored in Network Security, Computer Structure, Computer Application.

(510450 广东广州 广东建设职业技术学院计算机系)钟旺伟

(Computer Department of GuangDong Construction Vocational Technology Institute, Guangzhou 510450 China)Zhong, Wangwei

通信地址:(510450 广州市白云区广花二路 638 号广东建设职业技术学院计算机系)钟旺伟

(投稿日期:2006.1.25)(修稿日期:2006.2.27)