基于多Agent的入侵快速响应系统

周世杰，秦志光，张 峰，张险峰，刘锦德

(电子科技大学计算机科学与工程学院 成都 610054)

【摘要】从分析信息安全的现状入手，设计了一个基于多Agent的快速入侵响应系统CI^{2}D&R。结合该系统的网络部署设计，介绍了该系统两个主要组成部分安全间谍和安全警卫的主要功能，并提出了该系统的分层体系结构，分析了系统的主要组成部件及其相应功能，论述了该系统的数据流和接口设计及解决Agent可靠运行的方法。

关 键 词 入侵检测与响应; 多代理系统; 快速响应; 信息安全

中图分类号 TP393 文献标识码 A

A Multi-Agents Based Effective Response System for Intrusion

Zhou Shijie，Qin Zhiguang，Zhang Feng，Zhang Xianfeng，Liu Jinde

(School of Computer Science and Engineering, UEST of China Chengdu 610054)

Abstract Flexible intrusion detection and response system (ID&R) needs to maximize security while minimizing cost and making response automatically. A multi-agents based response system, CI^{2}D&R, the cost-based intelligent intrusion detection and response system, is proposed in this paper, which is originally developed as a facility to deal with network-based attacks and to take effective response automatically and intelligently. The networking environment deployed with the CI^{2}D&R consists of two major parts: Guard, which runs on the specific guarded host (GH), and Spy, which runs in guarded network (GN). The components of the CI^{2}D&R are introduced, which include intrusion detection, attack classification, damage analysis, attack path rebuilding, resources automatically safeguarding, disaster recovery, and security management. The several kinds of data flow in CI^{2}D&R are discussed, too. While CI^{2}D&R is only a prototype, some special safety considerations of agents are also addressed.

Key words intrusion detection and response; multi-agent system; effective response; information security

快速反应及灾难恢复技术是网络主动防御技术的重要内容。作为信息安全有效保护手段之一的快速响应及灾难防御系统应具有入侵模式识别、攻击建模、安全评估以及攻击取证功能，才能对入侵行为进行有效反击[1~3]。有效的入侵响应系统应该提供近似的攻击源定位技术[4]，并采取积极的预防性响应措施，从而可在一定程度上减少攻击带来的资源损失。此外，对信息安全来说，系统还必须具备足够的“灵性”，以应对复杂网络环境中的各种入侵行为。根据上述思想，本文采用多Agent技术，设计了一个协作式入侵检测及响应系统－基于成本的智能入侵回溯及响应系统(Cost-based Intelligent Intrusion Detection and Response System, CI^{2}D&R)[5]。

收稿日期：2003－01－02

基金项目：四川省科技厅项目(01GG0712)；国家863计划资助项目(2002AA142040)

作者简介：周世杰(1970－)，男，博士生，主要从事P2P，信息安全技术，开放系统与中间件技术，工作流技术方面的研究；秦志光(1956－)，男，博士，教授，博士生导师，主要从事开放系统与安全技术，ITS技术方面的研究.

1 CI²D&R系统网络部署设计

一个有效的入侵响应系统应能处理分布式网络环境中的攻击行为。从网络部署来看，CI²D&R系统属于分布式结构。CI²D&R系统分为相互协作的安全警卫(Guard)和安全侦探(Spy)两个部分。其中安全警卫运行在受保护用户主机(Guarded Hosts, GH)上；而安全侦探则分布在受保护网络(Guarded Networks, GN)中，其具体位置可以是网络的关键节点(Key Node, KN)，也可以是网络边界控制节点(Border Node, BN)。

1.1 受保护网络

受保护网络GN由计算机和各种网络连接设备组成，它们可以是逻辑上的独立单位，也可以是物理上的独立单位。在GN的关键节点或者其网络边界的控制点上，安全侦探Spy监控该GN内的数据流，并与特定的安全警卫协作，旨在完成特定的操作，例如切断连接、对指定攻击者发动必要的反击等。受保护网络和与之对应的安全侦探形成了一个逻辑上的安全域(Security Domain)。从整体来看，一个公司、企业或者国家可视为一个广义上的安全域，因此将范围较小的安全域称为安全子域(Security Sub-Domain)，以表示与广义上的安全域的区别。一个安全域包含一个或者多个安全子域，安全子域内可以运行一个或者多个安全侦探。安全域或者安全子域内的计算机等网络资源和系统资源，均受安全侦探的监控和保护。

1.2 安全侦探

安全侦探Spy是分布在安全域中的软件代理，其主要功能是监控网络流量和执行命令。对于网络流量监控，安全侦探对流经该安全域(或安全子域)的数据进行概率采样，并对采样的数据包打上安全标签。当发生网络入侵时，受保护主机可采集这些带有安全标签的数据包，并用数据挖掘的方法识别出攻击源或者攻击源区域即所谓的攻击源回溯。此外，安全侦探也可以和受保护主机上的安全警卫协同工作，执行安全警卫发布的命令或指令，从而对该安全域实施主动保护。

对于关键的安全域，安全侦探也可以具有入侵模式识别、自动保护、入侵事件分类、入侵破坏力分析和灾难性防御能力，从而可以实时地发现入侵，并主动地对入侵进行响应。具备这种能力的安全侦探，称之为智能安全侦探。如果安全域中分布有众多的智能安全侦探，则整个安全域可具备足够的“灵性”，从而可对入侵进行主动响应，并提高网络的安全韧性。

1.3 安全警卫

安全警卫是运行在受保护主机上的代理程序，其主要功能是入侵模式识别、入侵事件分类、入侵破坏力分析、攻击源回溯、自动保护与响应和灾难性防御。

当入侵发生时，安全警卫的入侵模式识别部件被触发，从而实时地检测出受保护主机上出现的各种系统异常或网络入侵事件。安全警卫如具备入侵识别功能，可实时地对受保护主机实施保护，从而提升主机和安全域的安全程度。在整个系统中，入侵模式识别部件是系统的数据采集部件之一，具有特殊的作用和地位。

检测入侵只是标示了入侵的发生。实际上，网络中有很多攻击，一些是无意的，有些则是恶意的，少数攻击对系统来说可能是灾难性的，而大多数攻击可能不会对系统带来太多的危害。如果对不同攻击采用“一视同仁”的响应，其有效性和可实施性很低。因此，安全警卫必须对检测到的入侵或者系统异常进行分类，并依据系统的安全策略和安全机制，对分类后的入侵进行智能分析，从而为进一步的处理提供可靠的基础信息。

破坏力分析是根据入侵事件分类[6, 7]，采用相应的算法，定性计算该入侵可能带来的系统资源或服务损失。破坏力分析是这个系统的关键，只有确定了入侵可能给系统带来的破坏程度，才能采取正确而有效的对抗措施，避免系统误反应或过激响应。目前，入侵破坏力的定量分析还没有很好的自动生成算法，主要根据系统参数，由安全专家给出近似的经验值。

在许多情况下，如果能正确标记和证实攻击源的身份，则不仅可提供有用信息来对攻击源实施主动、有效的响应，也可作为法律上的证据，使攻击者受到法律的惩罚。因此，安全警卫必须能够准确、实时地识别出攻击源。但是，由于目前TCP/IP系统自身的协议缺陷，不能单纯依靠安全警卫来标示攻击源。安全警卫只有与安全侦探通力协作，才有可能正确回溯地回溯到具体攻击源或者近似的攻击路径。在安全战略

预警系统中，即使是粗略的近似攻击路径，也可提供攻击源物理位置的有用信息，安全管理员可据此调整路由器或者防火墙的安全策略，从而在一定程度上减少攻击的危害。

在传统意义上，安全防护主要侧重于被动防御。由于消极防御安全手段缺乏智能性，因而不能有效地保护网络资源。为了提高系统的灵活性和智能性，安全警卫必须具备自动保护与主动响应能力，在受到可预测的攻击或破坏力较小的攻击时，主动保护系统，使系统服务优美降级；而在受到严重的灾难性攻击时，则可对攻击进行主动响应，提供系统资源或者关键服务的自动保护。

保护关键系统时，安全警卫应该具备灾难性防御能力。如果安全警卫识别出系统正遭受灾难性的攻击(甚至是系统异常)，则可以利用自动保护装置，使系统服务优美降级，从而在一定程度上减少系统损失。在自动保护失效时，灾难恢复功能则可保证对遭受灾难性破坏的系统快速恢复。灾难防御是系统最后的一道安全屏障，它在攻击检测与防范失效的情况下，可提供系统关键资源的快速恢复功能，从而确保信息资源的持久可用。

2　系统结构设计

图1是根据功能设计的CI^{2}D&R系统的分层结构示意图。在结构设计中，入侵检测Agent主要完成入侵模式识别功能；攻击源回溯Agent主要完成攻击源的回溯及记录功能；自动保护Agent在系统受攻击时进行自动保护，减少系统的损失，并使破坏最小化和局部化；灾难恢复Agent对系统进行灾难保护和恢复；快速反应Agent对攻击进行快速有效的反击和响应，并执行自动报警功能；攻击事件分类及形式化描述研究对攻击进行分类管理的方法，并为其他Agent提供参考信息；破坏力分析研究入侵的定量描述方法，并为其他Agent提供参考信息；安全策略管理则是研究如何提高系统的灵活性和适应性，属于用户界面性质的Agent。目前，对通信设施主要采用操作系统提供的TCP/IP服务。

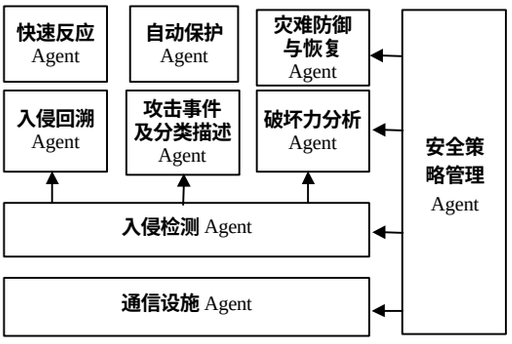

图1　系统组成结构示意图

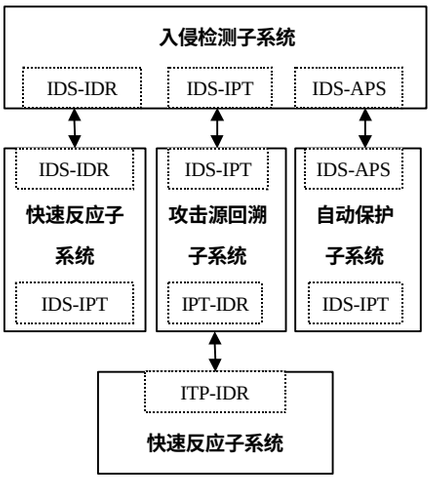

图2　系统内部接口示意图

3　系统接口设计及可靠性设计

依据系统体系结构，CI^{2}D&R系统的内部接口主要包括IDS Agent与攻击源回溯Agent之间的接口、IDS Agent与快速反应Agent之间的接口、IDS子系统与自动保护Agent之间的接口，以及攻击源回溯Agent与快速反应Agent之间的接口。

接口的实现可考虑采用接口Agent，这样可保证系统的可扩展性和适应性，并保证系统设计的结构化属性。在图2中分别标识了对应的接口Agent的逻辑位置。

这些接口之间包括信息流核控制流的交换，接口之间的消息交换由对应的接口Agent来实现，其对应关系如图2所示。IDS拥有三个接口Agent，如果IDS Agent意外中止，则将严重危及系统的健壮性和可靠性，因

此必须保证该Agent的可靠运行。CI²D&R系统目前没有考虑Agent的错误恢复问题，但可采用“挽救进程”方式来保证系统关键Agent的稳定性和可靠性。其基本原理是在每一关键Agent运行的主机上，均有一可称之为挽救进程的后台进程与之对应。挽救进程负责监视被保护Agent的生命周期，并以一定周期通过预定端口定时检查其状态。当Agent在规定的时间内没有响应时，挽救进程加快发送信号的频率。如果Agent仍然没有响应时，在发送一组信号之后，就假定该Agent失效。

4 结 束 语

目前，CI²D&R系统已经完成了原型设计，各Agent自成体系，可独立运行，也可相互协作。入侵模式识别采用开源的Snort系统，入侵源回溯采用包采样标记技术[4]，系统提供自动反击、自动报警、自动保护(包括文件保护、服务保护、系统保护和网络保护等)和包括灾难恢复在内的多种主动响应方式。测试结果表明，该系统对受控网络中的攻击，可进行快速源回溯；对可识别的入侵，根据系统安全策略进行有效的响应；对未知的或不可识别的灾难性攻击，实施系统的自动保护和报警，并在必要时提供资源恢复功能。

参 考 文 献

[1] Schnackenberg D, Holliday H, Smith R, *et al*. Cooperative Intrusion Traceback and Response Architecture (CITRA)[C]. In: Proceedings of the DARPA Information Survivability Conference and Exposition, Anaheim, 2001

[2] Schnackenberg D, Djahandari K, Sterne D. Infrastructure for intrusion detection and response[C]. In: Proceedings of the DARPA Information Survivability Conference and Exposition, Hilton Head, 2000

[3]Dipankar D, Fabio A G. An intelligent decision support system for intrusion detection and response[C]. Lecture Notes, Petersburg, 2001

[4] Savage S, Wetherall D, Karilin A, *et al*. Practical network support for IP tracebak[C]. Proceedings of the 2000 ACM SIGCOMM Conference, Stockholm, 2000

[5] Zhou Shijie, Qin Zhiguang, Lu Qin, *et al*. CI²D&R:Cost-based intelligent intrusion detection and response system[C]. In: Proceeding of 2002 5th International Conference on Algorithms and Architectures for Parallel Processing, Beijing, 2002

[6] Domingos P. MetaCost: a general method for making classifiers cost-sensitive[EB/OL]. http://www.gia.ist.utl.pt/~pedrod, 1999-08-05

[7] Wenke Lee. Toward cost-sensitive modeling for intrusion detection and response[J]. Journal of Computer Security, 2000, 10(1): 5-22

编 辑 熊思亮