第 32 卷 第 14 期 计 算 机 工 程 2006 年 7 月
Vol.32 № 14 Computer Engineering July 2006
·安全技术· 文章编号：1000—3428(2006)14—0166—03 文献标识码：A 中图分类号：TP393.08

多类型安全系统协同机制的研究与实现

刘庆云，杨超峰，刘利军
(北京航空航天大学计算机学院，北京 100083)

摘 要：为了综合不同的安全技术系统进行协同防护以增强整体防护能力，设计了一种统一的多类型安全系统协同机制，利用协同规则描述协同信息，信息总线传递协同数据，执行引擎完成协同操作，可以统一地支持多类型安全系统的协同功能的实现。实验结果表明该协同机制能有效地实现不同安全系统之间的协同功能，并具有通用性、可配置性和可扩展性强的优点。

关键词：协同机制；协同规则；信息总线

Research and Implementation of Multi-security-systems Cooperation Mechanism

LIU Qingyun, YANG Chaofeng, LIU Lijun
(School of Computer, Beijing University of Aeronautics and Astronautics, Beijing 100083)

【Abstract】 In order to enhance the security of network by using multi-security technologies, this paper designs and realizes a uniform security cooperation mechanism. This mechanism uses cooperation rules to describe cooperation information, uses information bus to exchange relative data, and make use of cooperation engine to realize the dynamic configuration and cooperation option. According to intensive tests, this cooperate mechanism can realize the cooperation between different security products easily, and can be deployed and expanded flexibly.

【Key words】 Cooperation mechanism; Cooperation rule; Information bus

近年来，已有一些著名的安全厂商推出不同的网络安全管理平台来实现多种安全系统的综合管理[1,2]，如赛门铁克(Symantec)的集中开放式安全管理系统(SESA)、IBM 的 Tivoli、启明星辰的网络安全资源管理平台等。但是，不同的安全产品系统结构和管理接口没有统一的标准，平台所管理的不同系统之间是松散集成的关系。不同产品之间的协同也只停留在对几种产品的日志信息进行统计分析的层面上，没有更深入有效的有机协同机制。虽然有些系统实现了一定程度的系统间协同[3~5]，但只是针对具体的安全系统，没有提出统一的协同机制，同时，协同的实现基本采用在系统内部进行硬编码的方法，极大地限制了系统的灵活性和可扩展性。

本文在深入研究不同安全系统结构和协同原理的基础之上，设计实现了一种统一的多类型安全系统协同机制，利用协同规则描述协同信息，信息总线传递协同数据，执行引擎完成协同操作，可以统一地支持多类型安全系统的协同功能实现。

1 通用安全协同机制设计实现

不同安全系统之间的协同操作按照协同效果的不同分为验证协同和响应协同。验证协同是指对于一个安全系统分析出的结果，调用另一安全系统来验证该分析结果的准确性。比如：入侵检测系统与漏洞扫描系统进行协同来检验入侵的真实性属于验证协同。响应协同是指根据一个安全产品分析的结果，触发另一种安全产品来采取相应的安全响应措施。入侵检测系统触发防火墙系统来阻断有入侵行为的主机的连接以保障网络的安全属于响应协同。

本文重点研究如何动态地调用不同的安全产品协同完成安全防护，主要解决如下两个问题：(1)不同系统的动态部署管理，协同机制能够自动根据不同系统的部署和运行情况做出动态调整，无须人工干预；(2)系统协同信息的统一描述解析机制，使得协同信息的描述和处理机制与具体的系统无关。为此给出了一种统一的多类型安全系统协同机制，由运行系统链表、协同请求队列、信息总线、规则解析引擎和协同执行引擎等部分组成，总体结构如图 1 所示。

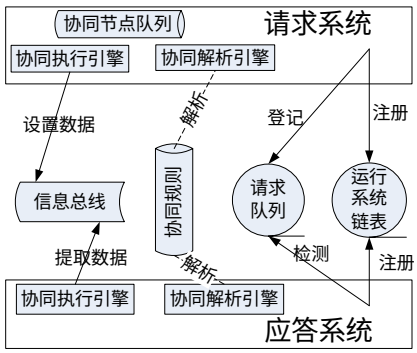

图 1 安全协同机制总体结构

1.1 协同规则设计

为了描述不同安全系统之间的协同操作，需详细地描述协同双方、协同条件和协同数据等信息，我们用安全协同规则来统一描述不同系统间的协同信息。协同规则由请求系统、应答系统、协同条件、协同数据、协同控制 5 个部分组成。

基金项目：国家“863”计划基金资助项目（2003AA144150）
作者简介：刘庆云(1980—)，男，硕士生，主研方向：网络安全；杨超峰，硕士生；刘利军，博士生
收稿日期：2005-07-10 **E-mail：**liuqy@act.buaa.edu.cn

(1)请求系统指发起协同请求的系统，协同发起方负责判断是否满足协同条件，准备相应的协同数据；

(2)应答系统指响应协同请求的系统,负责解析得到的协同数据，执行相应的协同动作；

(3)协同条件是指请求系统准备协同数据，触发协同动作之前需要检测的条件；协同条件只描述了具体系统发出协同请求需要满足的条件。应答系统的运行状态是协同发生的必备条件，不在协同规则当中描述；

(4)协同数据是指协同双方需要交互的有关数据信息；

(5)协同控制用于配置本条协同规则是否使用。协同操作的引入，增强了系统的功能，但是不可避免地消耗了系统的资源，影响了系统的检测效率，对于不同的用户，由于出发点不同，侧重点不同，导致对效率和准确率的需求不同，因此提供协同控制字段，使得用户可以在不同时刻根据自己的需要配置不同的协同规则的使用，达到预期的结果。

采用统一的协同规则描述机制，屏蔽了对具体操作细节的描述，减轻了对系统的依赖，提供了良好的扩展功能。

1.2 信息总线

为了实现不同安全系统之间的协同操作，需要在不同的系统之间进行数据的交互，为了提高信息交互的效率，我们设计并实现了一种通用的信息总线来实现数据的动态交互。

信息总线是一种格式化信息存储线性逻辑结构，记为L，用于动态地储存安全系统协同过程中需要在不同系统间传递和交换的数据信息，以有效地支持各种相关信息的协作与交换。该信息总线由一系列逻辑信息格（grid）组成，即$L=\{grid_i \mid i>0, i\in N\}$，其中信息格$grid_i$是信息总线中最小的逻辑存储分配单元。

我们根据发生协同的不同系统类型组合将协同数据存储区中的信息分为不同的段（segment），每个段根据协同数据结构的差异由不同数量的信息格组成。L 中的存储单元用于存储在不同安全系统间执行协同功能时需要的协同通信数据，由于能够完成的协同服务以及协同消息的格式都是在协同服务请求引擎和服务提供引擎之间约定好的，即这类信息的存储需求是固定的，因此对 L 中信息格的管理采用静态分配策略。静态分配策略的工作原理如下：

系统管理员在系统的协同规则中描述了不同安全系统之间的协同关系和协作时需要交互的数据项，每个系统的引擎在启动并实例化时会根据协同规则中描述的协同语义，在引擎实例的内存资源中为能够与该引擎发生协作关系的子系统引擎顺序分配相应的段，用以存储它们在协同完成扫描分析任务时需要交互的协作数据。由于段空间的分配是引擎在实例化时根据协同规则描述的协作需求进行计算并分配的，是必然满足协作需求的，引擎实例化过程中进行段分配以后在该引擎实例运行期间不再进行调整，因此是属于静态分配的策略。

采用信息总线规范了协同系统间交互信息的描述方式，为统一的安全协同机制奠定了实现基础。

1.3 协同规则解析引擎设计

协同规则解析引擎负责解析协同规则，初始化协同系统的部署地址，并动态监视协同系统的运行情况，具体可以分为请求解析引擎和应答解析引擎。实际实现中请求解析引擎和应答解析引擎可以共存在一个系统实例当中。

请求解析引擎工作流程如下：

(1)查询协同规则数据库中的规则，获取等于本系统编号的请求系统编号的规则。查询为空，转(6)。

(2)创建协同节点，加入协同节点队列。初始化协同节点中的系统编号为协同规则中的应答系统编号。

(3)在运行系统列表中查询应答系统的运行状态，如果系统正常运行，获取系统的运行配置情况，填入协同节点，并设置协同节点中系统运行状态为正常运转；否则给出提示信息，设置系统运行状态为停止。

(4)在请求队列中登记请求信息。

(5)按照协同规则中的协同数据初始化信息总线；转(1)。

(6)监听所有应答系统的运行情况。

应答解析引擎工作流程如下：

启动时：

(1)向运行系统列表注册本系统的服务信息，标记本系统为运行状态。

(2)检测请求系统链表，向请求列表中应答系统为本系统的请求系统发送运行命令。

退出时：

(1)检测请求系统链表，向请求列表中应答系统为本系统的请求系统发送停止命令。

(2)从运行系统列表注销本系统服务信息。

利用统一的协同规则描述和解析引擎机制，使得系统间的协同语义可以灵活地配置，当改变一个子系统的部署情况的时候，无须对其他要求协同的子系统进行修改，而且当不同的系统改变运行状态时，其他系统也可以自动地调整协同策略，无须人工干预，这种解析方式减轻了管理员的负担，提高了系统的灵活性和效率。

1.4 协同执行引擎设计

协同执行引擎按照协同解析引擎解析的协同规则，调动控制协同动作的执行过程。不同引擎在执行扫描过程中通过扫描信息总线进行引擎间协作的执行机制设计，原理如图 2。

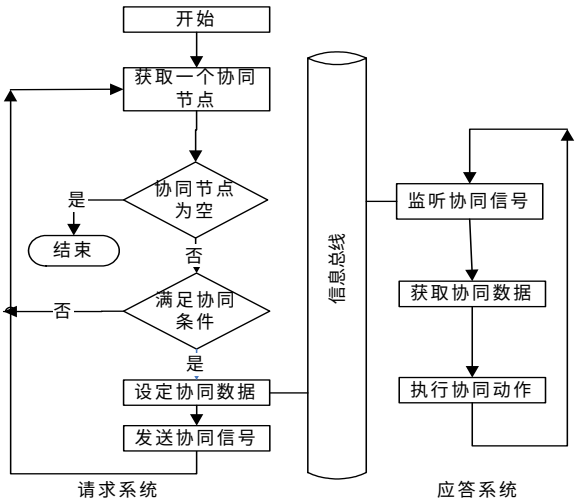

图 2 协同操作执行流程

协同请求方的工作流程如下：

(1)从协同队列当中获取一个协同节点，节点为空转(5)；

(2)检测协同条件，不满足协同条件转(1)；

(3)在信息总线的特定位置设置协同数据；

(4)发送协同信号，转(1)；

(5)结束协同。

协同应答方工作流程：

(1)监听特定的协同信号；

(2)从信息总线获取协同数据；

(3)执行相应的协同动作，转(1)。

在上述过程中，协同条件是在协同规则中描述的，协同

数据项也是在协同规则中描述的，但具体的协同数据在执行扫描的上下文场景中获得。另外，协同请求方和协同应答方可以分别处于网络中不同的主机上。实际中，信息总线在协同请求方（请求引擎）和协同应答方（应答引擎）的运行空间中各自有一个实例，但其结构和其中存储的数据是完全相同的，因此在图 2 中以单一的逻辑概念表示。

2 测试结果和实验数据

2.1 协同实例实现

下面以入侵检测与漏洞扫描、入侵检测与安全审计系统的协同作为实例介绍上述统一协同机制的实现。入侵检测系统在检测到入侵以后调用漏洞扫描系统验证入侵的真实性，调用安全审计系统记录入侵者的所有操作动作。定义两条协同规则如表 1。

表 1 协同规则实例数据

编号	请求系统	应答系统	协同条件	协同数据	协同控制
1	入侵检测系统	漏洞扫描系统	Sid	HostIp；CVE；	是/否使用
2	入侵检测系统	安全审计系统	Session	Srcip；Srcport；Dstip；Dstport；	是/否使用

协同条件中的 Sid、Session 是入侵检测系统初步分析产生的结果信息中可能包含的关键词，如果入侵检测分析结果内含有相应的关键词则执行相应的协同规则。

协同数据中 HostIP 是主机地址，CVE 是漏洞标准编号，漏洞扫描系统可以检查 HostIP 指定的主机是否包含有 CVE 编号指定的漏洞。安全审计系统可以记录由源 IP（Srcip）、源端口(Srcport)、目的 IP(Dstip)、目的端口(Dstport)共同确定的链接上的数据。

2.2 测试环境和步骤

为测试安全协同机制的功能，设计如下测试场景。测试环境包括 6 台 PC 机，带宽为 100Mbps 的以太网满负荷运行。各系统配置及功能如下：

5 台 PC 机（A1、A2、A3、A4、A5）运行 Redhat Linux 9.0 操作系统，一台 PC 机(B1)运行 Windows 2000 操作系统。

A1 运行入侵检测系统；A2、A3 分别部署漏洞扫描和安全审计系统。A4 执行我们开发的发包工具 PacketSender，模拟网络流量负载；A5 运行攻击模拟工具 snot，模拟入侵。B1 执行管理控制台程序，用于配置协同规则的使用。

目标 测试协同功能的正确性。漏洞扫描系统对入侵的验证能减少入侵检测系统的误报警。安全审计系统能正确地记录相应的数据。

步骤 在 A2 主机上部署安全审计系统，在 A3 上部署漏洞扫描系统。在不启用协同规则的情况下，用 snot 模拟入侵数据包多次。统计入侵报警中能够满足漏洞扫描协同条件的报警数目和满足安全审计条件的入侵测试。启用协同规则，重复入侵模拟，观察启用协同的结果见表 2。

表 2 协同测试数据结果

	模拟入侵次数	满足规则 1 协同条件的入侵数	满足规则 2 协同条件的入侵数	触发漏洞扫描次数	记录审计文件数目	最终报警数目
不启用协同规则	12	8	6	0	0	12
启用协同规则	12	8	6	8	6	6

表 2 数据显示，模拟的 12 次入侵中满足协同规则 1 的 8 次入侵成功地触发了漏洞扫描系统 8 次，经过扫描器扫描验证以后，最终报警从 12 次下降到 6 次，减少了报警次数。满足协同规则 2 的 6 次入侵报警触发审计系统 6 次，成功记录文件 6 次，为事后审计提供了有力的证据。

2.3 试验结果分析

从实验结果可以看出，入侵检测系统与漏洞扫描系统的协同，能够起到对入侵报警进行验证的功能，有效地减少了误报警，提高了检测准确率。入侵检测系统与安全审计系统的协同，能够记录相关的数据信息，为事后审计提供了有力的证据。

实验表明，本文中提出多安全系统统一协同机制能够有效地支持不同安全系统之间协同功能的实现，增强了整体防护的效果。在实验中同时可以验证，用户可以在控制台方便地配置协同规则是否使用，就能控制协同动作是否发生；同时系统应答系统的部署改变后，不需要重新配置请求系统，即可自动完成协同工作，增强了系统协同功能的易配置性。

3 总结

为了综合不同的安全技术系统进行协同防护以增强整体防护能力，本文设计并实现了一种统一的多安全系统协同机制。该机制独立于特定类型的安全系统，能够统一地支持多类型安全系统的协同功能实现。该机制已经应用在我们研制的综合安全监控管理平台 ACT-BroSA 中，有效地实现了入侵检测、漏洞扫描、安全审计等多种安全监控系统之间的有机协同互动，并具备通用性、可配置性和可扩展性强的优点。

参考文献

1 孟庆华，管　文，沈昌祥等. 大规模网络协议层协同安全管理研究模型的研究[J]. 计算机应用, 2004, 24(2): 30-32.

2 蒋文保，王常吉，杨大鉴等. 多组件协作式网络安全系统的分析与设计[J]. 计算机工程与应用, 2002, 38(23): 172-175.

3 王丽娟，任新华. 入侵检测及基于协同式的入侵防范[J]. 太原理工大学学报, 2001, 32(2): 182-184.

4 刘默玲，邹红军. 一种网络安全系统的研究[J]. 武汉大学学报(工学版), 2002, 35(3): 100-103.

5 段海新，吴建平. 一种分布式协同入侵检测系统的设计与实现[J]. 软件学报, 2001, 12(9): 1375-1379.

（上接第 150 页）

参考文献

1 张　宏，陈志刚. 一种新型一次性口令身份认证方案的设计与分析[J]. 计算机工程, 2004, 30(17): 112-113.

2 Menezes A J, Oorschot P C , Vanstone S A. Handbook of Applied Cryptography[M]. CRC Press, 1997.

3 Abadi R, Mark R. A Semantics for a Logic of Cryptographic[C]. Proceedings of the Tenth ACM Symposium on Principles of Distributed Computing. ACM Press, 1991-08: 201-216.

4 Syverson P, Paul C, Oorshot V. On Unifying Some Authenticati on Protocol Logics[C]. Proc. of IEEE Computer Society Symposium on Research in Security and Privacy, 1994-05: 14-28.