基于代理的协同结构网络安全对抗模型*

陈 文 斌
(中山大学软件研究所, 广东 广州 510275)

摘 要: 研究目的是建立一套能在互联网上进行协同攻防演练的网络安全平台。所建模型在可复用的构架下, 实现了移动代理与现在成熟安全软件技术的结合, 在一定程度上提升了现有安全软件设计的技术和理论层次。

关键词: 网络攻击; 网络防御; 移动代理; 协同
中图分类号: TP309 文献标识码: A 文章编号: 0529-6579 (2005) S1-0142-04

近年来, 网络系统的规模、复杂度和易受攻击程度大幅成长。在这种分布的环境下, 网络攻击需要协同, 网络防护需要协同, 攻击和防护之间也需要协同, 协同是未来网络对抗的发展趋势。事实上, 国内尤其在协同网络攻击方面的研究很少, 国家和大型机构等都需要更多创新的解决方案进行安全测试、攻防演练和研究, 才能处理现在和未来的各类威胁。

本文基于网络安全的定义, 对基于协同结构的网络安全对抗系统模型设计和建立进行描述, 主要分为协同网络攻击模型和协同网络防御模型。模型着重研究了基于移动代理 (Agent) 的协同攻击, 同时结合专家系统和入侵检测系统技术, 模型具有攻防平台统一性、功能伸缩性和性能智能化等特点。

1 协同网络安全对抗模型设计

一个合理的网络对抗模型应该既可以发动攻击, 又可以防御各种攻击。如图 1 所示是协同式网络安全对抗模型。

模型建立在支持平台之上, 支持平台则由信息基础设施、分布式计算技术和网络安全评估等环节构成。信息基础设施提供了网络对抗的环境; 分布式计算技术则为分布式环境下的网络攻击和防御创造了条件; 在网络攻击和防御过程中, 需要网络安全评估平台的支持, 对当前状态进行评估和响应。。

1.1 网络安全体系设计原则

安全攻击、安全机制和安全服务三者之间的关系如表 1 所示。

针对一个信息网络系统, 如果在各个系统单元都有相应的安全措施来满足其安全需求, 则认为该信息网络是安全的。我们将安全防范体系的层次划分为物理层安全、系统层安全、网络层安全、应用层安全和安全管理。

表 1 安全攻击、安全机制和安全服务

Tab. 1 Safe attack, safe modcl and safe service

释放消息内容	流量分析	伪装	重放	更改消息	拒绝服务	安全攻击 / 安全机制 / 安全服务	加密	数字签名	访问控制	数据完整性	认证交换	流量填充	路由控制	公证
		√				对等实体认证	√	√			√			
		√				数据源认证	√	√						
		√				访问控制			√					
√						机密性	√						√	
	√					流量机密性	√					√	√	
			√	√		数据完整性	√	√		√				
						非否认服务		√		√				√
					√	可用性				√	√			

* 收稿日期: 2005-02-02
作者简介: 陈文斌 (1971 年生), 男, 研究生; E-mail: banksg@gmail.com

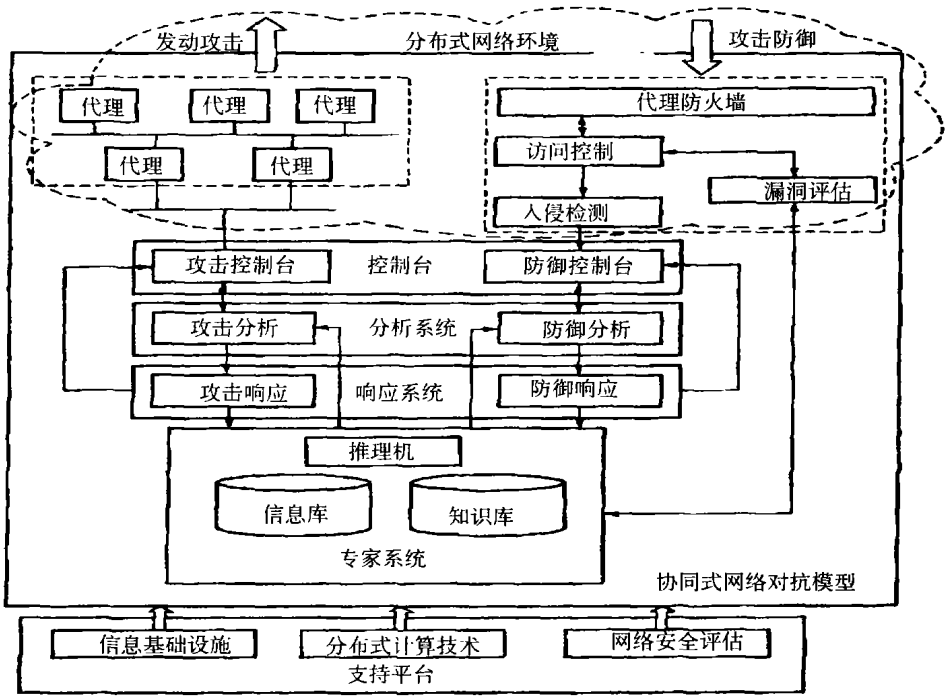

图 1　协同式网络安全对抗模型

Fig. 1　Coordination structure network safe countermodel

网络安全防范体系在整体设计过程中应遵循以下 9 项原则：1. 网络信息安全的木桶原则；2. 网络信息安全的整体性原则；3. 安全性评价与平衡原则；4. 标准化与一致性原则；5. 技术与管理相结合原则；6. 统筹规划，分步实施原则；7. 等级性原则；8. 动态发展原则；9. 易操作性原则。

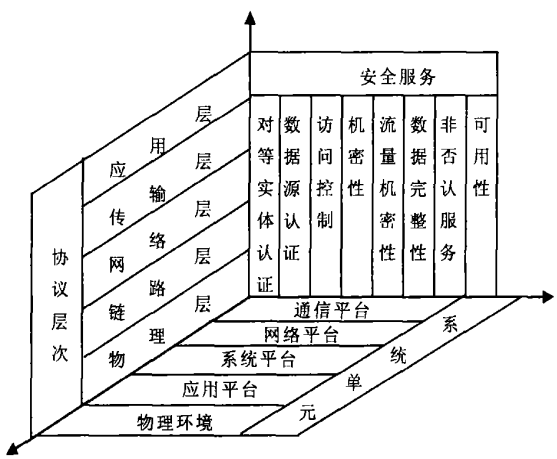

图 2　三维安全防范技术

Fig. 2　3D safe defence technology

1.2　协同式结构

协同式结构（如图 3 所示）的定义：一个有限集合 L，数量为 n，对于分布的每一个节点 l，都有 $l \in L$，在协同式的结构中，每个 l 都有一个代理（Agent）。

由叶节点完成信息收集和攻击，信息经过中间节点发送和返回，根节点将信息汇报给用户控制台，是一个作出攻击和防御响应的命令控制系统，发布命令、确定反应措施和位置。

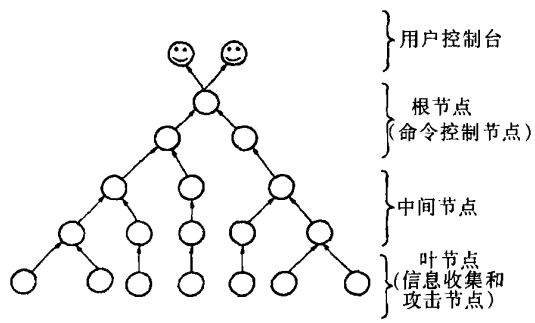

图 3　协同式结构

Fig. 3　Coordination structure

1.3　移动代理（Agent）形式化定义

为了便于任务分解算法对任务的处理，网络任务定义接口首先对任务进行简单的形式化抽象，主要包括以下几个定义。

网络管理任务：一个网络管理任务由多个子任务组成，网络管理任务用 T 表示。

数据依赖：服务单元作为数据库的记录存储在数据库中，每一服务单元都有其永久依赖集和临时

依赖集。无论在何种网络管理任务中，某一服务单元都需要一组服务单元的执行结果，这组服务单元称为这一服务单元的永久依赖集。临时依赖集是指在本次管理任务流程中，某服务单元需要一组服务单元的执行结果，这组服务单元称为此服务单元的临时依赖集，临时依赖集可以依据永久依赖从管理任务的定义中提取。永久依赖集用（sd1，sd2….）表示，临时依赖集用（td1，td2….）表示。总之，服务单元必须在它的临时依赖集执行之后执行。服务单元之间的这种次序关系称为数据依赖。

子任务：子任务用（Ti，Si，Ai）表示，T（Task）代表子任务所属的总任务，S（service）代表子任务所用的服务单元，A（Address）代表子任务被执行的网络地址，也可能是一组节点地址，网络管理任务与网络中的位置密不可分，所以我们把 Address 作为子任务的一个元素。

Agent 状态：本文所描述的 agent 状态表示为（g，T，S，A，R），表示名字为 g 的 agent 在 IP 地址为 A 的网络节点上执行任务 T 中的子任务 S，其中 R 为一布尔变量，R 为 0 时表示子任务 S 已完成，R 为 1 时表示子任务 S 正在执行。

1.4 移动代理（Agent）结构

本文所描述的多移动代理技术是一种新型的分布式网络计算模式，它很好地解决了网络间任务分配合作的问题。移动代理是指能在同构或异构网络主机之间自主地进行迁移的有名字的程序。程序能自主地决定什么时候迁移到什么地方。

由于移动代理是一些驻留在漏洞主机上的小程序或代码片段，只要解决移动代理之间以及和后台程序间的安全通信问题，则很容易建立、撤消、迁移和维护。同时，后台的专家系统能对新增的安全事例进行学习。所以，本模型具有快速适应目标系统的变化的优点。

移动代理有许多独特的特性：①主机间动态迁移；②智能性；③平台无关性；④分布的灵活性；⑤低网络数据流量；⑥多代理协作；

协同式网络攻击和防御的自动控制是利用协同式 IP 网络上客户/服务（Client/ Server）的特性完成，有多个移动代理（Agent）嵌入驻留在拓扑结构独立的主机上，在逻辑上统一地集中化管理攻击者和防御者之间传输的安全信息。协同式体系结构能有效创建一个集中控制和大规模的智能化的攻防系统平台。

2 协同网络攻击模型的主要思想

协同式网络攻击模型主要包括 4 部分：用户端、攻击控制引擎、接口（拨号）工作站、代理。模型如图 4 所示。

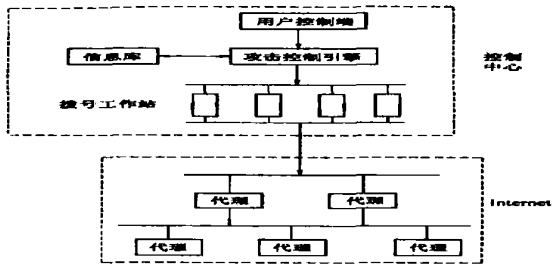

图 4 协同式网络攻击模型

Fig 4 coordination structure network attack model

（1）用户端是整个模型与用户交互界面，用户通过控制端了解控制攻击的情况。

（2）攻击控制引擎（ACE，Attack Control Engine）是负责协调、控制和管理整个攻击过程。

（3）接口工作站是攻击控制引擎与互联网连接的一个接口。

（4）代理（Agent）是一个安装在漏洞主机上的程序，实施具体的攻击任务。

Agent 在结构上由信息数据库、分析器、通信处理器和信息收集单元等部件组成，在结构和功能上相当于一个小型的攻击控制引擎系统。在协同式代理结构中，所有的 Agent 和 ACE 组成一个树形结构，ACE 是根节点，Agent 都是分布在树上的任一节点。

3 协同网络防御模型的主要思想

3.1 P2DR 安全模型

P2DR 安全模型包含 4 个主要部分：策略（Policy）、防护（Protection）、检测（Detection）和响应（Response），如图 5 所示。

图 5 P2DR 模型

Fig 5 P2DR model

在此安全模型中重要的性能指标为：Pt 当攻击发生时所需要的时间；Dt 检测系统安全的时间；Rt—安全事件的反应时间；Et 系统暴露的时间。

如果一个信息系统的 Pt＞Dt＋Rt，那么称该系统是安全的。如果 Pt＜Dt＋Rt，那么 Et＝（Dt＋Rt）——Pt 称为该系统的暴露时间，在这段时间内系统是不安全的。

按照公式 Pt＞ Dt ＋ Rt，和 Et＝Dt＋Rt（Pt＝0），应提高系统的防护时间 Pt，降低检测时间 Dt 和响应时间 Rt

3.2　协同式网络防御安全模型

基于 P2DR 模型思想提出以下防御模型体系，如图 6 所示。

访问控制、防火墙等技术属于静态防御，而应对网络上日益增多的协同式攻击，必须有动态的防御技术，这样入侵检测技术就成了抵抗攻击的第二道防线。同时，系统备份也很重要，应把系统备份作为另一个防御手段。防火墙是第一层防护；入侵检测系统是第二层防护；第三层防护是用户控制。

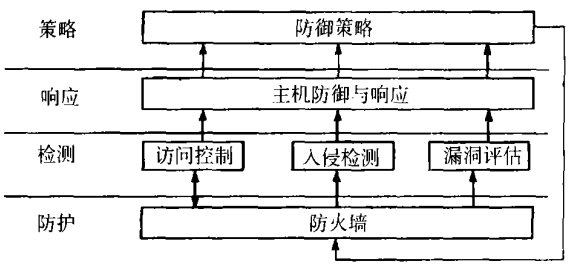

图 6　防御模型体系

Fig. 6　Defence model system

4　结　语

模型是一个整体的分布式平台，使得协同网络攻击模型和协同式网络防御模型有机地统一。基于移动代理的技术使得协同结构的分布式攻击和防御得以实现。对于移动代理本身的安全脆弱性，灵活的安全策略包括安全通道的方式能适用于协同式系统的动态要求。目前成熟的移动代理技术、攻击技术、防火墙技术、入侵检测技术和用户控制相结合，形成协同式网络攻防概念模型的攻防层次，使整体模型得以容易建立。

下一步方向在于：在模型中加入基于蜜网的网络安全防御技术和基于免疫的动态计算机病毒检测技术，完善专家系统的建立。模型中代理技术的优化。包括代理分组优化、代理自我学习能力、代理综合测试等。进一步尝试应用成熟网格技术的构建基于网格的协同安全对抗模型。

参考文献：

[1]　武骏，程秀权，于晓芸，等. 网络安全防范体系及设计原则[EB/OL]. 中国电信网 2004－05.

[2]　董晓梅，于戈. 分布式入侵检测与响应协作模型研究[EB/OL]. 中国科技论文在线，2004－02.

[3]　BONIFACIO J，MAURICIO Jr，CANSIAN A M，ANDRE C P，et al. Neural Networks Applied in Intrusion Detection Systems[J]. IEEE，1998(5)：1072－1090.

[4]　李涛. 网络安全概论[M]. 北京：电子工业出版社，2004.

Agent Based Safe Network Countermodel with Cooperative Structure

CHEN Wen bin

(Sofeware Institute of Sun Yat-sen University，Guangzhou 510275，China)

Abstract：Setting up a safe network platform on Internet which is able to attack and defense based on coordination structure is the purpose. Providing support of dynamic reconfiguration，the mobile agent and safe technology are combined. Both technology grade and theories of safe sofeware design are advanced to a certain position.

Key words：network attack；network defence；mobile agent；cooperative structure