文章编号: 1001- 2486(2003) 02- 0060- 04

动态网络安全的框架模型*

陈海涛, 胡华平, 徐传福, 龚正虎
(国防科技大学计算机学院, 湖南 长沙 410073)

摘 要: 针对现有的静态网络安全模型存在的问题, 提出了一种动态网络安全框架模型。该安全模型利用各种安全组件构建了立体的五层防御体系, 并实现了防御能力的动态升级。

关键词: 网络安全; 安全模型; 多层防御; 动态升级
中图分类号: TP393 文献标识码: A

A Framework Model for the Dynamic Network Security

CHEN Hai-tao, HU Hua-ping, XU Chuan-fu, GONG Zheng-hu
(College of Computer, National Univ. of Defense Technology, Changsha 410073, China)

Abstract: A dynamic network security model to solve the limitations of classic static network security model is proposed. This security model makes use of all kinds of security components to construct a five-layer defense architecture whose defensive ability can upgrade dynamically.

Key words: network security; security model; multi-layer defense; dynamically upgrading

层出不穷的安全漏洞, 自动传播的网络病毒, 网络上随处可以下载的攻击程序, 尤其是分布式、协同式攻击的出现, 对网络安全造成了巨大的威胁[1]。传统的静态网络安全观念(认为安全是静态的, 可以一劳永逸的, 只要精心挑选安全工具, 精心布置以后就不用维护了) 不能适合现代网络安全的需要。

网络的发展是动态的, 不断有新的协议、操作系统、应用软件发布和应用, 伴随出现的有大量新的漏洞、病毒、攻击程序, 相应的网络安全模型也必须是动态的。在对现有的各种安全技术做了深入分析的基础上, 本文提出了一种动态网络安全框架模型。该动态安全模型将现在已有的安全技术和成功的安全经验结合在一起, 构造了一种多层次、综合各种安全工具、相互联动的安全体系。该安全体系强调动态, 系统的防御能力是随着时间递增的, 能够根据现有的安全状况自动调整。

1 传统静态网络安全框架模型的不足

网络安全框架模型中包括各种网络安全组件, 如防火墙、加密和认证系统、入侵检测系统、防病毒系统、漏洞扫描和补漏系统、灾难恢复、攻击陷阱、攻击反击等[2, 3]。网络安全框架模型主要定义所使用的安全组件以及模型内各安全组件的关系。

静态网络安全框架模型主要有以下特征:

(1) 主要采用了静态网络安全技术, 如防火墙, 加密和认证技术等。

(2) 模型内各部件的防御或检测能力是静态的。

(3) 模型内各部件孤立工作, 不能实现有效的信息共享、能力共享、协同工作。

静态网络安全框架模型存在的问题:

(1) 静态的网络安全技术提高了黑客攻击成功的门槛, 能够挡住大多数的攻击, 但是少数能够穿透静态网络安全技术构成的屏障攻击将对系统造成极大的危害。

(2) 静态网络安全组件的防御能力是固定的, 不能随着环境的变化而不断变化, 而攻击者的攻击能

* 收稿日期: 2002- 11- 02
基金项目: "十五" 863 课题项目(2001AA142030)
作者简介: 陈海涛(1977—), 男, 博士生。

力是不断提升的。在安装的初始阶段, 安全组件的防御能力大于黑客的攻击能力, 但随着时间的推移, 黑客的攻击能力终将超过安全组件的防御能力。

(3) 静态网络安全组件的防御或检测能力不能动态地提升, 只能以人工或者定期的方式升级, 但这往往是亡羊补牢。

(4) 单个的安全组件所能获得的信息是有限的, 不足以检测到复杂攻击, 即使检测到了也不能做出有效的响应。

总之, 传统的静态网络安全框架模型不足以解决现有的各种安全威胁, 不能构建一套有效的网络安全防护体系。面对日益流行的分布式、协同式攻击, 任何单个的安全组件防御能力是有限的, 只有各安全组件实现有效的互动, 构成整体安全解决方案, 才能进行有效的检测和防护。

2 动态网络安全的框架模型

2.1 模型体系结构

该框架模型将各网络安全组件构建成多层的纵深防御体系, 形成对系统的全方位、多层次的立体防护。模型体系结构见图 1, 该模型共分为五个层次。

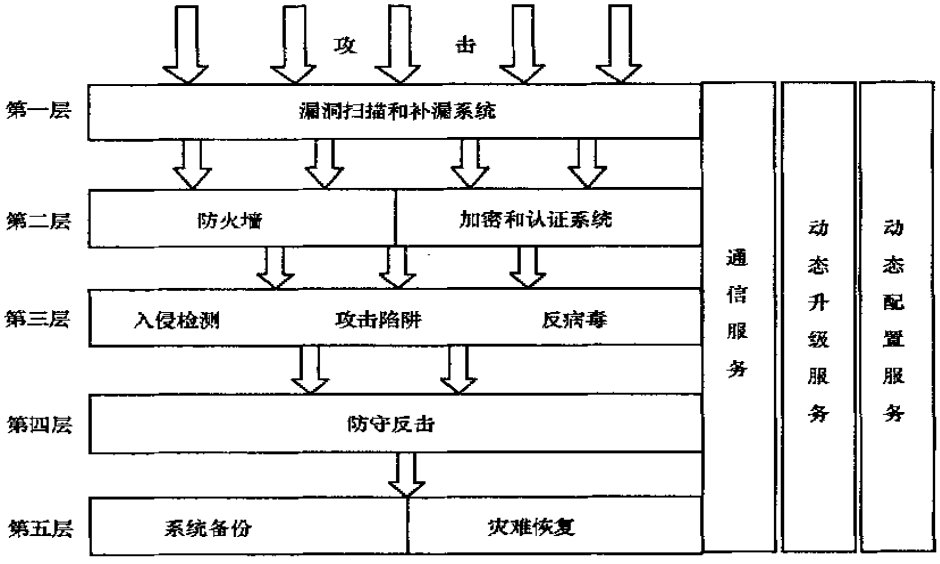

图 1 动态网络安全框架模型的体系结构

Fig. 1 Architecture of dynamic network security framework model

(1) 第一层由漏洞扫描和补漏系统组成, 主要任务是主动检查并补上系统漏洞。历史数据显示大多数的黑客进攻都是利用已有的系统漏洞, 该防御层能有效减少黑客进攻成功的可能性。

(2) 第二层由防火墙系统和加密认证系统组成, 它们是典型的静态防御技术, 能抵御多数黑客的攻击, 大大提高黑客发动成功进攻的技术门槛。

(3) 第三层由入侵检测、攻击陷阱、反病毒系统组成, 它们是动态安全检测技术, 用于及时发现黑客与不良程序的入侵。

(4) 第四层由防守反击系统组成, 主要任务是根据接收到的入侵检测系统和攻击陷阱系统的报警后, 对攻击者进行反击。

(5) 第五层由备份、灾难恢复系统构成。备份系统对系统的关键信息做备份, 灾难恢复系统则利用备份信息对受损的系统进行恢复。

除了五层防御以外, 框架模型还包括一些基本的服务。通信服务向安全组件提供通信服务; 动态升级服务动态提升系统的防御能力; 动态配置服务根据环境的变化调整系统的配置。

防御体系充分利用现有的网络安全技术, 将其组合, 使之发挥最高的防御能力, 并且承认风险的存

在, 有效利用备份及灾难恢复技术, 使灾难损失减小到最低限度。防御体系的理想效果是使能穿透防御层的黑客攻击数逐层减少, 到达第五层的攻击将对系统造成损害, 但只要其不能穿透第五层, 其危害将是有限的。

2.2 模型数据结构

模型的数据结构是实现动态模型的关键环节。本模型的数据结构由 10 个部分组成: 漏洞库; 漏洞补丁库; 攻击特征库; 病毒特征库; 响应策略库; 备份数据库; 攻击程序库; 防火墙规则; 中间结果库; 管理员。模型数据结构有如下特点:

(1) 漏洞库、漏洞补丁库、攻击特征库、病毒特征库通过 CVE 编号相关联。

(2) 各安全组件有公用的中间结果库, 可以进行关联分析。

(3) 响应策略库定义了从动态配置防火墙、启动攻击程序到灾难恢复等多种响应策略。

(4) 将管理员作为数据结构的重要一员。理由是管理员拥有丰富的知识, 其知识可以经常升级, 该框架模型利用管理员的知识对其它数据结构进行维护。目前的网络安全技术还没有发展到无需人的干预也可以可靠有效地运行, 各种机器学习和自适应系统也都有缺陷, 本模型将管理员的知识作为一个重要的数据结构引入, 并利用其动态性更好地实现模型的动态。

2.3 动态升级机制

静态网络安全模型内部各部件的防御或检测能力是静态的, 其防御或检测能力不能随着环境的变化而不断有效地得到提升。本模型通过以下手段实现了系统防御或检测能力的动态提升:

(1) 各安全组件有专门的升级代理, 其功能是在 Internet 上寻找相关的升级信息。

(2) 升级代理综合利用 PUSH 和 PULL 实现有效的升级。

(3) 根据运行的结果由管理员进行能力调整或升级。

图 2 以入侵检测系统攻击特征库的动态升级说明了模型的动态升级机制。

2.4 通信机制

动态网络安全框架模型涉及复杂网络环境下的多样化系统之间的通信, 其通信需求如下[4]:

- 能实现异构操作系统平台之间的通信, 如 Windows、Unix、Linux 等平台。
- 最大限度地实现异构网络之间的通信, 如以太网, FDDI、广域网等。
- 传输的信息有标准的表示机制, 支持扩展。
- 有很强的安全机制, 支持认证和加密。
- 支持信息在复杂网络环境下的可靠传输, 有缓存机制。
- 能兼顾实时性和传输性能的考虑。
- 同时支持信息的 PUSH 和 PULL 技术。

综合考虑各种传输技术, 采取的通信机制如图 3 所示。该通信机制的特点是:

- 采用成熟的 CORBA 中间件技术有效地解决了异构网络、异构系统下的安全通信。
- 采用消息事务层解决消息的可靠传送、实时性等事务性问题。
- 消息采用符合国际标准的 XML 格式表示, 有很好的通用性和扩展性。

3 模型分析

动态网络安全框架模型的特点如下:

(1) 多层防御体系。各安全组件按其功能和特点构成多层防御体系, 各层之间既能互动, 又保持相对的独立。黑客必须突破所有的防御层才能对系统造成损害。

(2) 系统的防御能力能动态提升。

(3) 模型内各安全组件能实现互动。模型内的安全组件是相互协作的, 如入侵检测的结果将检测结果通知防守反击系统, 它根据响应策略库进行各种响应, 例如通知防火墙切断黑客的入侵连接或者调用攻击程序对黑客实施反击。

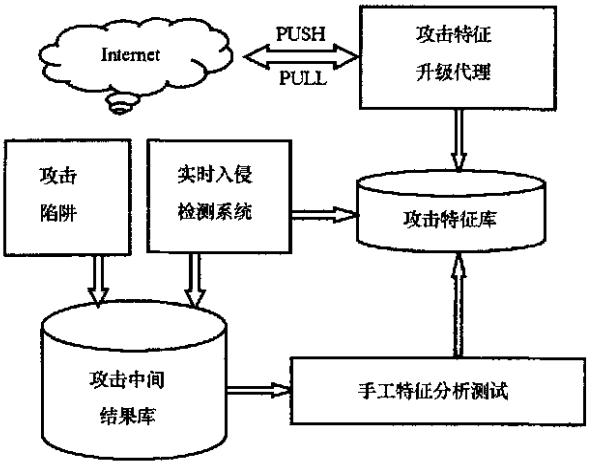

图 2 入侵检测系统的动态升级
Fig. 2 Dynamically upgrading of intrusion detection system

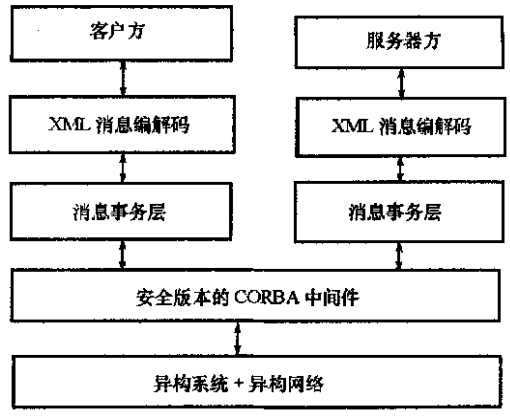

图 3 模型的通信机制
Fig. 3 Communication mechanism of model

(4) 自动化响应与人的智能相结合。该框架模型除了充分利用自动化响应提高对抗黑客的能力和减轻管理员负担义务以外, 还将管理员置于非常重要的地位。

4 结束语

黑客的进攻对因特网造成了严重的威胁, 如何有效抵御黑客的进攻已经成为一个关系国家经济和军事安全的重要问题。针对现有的静态网络安全模型存在的问题, 提出的动态网络安全模型, 利用各种安全组件构建了立体的多层防御体系, 并能实现防御能力的动态升级。

参 考 文 献:

[1] 胡华平, 陈海涛, 等. 入侵检测系统研究现状和发展趋势[J]. 计算机工程与科学, 2001, 23(2): 20- 23.

[2] 胡华平, 等. 网络安全深度防御体系研究[J]. 计算机工程与科学, 2002, 24(6): 7- 10.

[3] IATF Document 3.0 [S]. URL: www.iatf.net/ framework-docs / version-3 _0 /index.cfm.

[4] 陈海涛. 基于多代理的入侵检测系统的实现技术研究[D]. 国防科学技术大学硕士论文, 2002.