文章编号：1005-8451（2007）12-0034-04

基于大规模Intranet的主动式防御系统的研究与设计

虞宏霄，谭敏生，刘芳菊
（南华大学 计算机科学与技术学院，衡阳 421001）

摘 要：针对目前大型企业内部网络的信息安全问题，提出一个完整的基于大规模Intranet的主动式防御系统的设计方案。该主动式防御系统分为陷阱网络层、控制层、应用层3个部分，同时该系统综合蜜网、入侵检测、重定向等多种最新技术，能够实时有效地收集各种网络攻击行为，并通过对已知攻击性网络行为的转移和对未知网络行为的分析，达到保护企业内部网络信息安全的目的。

关键词：主动防御；网络安全；蜜网；入侵检测系统
中图分类号：TN925.1 文献标识码：A

Research and design of Proactive Defense System based on large scale Intranet

YU Hong-xiao, TAN Min-sheng, LIU Fang-ju
(School of Computer Science and Technology of Nanhua University, Hengyang 421001, China)

Abstract: For solving the problems of the information security of large scale Enterprise networks, an Integrated Proactive Defense System based on large scale Intranet was designed. The System was divided into honeynets layer, control layer and application layer. Some new technologies were also colligated in the System, such as the technology of Honeynet, IDS and Redirection. The System could collect various network-based attacking behaviors effectively and in real time. So, the information of the Intranet could be protected by analyzing the unknown network-based behaviors and redirecting the known network-based attacking behaviors.

Key words: proactive defense; network security; Honeynet; IDS

自上世纪末，互联网（Internet）得到了迅猛的发展，将人类社会带入了信息化时代。网络在为人类提供服务的同时，其自身的安全问题也随之显露。由于互联网早期是开放的、非赢利性的信息共享载体，其可靠性要优于安全性，因此，在设计上存在着众多的安全漏洞。基于网络的黑客攻击以及病毒蔓延，已经在世界范围造成了巨大的影响和经济损失，然而单纯地依靠基于策略控制的防火墙技术和基于特征匹配的入侵检测系统（IDS）不能完全适应网络攻击行为的新趋势[1]。因此，为了能够更好地保护大型企业内部网络的信息安全，综合主动

收稿日期：2007-04-25
基金项目：国家自然科学基金(60572137)；湖南省科技计划项目(2006GK3084)。
作者简介：虞宏霄，在读硕士研究生；谭敏生，教授。

设计简化，系统功耗降低，稳定性提高，设计成本减少，产品开发周期缩短。ADXL202作为此仪表的关键部分，也会随之具有巨大的发展潜力。该系统的调试结果较为理想。能够在大部分条件下实现比较准确的列车监测，抛车报警。列车完整性监测系统的使用为列车现场实时运行状况的监测提供了一种切实有效的方法，应用前景广泛。随着微电子技术和半导体集成电路工艺的日臻完善，在不久的将来，微电子机械系统（MEMS）一定会有其更加广阔的应用前景。

参考文献：

[1] 田 泽. 嵌入式系统开发与应用[M]. 北京：北京航空航天大学出版社，2005.

[2] Labrosse Jeanj. 嵌入式实时操作系统uC/OSII[M]. 邵贝贝. 北京：北京航空航天大学出版社，2003.

[3] 李建军，姜 雪，杨天池. ADXL202在组合车载导航系统中的应用[J]. 世界电子元器件，2004（4）：36-38.

[4] 田小芳，熊 超，陆起涌. 基于加速度传感器的GPS盲区内定位方案研究[J]. 微电子学与计算机，2006，23（5）：187-192.

防御技术研究领域的最新成果，设计了一个全新的层次型主动式防御系统。

1　主动防御技术概述

主动防御源于英文“Proactive Defense”。其确切含义为：前摄性防御[1]。具体是指由于某些机制的存在，使得毋需在人为被动响应的情况下，提前预防攻击者对目标的攻击。主动防御属于动态防御技术，与传统的静态防御技术如防火墙技术和入侵检测技术相比，在发现未知攻击、实时获取攻击信息以及提前采取预防措施等方面具有突出优势。

对于主动防御技术的研究始于美国，最初是对网络入侵行为进行诱骗的研究。

近年来，对于主动防御的研究主要集中在入侵诱骗和陷阱网络上。其中，Honeypot（蜜罐）技术和 Honeynet（蜜网）技术受到了各国学者的广泛青睐。目前，国际上致力于蜜网技术研究的有两大组织，即：蜜网项目组（Honeynets Project）和蜜网研究联盟（Honeynets Research Alliance）。他们的主要目标是将部署在世界各地的蜜网所收集到的黑客攻击信息汇总到一个中央管理系统中，以方便研究人员对黑客攻击行为的分析。我国对于蜜网技术研究的著名组织是北京大学计算机研究所，他们的研究项目“狩猎女神”（Artemis）已于 2005 年 2 月正式被批准加入蜜网研究联盟，并成为该联盟组织的第 1 支中国科研团队。

2　主动式防御系统的体系结构

针对目前各大型企业内部网络的实际运行情况，本文所提出的层次型主动式防御系统的框架包括：陷阱网络层、控制层和应用层 3 个部分，体系结构如图 1。

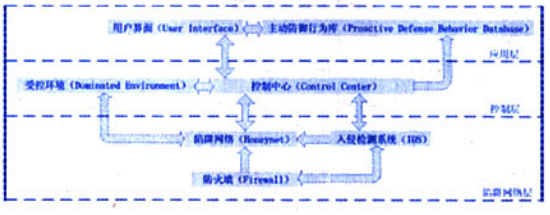

图 1　主动式防御系统体系结构

主动式防御系统的最底层是陷阱网络层[2]，其主要功能是吸引黑客攻击，同时配合入侵检测系统，将符合特征匹配库的攻击数据流信息做出标记并捕获攻击数据包，然后转交给控制中心。

中间层是控制层，也是整个主动式防御系统的控制核心。它的主要功能是当 IDS 检测出危险攻击数据信息后，控制中心将立刻通知用户界面报警，同时利用重定向技术将攻击行为转移至受控环境。它的另一个主要功能是从陷阱网络层陷阱机所收集到的大量数据信息中提取出已知的攻击信息，然后再将剩余数据信息送至主动防御行为库进行分析，以便发现更多的未知攻击行为。

主动式防御系统的最高层是应用层，它提供了用户与系统的接口（用户界面），用户可以通过用户界面实时掌握控制中心的处理情况。主动防御行为库负责对陷阱机和受控环境收集到的网络行为数据进行分析与处理。

3　主动式防御系统的设计

3.1　陷阱网络层的研究与设计

陷阱网络层主要包括防火墙、陷阱网络（Honeynet）及入侵检测系统（IDS）3 大部分。其中 Honeynet[3]（蜜网）由多台陷阱机组成，每台陷阱机都是真实的计算机，上面运行着 WindowsXP/2003Server、Linux 或 Solaris 等多种真实的操作系统与应用程序[4]，同时陷阱机上开放了众多服务，如 FTP、Telnet 服务等。整个陷阱网络的拓扑结构如图 2。

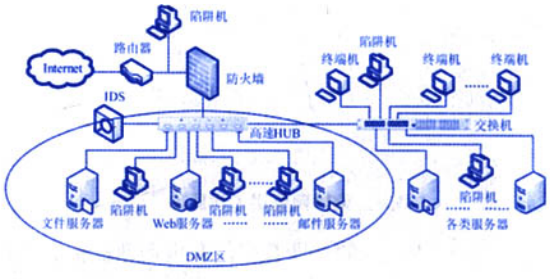

图 2　陷阱网络拓扑结构

陷阱机将按照系统需要灵活地部署在企业内部网络中的各个位置，不同区域的陷阱机所探测到的攻击类型以及对整个陷阱网络系统的作用是不同的[5]。

（1）部署在防火墙外：当该区域陷阱机受到攻

击时，对于防火墙内部网络的危险性不会增加，但由于该区域分布在防火墙之外，黑客对于端口的大量扫描信息等将不会被防火墙日志所记录，而且该区域陷阱机收集到的网络信息量较大，其中包含了较多的冗余信息。

（2）部署在非军事区。非军事区（DMZ区）指的是通过防火墙而独立于其它系统的部分网络，外网（Wan）和内网（Intranet）均可对该区域进行访问。由于DMZ区受到较严格的保护，仅允许部分外网信息通过防火墙进入，因此，企业内部网络中的对外服务器，如邮件服务器、Web服务器等通常布置在该区域。部署在该区域的陷阱机将模拟对外服务器所提供的服务，可以收集较多有价值的攻击信息，但该区域的陷阱机需要在防火墙上开放相应的端口，提高了企业内部网络的风险度。

（3）部署在防火墙内。部署在该区域的陷阱机主要收集来自企业内部网络的攻击行为，而且所有通过防火墙进入该区域陷阱机的外网数据信息均能被防火墙日志详细记录。由于目前将近80%的网络攻击行为来自企业内部，因此，部署在该区域的陷阱机对于保护企业内部网络信息安全起着致关重要的作用。

陷阱网络层采用分布式系统设计，防火墙组件和IDS组件[6]分布在整个系统中，通过各个组件之间相互合作完成攻击数据捕获过程。陷阱网络层的工作原理如图3。

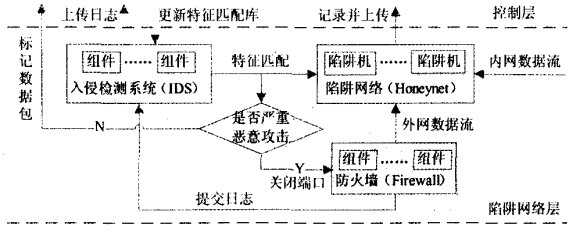

图3 陷阱网络层工作原理

流入陷阱机中的外网数据流和内网数据流，将被陷阱机记录并上传到控制层。IDS对陷阱机中的数据流进行实时特征匹配，当检测到攻击数据流后先判断是否为外网严重恶意攻击，如拒绝服务攻击（DOS攻击）或洪水攻击等。若发现外网严重恶意攻击，将直接通知防火墙切断其端口连接。其它非严重恶意攻击的信息，IDS将对其进行标记并捕获攻击数据包，然后再转交给控制中心处理。

防火墙是外网数据控制的第1层，对所有陷阱机的外发连接进行控制，当陷阱机的外发连接数达到最大值时，防火墙将自动切断其后的所有外发连接。防火墙组件定期将日志备份副本提交给IDS，IDS组件再将日志副本上传至控制中心，控制中心会定期根据主动防御行为库对于未知攻击信息的分析结果更新IDS特征匹配库。

3.2 控制层的研究与设计

控制层包括受控环境和控制中心两大部分，控制层的主要任务是从陷阱机收集到的大量数据信息中提取出已知的攻击信息，然后将剩余信息送至应用层分析处理。并且当发现攻击时，控制中心及时将攻击转移。控制层的工作原理如图4。

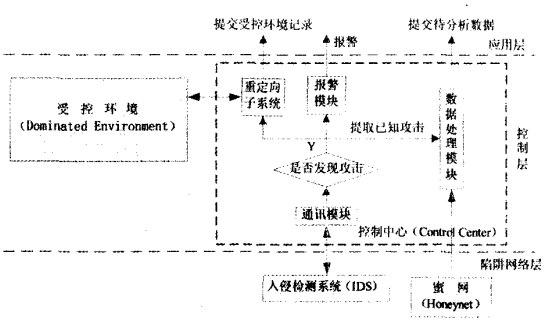

图4 控制层工作原理

受控环境是一个包含有防火墙、网关、路由器及多台真实主机的子网，在受控环境中存储着一些伪造信息用以迷惑攻击者，而且在受控环境中存在着仿真网络数据流量，用以模拟真实的子网环境。

控制中心是整个控制层的核心部件，所有被陷阱机所记录的数据信息均传到控制中心的数据处理模块。控制中心的通讯模块负责与IDS进行信息交互，当通讯模块检测到被IDS标记过的攻击数据信息时，数据处理模块将已知的攻击行为数据进行提取，然后将剩余数据信息转交给应用层的主动防御行为库进行分析，以便从中确定出更多的未知攻击行为。

当发现攻击行为时，通讯模块将立刻通知报警模块将向用户界面报警。同时重定向子系统根据被IDS捕获的攻击数据包确定攻击数据源，提供给入侵者部分企业内部网络运行的仿真数据与之交互，以暂缓攻击。然后启动重定向功能[7]，将黑客的攻击行为转移至受控环境。黑客在该环境中的所有行为记录均被返回给重定向子系统，重定向子系统再

将受控环境记录上传至主动防御行为库做进一步分析。重定向技术的实现算法如图 5。

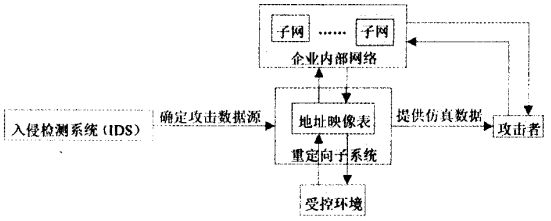

图 5　重定向实现算法

事先创建好的地址映像表[8]将企业真实网络各子网中的主机与受控环境中的主机进行地址映射。当发现攻击行为时，重定向子系统先读取地址映像表，再将针对某真实子网攻击的数据信息通过地址映射转移到受控环境中的相应位置，受控环境的反馈信息同样通过地址映射转移到真实子网的相应位置，然后再反馈给攻击者。由此，攻击者所得到的交互信息均来自受控环境，而并非来被攻击的子网。

重定向子系统仅针对 IDS 所确定的攻击数据源将攻击行为数据进行重定向，企业内部真实网络中的其它数据信息仍可进行正常交互，不影响企业真实网络的正常运行。

3.3　应用层的研究与设计

应用层主要包括用户界面和主动防御行为库两个主要部分。用户界面是用户与系统的接口，用户可以通过用户界面实时掌握整个系统的运行情况。应用层的工作原理如图 6。

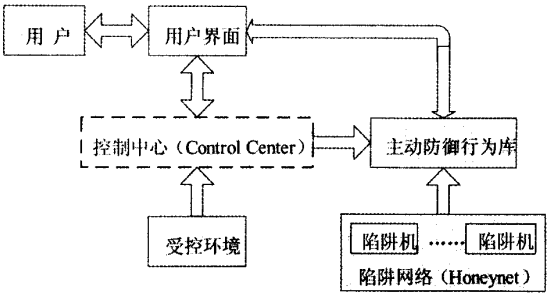

图 6　应用层工作原理

主动防御行为库的主要任务是通过分析来自陷阱机和受控环境中的数据信息，发现未知攻击行为，然后通过用户界面反馈给控制中心更新 IDS 特征匹配库。在应用层用户还能够通过用户界面对主动防御行为库中的数据进行人工查询和分析等。

4　结束语

本文作者的主要创新点有两个：（1）提出一个层次型的主动式防御系统的体系结构，并对各层所实现的功能进行了深入的分析；（2）将当前主动防御研究领域的热点技术进行有机地综合。该系统能够很好地保护企业内部网络的安全运行，同时收集到的大量黑客攻击行为数据，为保护企业权益和合法取证等方面提供可靠的数据资料。

参考文献：

[1] 罗璎珞，应向荣. 主动防御技术的由来与发展[J].计算机安全，2003（8）：27-29.

[2] 刘宝旭，曹爱娟，许榕生. 陷阱网络技术综述[J].网络安全技术与应用，2003（1）：65-69.

[3] Know Your Enemy:Honeynets.Honeynet Project[EB/OL]. http://project. honeynet.org,31 May, 2006.

[4] JOHN G.LEVINE,JULIAN B.GRIZZARD,HENRY L.OWEN. Using Honeynets to Protect Large Enterprise Networks[J]. IEEE Security & Privacy, NOVEMBER/DECEMBER 2004:73-75.

[5] Lance Spitzner.The Value of Honeypots, Part One：Definitions and Values of Honeypots[EB/OL]. http://www. securityfocus.com/infocus/1492, Oct, 2001.

[6] Mukherjee B, Levitt T L. Network Intrusion Detection [J].IEEE Network,1994, 8(3): 26-41.

[7] David Watson,Thorsten Holz, Sven Mueller. Know Your Enemy: Phishing.Honeynet Project[EB/OL]. http://project. honeynet.org,16 May, 2005.

[8] RFC2663. IP Network Address Translator (NAT) Terminology and Considerations[EB/OL]. http://www.ietf.org/rfc,August, 1999.