基于网络主动防御安全模型的入侵诱骗系统

赵洪静[1]， 周创明[1]， 翟平利[2]， 于 焕[3]， 赵明莉[4]
(1. 空军工程大学 导弹学院，陕西 三原 713800;2. 93861部队，陕西 三原 713800;3. 新松机器人自动化股份有限公司，辽宁 沈阳 110168;4. 中国人民解放军驻631所军事代表室，陕西 西安 710068)

摘 要：当前网络安全形势日益严峻，传统的安全技术如防火墙、入侵检测技术存在着对未知入侵模式的攻击不能有效识别等诸多缺陷，Honeypot技术作为一种网络主动防御的安全技术，也具有一定的局限性。针对以上单一技术在网络安全防御上的缺陷，从主动防御的角度，基于网络主动防御安全模型构建了入侵诱骗系统的体系结构，并且设计了Honeypot与防火墙、IDS的联动系统，既克服了防火墙不能提供实时检测的缺陷，又降低了IDS的漏报率和误报率，弥补了各自的不足，充分发挥了优势，从而提高了网络系统的主动防御能力。同时，给出了有限自动机模型，模拟了入侵诱骗系统的基本功能，为系统的行为描述和结构设计提供了理论依据和论证。

关键词：主动防御；入侵诱骗；Honeypot；虚拟网络服务；有限自动机
DOI：10.3969/j.issn.1009-3516.2010.03.017
中图分类号：TP393.08 **文献标识码**：A **文章编号**：1009-3516(2010)03-0076-04

全球信息化已成为人类社会发展的大趋势，信息时代的到来使得信息可用性、完整性、安全性面临巨大的挑战。随着入侵活动的日益猖獗，传统的安全技术已经不能适应动态多变、多维多联的网络环境。这就需要计算机网络安全防护由被动防御转为主动防御。网络主动防御技术就是在增强和保证本地网络安全性的同时，还要及时发现正在遭受的攻击并及时采取各种措施使攻击者不能达到其目的，使己方的损失降到最低的各种方法与技术[1]。入侵诱骗作为一种攻防技术充分体现了主动防御的思想，能够使网络安全被动挨打的局面得以扭转，极大增强了网络的安全性和生存能力。本文基于网络主动防御安全模型对入侵诱骗系统进行了研究，实现了防火墙技术、入侵检测技术、诱骗技术的联动协作，能够积极主动地应对网络攻击，进一步提高了网络环境的安全。

1 网络主动防御安全模型

防火墙技术和入侵检测技术都属于传统的安全模型，传统的安全模型建立在静态的、基于开环控制的体系下，对动态的安全威胁、系统的脆弱性缺乏足够的描述和应对措施，不能够对网络中的远程攻击和威胁作出必要、快速的反应以及反馈。动态网络安全模型因此应运而生[2]。PPDR模型就是动态网络安全模型一种代表性模型。虽然PPDR模型中防护、检测、响应组成了一个完整的动态循环[3]，指导思想比传统静态安全方案有突破性的提高，但是该模型方案取得成功依赖于系统正确的设置和完善的防御手段，并且在很大程度上针对固定的威胁和环境弱点，它忽略了网络安全的主动性。

文献[2]提出了一种基于闭环控制的、基于主动防御的动态网络安全模型P^2DR^2C模型。P^2DR^2C模型的原理图见图1。其体系结构见图2。该模型对以往的动态网络安全模型进行了细化和扩展，能有效地增加系统的主动性、适应性和可生存性。

收稿日期：2010-03-16
基金项目：国家自然科学基金资助项目(60773209)
作者简介：赵洪静(1985-)，男，山东汶上人，硕士生，主要从事网络与信息安全研究. E-mail:andylau_1999@163.com

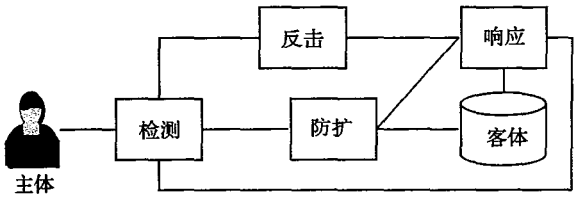

图1　P^2DR^2C 模型原理图

Fig. 1　P^2DR^2C model

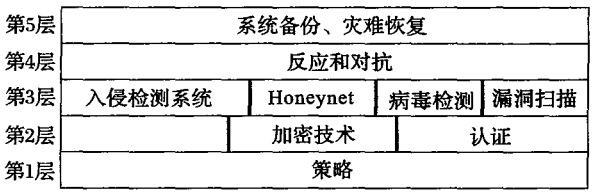

图2　P^2DR^2C 模型的体系结构

Fig. 2　The architecture of P^2DR^2C model

模型用6元组表示为[2]:P^2DR^2C = (Policy, Protection, Detection, Response, Recovery, Counterattack)。模型用文字描述为:安全 = 风险分析 + 执行策略 + 漏洞监测 + 实时响应 + 主动对抗 + 及时恢复。

在网络主动防御安全模型中,网络系统安全策略是网络安全的基础,在整体的网络系统安全策略的控制和指导下,综合地运用安全操作系统、防火墙、认证、加密技术等安全防护措施和手段来保证网络系统的安全性,利用入侵检测系统、弱点漏洞分析和评估工具对网络的安全状况进行评估和分析,实时监控网络事件,尽力保持网络处于相对安全状态。

2　基于网络主动防御安全模型的入侵诱骗系统

2.1　入侵诱骗系统的提出

入侵诱骗系统是网络主动防御模型中非常重要的一个环节,是整个模型主动性、动态性的重要体现。它是在入侵检测之后对检测结果所做出的一种响应。

诱骗环境其实是一个可控的 Honeypot,它替代真实的系统,是整个入侵诱骗系统的核心。Honeypot 是一个置于网络上诱骗黑客攻击的信息资源系统,其价值就在于被无认证地、非法的使用[4-5]。

根据以上的分析研究,本文基于网络主动防御安全模型 P^2DR^2C 构建入侵诱骗系统,其体系结构见图3。

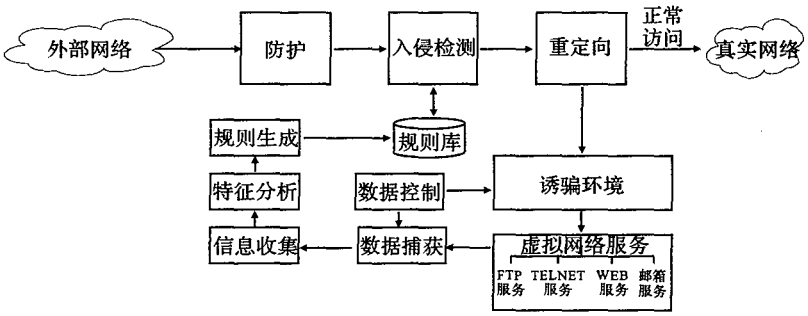

图3　入侵诱骗系统体系结构

Fig. 3　The architecture of intrusion deception system

1)作为一个诱骗环境,其价值在于让入侵者浪费大量或者全部的资源和时间去攻击,这就必然要提供入侵者感兴趣的网络服务。虚拟网络服务通过提供一些相关网络服务,使入侵者产生浓厚兴趣,以达到吸引入侵者攻击的目的。

2)数据控制控制进出诱骗环境的数据流量,限制最大外发连接数,既防止蜜罐收到拒绝服务攻击(DOS),也可防止入侵者绕过虚拟文件系统和虚拟服务把入侵诱骗虚拟环境作为跳板去控制其他真实主机。

3)数据捕获就是捕捉入侵者的行为,主要是指防火墙日志、IDS 日志包和 honeypot 主机的系统日志"三重捕获"。对这些捕捉到的行为进行分析,从而得知入侵者所使用的攻击工具、攻击策略和入侵动机等。

4)信息收集负责收集虚拟环境系统事件,对入侵者的行为进行详细的记录,进行行为跟踪,并为入侵响应及随后可能进行的对入侵者的法律制裁提供证据。

5)特征分析根据收集到的数据信息对可疑行为或入侵行为进行进一步分析,将分析生成的新规则更新到防火墙以及入侵检测系统的知识库中,增强防火墙和入侵检测的能力。

2.2　入侵诱骗系统中 Honeypot 与防火墙、IDS 的联动设计

传统的安全技术如防火墙、入侵检测系统(IDS)都是依据具体特征库进行判断,对系统依赖性过强,面对新型的攻击模式显得无能为力。Honeypot 作为一种网络主动防御技术引进了主动控制、人工智能等思想[6],更具主动性、交互性和学习性。网络安全管理员通过 Honeypot 系统能更详尽地学习了解入侵者的思路、所用的网络工具和攻击目的[7],从而及时采取相应的应对措施。然而 Honeypot 也存在着一定的缺陷:视

野狭窄,只能针对自身的入侵行为;具有一些专业的特征和行为,使入侵者鉴别出它的存在,并破坏记录的信息;Honeypot 一旦被攻陷可能被作为攻击、渗透其他系统的跳板。根据 Honeypot 和防火墙、IDS 各自的特点,充分发挥各部分的优势,本文将 Honeypot 技术与防火墙、入侵检测系统联动结合,构建一个全新的安全机制,改变传统的网络安全被动防御策略为主动防御。

图 4 中,系统前端的防火墙作为第 1 道防线,采取"宽进严出"的配置策略,允许所有外部数据包进入 Honeypot。在 IDS 和重定向的功能作用下,Honeypot 引诱穿透防火墙进入的攻击者,减少对内部网络的攻击,同时捕获所有进出 Honeypot 的数据包;IDS 能减少攻击者的攻击和干扰,使攻击者浪费时间和精力用在通过防火墙的漏洞渗透过来的攻击检测上,同时能够检测异常并及时报警,使 Honeypot 日志系统启动以便记录入侵信息;防火墙可疑追踪从 Honeypot 出来的每个网络连接,从而对入侵者进行监控。为了保证内网的安全性,增加了一个额外的防火墙进行有效地隔离,同时在防火墙和 Honeypot 之间安置了路由器,提高了 Honeypot 的逼真度,而且路由器能够控制访问权限,补充防火墙的控制能力,以确保 Honeypot 不被用作跳板攻击其他网络系统。

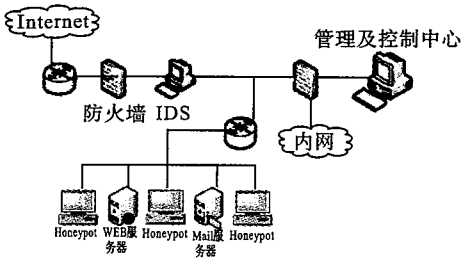

图 4 Honeypot 与防火墙、IDS 联动系统

Fig. 4 Linkage system of Honeypot and firewall, IDS

图 4 所设计的联动系统具有以下优势:通过 Honeypot 发现新的入侵特征,弥补了由于防火墙、IDS 入侵特征库不够完备导致易错报、漏报的缺点;通过 Honeypot 与防火墙、IDS 联动,弥补了单纯的几种安全技术力不从心的不足,体现了价值,增强了网络的安全性。

2.3 虚拟服务的实现

Honeypot 作为整个入侵诱骗系统的核心,能否记录、分析出可疑行为特征直接关系到诱骗的成败,而虚拟服务作为诱骗环境的"诱饵"[8]在这其中扮演了不可或缺的重要角色。为能够有效模拟真实的网络服务,采用有限自动机技术[9]建立虚拟网络服务。针对要模拟的网络服务如 FTP、TELENT,构造相应的有限自动机,当入侵者攻击 Honeypot 时,有限自动机根据入侵者所处的状态产生响应的输出,以便达到迷惑入侵者的目的。虚拟网络服务本质上可以看作是一个状态机:对于客户端的一个请求,服务器给一个响应。这从状态机的观点看便是服务器在某一个状态接受到客户端的一个输入(请求),然后输出一个值(响应),并转移到下一个状态。

根据以上分析,为模拟诱骗系统中各功能部件工作状态的转换过程,可以抽象 $L=(R,\Sigma,F,P_0,S)$ 为诱骗系统的有限自动机。假设确定型有限自动机 $L=(R,\Sigma,F,P_0,S)$。其中,R 是诱骗系统当前状态的所有有限集合,$R=\{P_0,P_1,P_2,P_3,P_4,P_5,P_6,P\}$;$\Sigma$ 是有限输入字符表,$\Sigma=\{0,1\}$,它在此表示有穷事件;F 是 $R\times\Sigma$ 到 R 得一种映射,即映射 $F:R\times\Sigma\to R$;P_0 表示初始状态,且 $P_0\in R$;S 是结束状态集合,$S=\{P\}$ 且 $S\in R$。假设有限自动机 L 处于状态 P,输入字符 a(0 或 1)时,根据指令自动机 L 将转到状态 Q,则记为 $F(P,a)=Q$。即:$F(P_0,0)=P$,$F(P_0,1)=P_1$;$F(P_1,0)=P_0$,$F(P_1,1)=P_2$;$F(P_2,0)=P_2$,$F(P_2,1)=P_3$;$F(P_3,0)=P_0$,$F(P_3,1)=P_4$;$F(P_4,0)=P_4$,$F(P_4,1)=P_5$;$F(P_5,0)=P_5$,$F(P_5,1)=P_6$;$F(P_6,0)=P_0$,$F(P_6,1)=P_1$。

有限自动机 L 的状态转换见图 5。根据图 3 入侵诱骗系统体系结构,图 5 中各工作状态的含义是指:P_0 为诱骗系统的初始状态,P_1 为入侵检测,P_2 为入侵重定向,P_3 为 Honeypot,P_4 为入侵日志记录,P_5 为入侵数据提取、融合,P_6 为入侵行为特征分析,P 为诱骗系统终止状态。

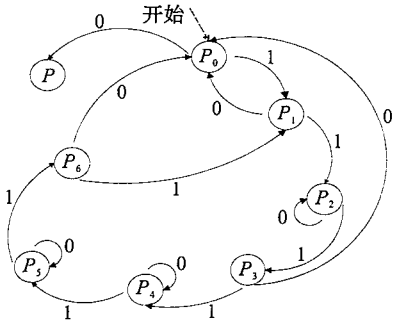

图 5 有限自动机 L 状态转换图

Fig. 5 A state switch chart of limited automaton L

诱骗系统首先处于 P_0 初始状态。若用户有连接请求时,有限自动机 L 从 P_0 转换为 P_1 状态,即入侵检测状态,针对连接请求进行检测,监测异常网络信息,同时还可以根据 Honeypot 控制命令进行规则库的更新工作;若用户退出系统或系统管理员终止诱骗系统的运行,L 从 P_0 状态转换为 P 状态。当发现可疑行为,就将检测结果告知入侵重定向,自动机 L 从

P_1 状态转换为 P_2 状态;若连接请求是无攻击性的,L 从 P_1 转换为 P_0 状态。P_2 状态中,重定向对检测结果进行处理,对于确定的入侵行为,则直接切断入侵者与实际网络的连接;同时把可疑行为重定向至预先设定好的 Honeypot,L 从状态 P_2 转换为 P_3 状态;重定向如果失败,继续维持 P_2 状态,等待修复。P_3 状态为 Honeypot,通过数据控制功能防止入侵者以诱骗环境为跳板去攻击真实网络,以及数据捕获对入侵行为进行捕捉,然后调用入侵日志记录对捕获的信息进行记录,此时由 P_3 状态转换为 P_4 状态;若没有后继攻击,L 从 P_3 状态转换 P_0 状态。在 P_4 状态,入侵日志记录对 Honeypot 的所有活动做严格详细的多级日志记录。随后提取记录的数据并进行融合,此时 P_4 状态转换为 P_5 状态;反之,继续维持 P_4 状态,进行行为日志记录。而 P_6 状态则是对融合提炼的数据进行分析,生成新的入侵规则,更新 IDS 知识库,L 从 P_6 状态转换为 P_1 状态;反之,如果不存在新的攻击,则完成特征分析,从 P_6 状态转换为 P_0 状态。

有限自动机是真实系统的抽象模型,这类系统具有有限数目的内部状态和若干个不同的输入序列,在输入序列的作用下,系统内部状态不断地相互转换,并且可能产生某种形式的输入序列[10]。文中有限自动机 L 模拟了诱骗系统的各功能模块的基本功能,描述了入侵检测、Honeypot、数据记录、特征分析等功能模块的运行全过程,为入侵诱骗系统的行为描述和体系结构设计提供了理论依据。

3　结束语

入侵诱骗技术变被动防御为主动防御,在网络安全领域中处于举足轻重的地位,对提高网络信息的安全性起到了重要的作用。针对单纯的防火墙、IDS 不能有效防御新型的攻击模式,本文通过对入侵诱骗系统的研究,设计了 Honeypot 与防火墙、IDS 的联动系统,将他们有机结合,互相弥补不足。提高了网络安全性能。在研究了系统体系结构的同时,采用有限自动机技术对虚拟网络服务进行了设计实现,从而保证动态安全模型的主动防御能力,实现了网络的动态安全防护。

参考文献:

[1] 周海刚, 肖军模. 网络主动防御体系结构[J]. 电信科学, 2003,48(1):20 - 22.
ZHOU Haigang, XIAO Junmo. The Architecture of Network Active Defensive System[J]. Telecommunications Science, 2003, 48 (1): 20 - 22. (in Chinese)

[2] 李家春, 李之棠. 动态网络安全模型的研究[J]. 华中科技大学学报:自然科学版, 2003, 31(3): 40 - 42.
LI Jiachun, LI Zhitang. Dynamic Network Security Model[J]. Journal of Huazhong University of Science & Technology:Natural Science Edition, 2003, 31(3): 40 - 42. (in Chinese)

[3] 韩锐生, 徐开勇, 赵彬. P_PDR 模型中策略部署模型的研究与设计[J]. 计算机工程, 2008, 34(20): 180 - 183.
HAN Ruisheng, XU Kaiyong, ZHAO Bin. Research and Design of Policy Deployment Model for P^2DR Model[J]. Computer Engineering, 2008, 34(20): 180 - 183. (in Chinese)

[4] Provos N. A Virtual Honeypot Framework[EB/OL]. [2004 - 12 - 29](2009 - 10 - 30). http://www. usenix. org/event/sec04/tech/full - papers/provos/provos - html.

[5] Spitzner L. Open Source Honeypots: Learning with Honeyd[EB/OL]. [2003 - 12 - 29](2009 - 10 - 30). http://www. security focus. com/infocus/1659.

[6] Honeynet Project. Sebek[EB/OL]. [2003 - 11 - 17](2009 - 10 - 30). http://www. xfocus. org/honeynet/papers/honeynet.

[7] 王铁方, 李云文, 叶宝生. 一种基于蜜网的网络安全防御技术[J]. 计算机应用研究,2009,26(8): 3012 - 3014.
WANG Tiefang, LI Yunwen, YE Baosheng. Honeynet - based Network Security Defense Model[J]. Application Research of Computers, 2009,26(8): 3012 - 3014. (in Chinese)

[8] 姚兰, 王新梅. 基于欺骗的网络主动防御技术研究[J]. 国防科技大学学报, 2008, 30(3): 65 - 69.
YAO Lan, WANG Xinmei. A Study on the Network Active Defense Technology Based on Deception[J]. Journal of National University of Defense Technology, 2008, 30(3): 65 - 69. (in Chinese)

[9] 王璐, 秦志光. 业务蜜网系统的有限自动机机[J]. 重庆邮电学院学报, 2004, 16(3): 87 - 90.
WANG Lu, QIN Zhiguang. Turing machine of Production Honeynet System[J]. Journal of Chongqing University of Posts and Telecommunications, 2004, 16(3): 87 - 90. (in Chinese)

(下转第 94 页)

(1. Science Institute Air Force Engineering University, Xi'an 710051, China; 2 State Key Laboratory of Solidification Processing, Northwestern Polytechnical University, Xi'an 710072, China; 3 The College of Chemistry & Environmental Science, Hebei University, Baoding 071000, Hebei ,China)

Abstract: With the development of science and technology and environment, lead - free piezoelectric ceramics has been a necessary trend, and potassium - sodium niobium (KNN) based lead - free piezoelectric ceramics has become a hotspot because of its high Curie temperature and piezoelectric properties. This paper firstly summarizes and analyzes the study direction and actuality of potassium - sodium niobium (KNN) based lead - free piezoelectric ceramics from new component, ions substitute, sintering reagent and temperature dependence in recent years, and then indicates the future hotspot and problem. We think it can improve the temperature stability to introduce diffusion mechanism into KNN based ceramics. Meanwhile, we also should study the effect of nano - sized domain on properties of KNN ceramics. At last, the paper forecasts the future study direction——the study of electric properties, of temperature stability and micro mechanism.

Key words: potassium - sodium niobium (KNN); lead - free piezoelectric ceramics; piezoelectric properties; nano - sized domain

(上接第 79 页)

[10] 王伟平,李甦,崔锦法. 一种基于蜜罐技术的入侵诱骗模型的研究与建立[J]. 云南大学学报:自然科学版, 2006,28(S1):117 - 120.
WANG Weiping, LI Su, CUI Jinfa. Research and Modelization of Intrusion Deception Based on Honeypot Technique[J]. Journal of Yunnan University: Natural Science Edition, 2006, 28(S1): 117 - 120. (in Chinese)

(编辑:徐楠楠)

Study of Intrusion Deception System Based on Network Proactive Defensive Security Model

ZHAO Hong - jing[1], ZHOU Chuang - ming[1], ZHAI Ping - li[2], YU Huan[3], ZHAO Ming - li[4]
(1. Missile Institute, Air Force Engineering University, Sanyuan 713800, Shaanxi, China; 2. Unit 93861, Sanyuan 713800, Shaanxi, China; 3. Siasun Robot & Automation Co. LTD, Shenyang 110168, China; 4. No. 631 Military Representative Room of PLA, Xi'an 710068, China)

Abstract: The situation of present network security is becoming rigorous day by day, the traditional security technologies such as firewall, intrusion detective system have some kinds of defects, that is, they cannot identify the unknown intrusion pattern effectively, the honeypot technology as a proactive defense method also has its own limitations. As to the defaults of the above every single technology and from the angle of active defense, the paper builds up an Intrusion deception architecture based on network active defensive security model, and simultaneously designs an interface system among the honeypot, firewall and the IDS to overcome the default that the firewall can not perform unreal time detection. This can decrease the false alarm and leaking alarm of IDS, make up the deficiency and unleash the superior of each method, thus, the proactive defense capacity of the network systems is enhanced. The paper also gives out a finite state auto - machine model, simulates the basic functions of the intrusion deception system, which provide a theory and reasoning supplement for the system's action description and architecture design.

Key words: proactive defense; intrusion deception; Honeypot; virtual network server; finite state auto - machine