基于闭环控制的军事网络纵深防御模型研究

刘升俭
(西安陆军学院信息化研究实验室 西安 710108)

摘 要 依据军事网络防御体系构建的特殊需求,提出了一种基于闭环控制的军事网络防御模型APR-WPDRRC。该模型采用了多层深度防御的技术策略,融合了层级架构的纵深防御技术手段,可以实现快速预警、主动保护、实时检测、紧急响应、动态恢复和精确反击诸多功能的协同联动与闭环控制,尤其在对抗大规模、分布式、瞬时万变的网络攻击时具有良好的适应性、应变性和耐攻击、强生存的网络防御能力。

关键词 军事网络,纵深防御,防御模型,闭环控制,容侵攻击
中图法分类号 TP393.08 **文献标识码** A

Study on Military Networks Defense In-depth Model Based on Closed-loop Control

LIU Sheng-jian
(Laboratory of Informatization Research, Xi'an Military Academy, Xi'an 710108, China)

Abstract According to the specific construction demand of military networks defense system, this paper proposed a new military network defense in-depth model of APR-WPDRRC based on closed-loop control mechanism. Since the model adopts technique policy of multilayer defense in-depth and integrate layer-class frame of defense in-depth technique method, it can achieve cooperation linkage and closed-loop control of fast warning, initiative protection, real-time detection, urgent response, dynamic restore and precision counterattack. The model has a good networks defense agility of adaptability, intrusion tolerance attack and strong survivability when it is confronted with large-scale, distributed, instantaneous changing network attacks.

Keywords Military network, Defense-in-depth, Defense model, Closed-loop control, Intrusion tolerance attack

军事网络系统是军队基于信息系统体系作战的基础支撑。围绕"破网"与"护网"的网络对抗日渐成为军事信息对抗的主要样式,也是军事信息系统建设的重要任务。由于网络攻击技术常常超前于网络防御技术,而且网络攻击是"点"的攻破,因此网络防御是"面"的防护,这使得网络攻防对抗具有易攻难防的特性。面对大规模、分布式、瞬时万变的网络攻击,近年来逐步形成的主流防御模型也受到了极大的挑战。尤其对于军事网络系统而言,构建具有良好的主动性、应变性和耐攻击、强生存能力的网络防御体系新模型,是军事网络信息对抗面临的新课题。

1 军事网络纵深防御的技术策略

当前军事网络系统的安全防御手段从最初的被动防御,如硬件防火墙(HFW);到后来的主动防御,如入侵检测(IDS);再发展到较为智能化的综合防御,如入侵防护系统(IPS)。这些手段的应用基本上都采用安全产品与技术的叠加组合的方式,即在各个相互孤立的网络关键节点"串葫芦式"地部署或简单地堆砌各种安全产品。虽然可以容易实现对小规模、已知的网络攻击行为的有效发现和阻断,但在大规模网络攻击发生时,尤其在遭受未知的新型网络攻击入侵时,其因为缺少统一安全管理而导致束手无策,同时不仅增大了安全产品的安装购置成本,也加大了后期运维管理的难度。面对日趋复杂的未知网络攻击与"海量威胁",传统的基于填空式、补丁式的安全防御模式受到了挑战,而网络多层纵深防御的技术思想应运而生,也日渐成为实现军事网络信息安全保障的核心策略。

军事对抗历史告诉我们,永远不能依赖一个单一的防线。事实上,一个网络系统的安全防御战略的谋划,就是要预先假定每个系统部件都包含了未知的但又可能被攻击者所利用的安全漏洞。任何网络防御技术手段都不可能是绝对安全的,永远不能只依赖于单一的技术手段来对抗攻击者,人们必须在降低风险性和支持防御性之间运用一种平衡策略——多层纵深防御,即在整个网络防御体系中,需要为入侵攻击者设置层层屏障。当攻击者侵入系统时,会被多个防御层阻击,并且各层防御实现功能互补,当一层防御被攻破时,其它层防御仍可保护网络的安全。这样每一层防御就降低了攻击者发现利用其脆弱性的几率。由于军事信息网络带有核心军事机密,建立多层纵深防御战略就显得尤为重要,其实现的机理就是不仅要从网络架构、操作系统、应用系统、数据库系统等广度层面上考虑全面防护,而且更要注重融合网络入侵容忍技术,从桌面PC、网络边界、内部网络乃至核心服务器等深度层面上加强积极防御;不仅能对网络入侵者增大攻击难度,而且能

本文受军队信息对抗研究重点项目(2009091504)资助。
刘升俭(1955—),男,教授,主要研究方向为军事信息安全、网络对抗技术等,E-mail:xllsj@hotmail.com。

在网络攻防对抗过程中不断完善并形成新的防御策略，即使某层防护机制遭到破坏时，也能快速发挥深层配置的安全产品优势，最大限度地实现全方位防御。如图 1 所示，一个 n 层的军事网络纵深防御体系构建策略应主要考虑从主动防护、实时检测和容侵攻击诸多方面精心设计。

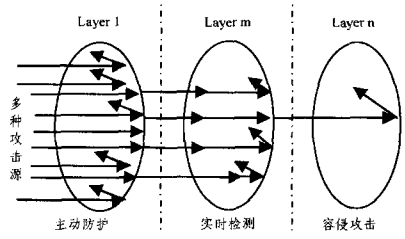

图 1　军事网络纵深防御技术策略

1）主动防护。由于军事网络系统愈来愈复杂，网络攻击的手段也与时俱进，花样翻新。因此，网络安全产品通常不可能发现所有的网络脆弱性及其外部攻击。即使在安全产品推出时，尽可能设计了全面的安全防御功能与服务，但随着时间的推移和攻击技术的发展，总会有未知的、新的攻击未被击退而穿透防护层。

2）实时检测。即使一个多层的防御也不排除被成功攻破的可能性，必须利用各种技术手段来对那些没有被成功击退的攻击能进行实时检测。然而，当今的网络入侵检测产品通常只能对那些之前已知的攻击进行检测，同时伴有一个非常高的漏检、虚警等技术缺陷。无疑，一个网络防御体系可能面对的是一种检测系统永远不可预知的新型网络攻击。

3）容侵攻击。入侵容忍（Intrusion Tolerance）技术融合了数据容错、免疫理论、门限密码、数据恢复等相关理论和技术，使用可信计算、可信网络、容错协议等组件，采取硬件或数据冗余、备份恢复策略和入侵屏蔽等容忍设计，对防御各系统进行融合设计，完全摒弃了传统的依赖 IDS 成功检测所有入侵攻击的主观臆断，使网络系统具有能够最大限度地容忍各种入侵攻击、自我修复和强生存等防御能力，做到即使其遭受强攻击，而仍能维持网络正常运行，仍然能够连续地提供网络服务，实现网络系统主动应变的安全运行。

2　军事网络纵深防御的层级架构

当前传统的网络安全防御体系基本上属于典型的安全设备和技术的层级组合模式。依据纵深防御技术策略，军事网络安全体系依次可划分为机密层、核心层、安全层、基本安全层、可信任层、非安全层、危险层等多个不同的安全域。分析各个安全域的信息类别，评估其可能遭受到的攻击级别，按防御层次的不同目标，配置相应的安全防御机制，采用相应的安全防御技术手段，形成一个军事网络线性纵深防御层级架构，如图 2 所示，它能够实现对网络节点 1－7 层协议的执行与服务状况的线速、全域的分析和监视，校核访问权限，监控非法、异常入侵行为。从线性层次的角度，由内向外，各个层次的安全性逐层递减；而从攻击者的角度，由外向内，各个层次的防御性逐层递增，以此形成了一种线性层级防御体系。面对日益增多的网络攻击源，该架构认可风险的存在性，其理想效果就是尽可能地使攻击者穿越防御层的机会逐层递减，穿越最末层的概率几乎趋于零。事实上，各层防御技术手段的有效运用，可以选用不同的安全产品，形成不同层级的安全防御解决方案。在军事网络纵深防御体系层级架构中，通常以 HFW、防毒网关、VPN 以及基于多核＋FPGA 硬件架构、集成 HFW、IDS/IPS 和防毒网关等多功能于一身的统一威胁管理（UTM，Unified Threat Management）平台等防护手段形成一级防线；而以基于 BPDU Guard、PVLAN、MPLS 隔离与认证等安全机制构成二级防线；再以基于 ACL、Honeynet、IPSec 的访问控制手段形成三级防线；其后依次以基于状态检测的隔离技术、基于流量分析的关联识别、基于内容分析的行为识别、基于专家系统的威胁识别和基于行为模型的应用识别等防御手段，如此形成四级、五级等多层级向纵深发展的防线，其将主动防护、实时检测和容侵攻击的关键防御技术融合到体系之中，由此实现线性多层级的深度防御功能：一是为军事网络提供强有力的安全保护手段，阻止非法入侵和恶意攻击；二是在未能有效防范攻击的情况下，提供动态检测手段，实现对入侵攻击的实时响应；三是当军事网络遭受各种新型攻击威胁时，形成对入侵攻击的行为识别、全程监视、实时追踪以及隐蔽诱骗，从而保障军事网络系统的正常安全运行。

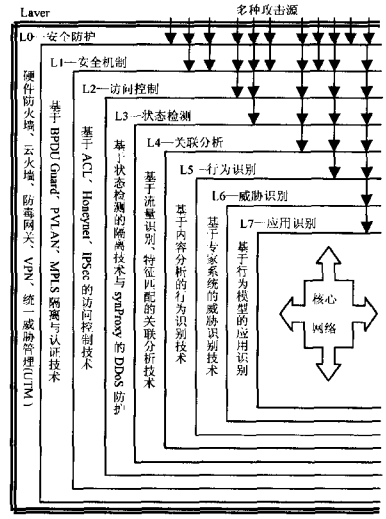

图 2　军事网络纵深防御体系层级架构

3　基于闭环控制的军事网络纵深防御模型

随着网络安全技术的发展，业界先后提出了多种网络安全防御模型，尤以 P-PDR 主流模型为代表。P-PDR 的实现过程就是在安全策略（Policy）指导下，防护（Protection）、检测（Detection）和响应（Response）3 种防御手段实现的一种线性层次防御。虽然它能通过检测和响应（DR）手段完成动态防御，但它既不能在网络攻击前发出预警，也不能实时地在网络攻击时实现告警，更不能在网络攻击后迅即恢复系统，并运用有效的网络反击预案，快速形成反击能力。因此，P-PDR 模型虽具备了防御层次，但对防御大规模、分布式、瞬时变化的军事网络攻击缺乏强有力的抗击能力，无力应付新的网络安全威胁行为，尤其是不能增强网络系统自身免疫能力的动态提升。针对现有网络防御模型存在的缺陷，依据军队信息安全保障体系建设需求，采用纵深防御的技术策略，融合防御体系层级架构的技术手段，提出了一个基于闭环控制的军事网络防御模型 APR-WPDRRC，如图 3 所示，主要包括以下要素：

3 个重要环节 APR：风险评估（A）＋安全策略（P）＋技装

资源(R)。网络安全风险分析(Analysis)是网络防御的首要环节,主张通过风险评估与控制机理,预期网络系统的安全风险,为确定安全策略提供依据;安全防御策略(Policy)指导防御技术手段的有效实施,在整个网络安全防御中处于指导地位,是防御体系的核心。技装资源(Resources)包括力量、装备和技术等网络防御资源。网络防御的主要力量源自新型网络对抗装备武装并掌握网络对抗技术的网络士兵。

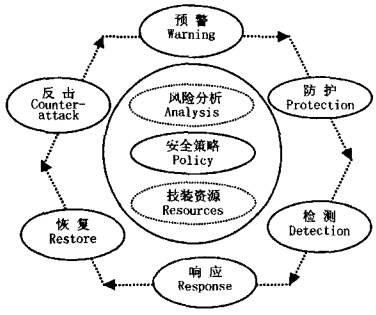

图3 军事网络防御APR-WPDRRC模型

6种技术手段WPRDRRC:W(预警)+ P(防护)+ D(检测)+ R(响应)+ R(恢复)+ C(反击)。它是在PDR中融入纵深防御层级架构技术,并在PDR前增加了预警(Warning),在其后增加了恢复(Restore)和反击(Counterattack),使防御体系具有较强的时序性、可控性和协作性,突出了网络防御要从"事前"(攻击发生前)的入侵预警+安全防护、"事中"(攻击发生时)的动态检测+实时响应、"事后"(攻击发生后)的灾难恢复+精确反击3方面全程考虑,强调了在加强安全防护的同时,还要形成对攻击威胁的快速反应;也强调了在提高网络系统抗击能力的同时,更突出了系统被攻陷后的恢复和反击能力;还强调了闭环控制下反馈机制的形成,更注重了系统防御能力的动态提升。从逻辑层次上,WPDRRC是以WPD实现积极主动防御,以RRC实现系统整固防御,6种技术手段轮式往复,构成了一个具有闭环控制机制的纵深防御模型。其中:入侵预警(W)通过建立有效的"预警反应"机制,当发现网络违规模式和未授权的网络访问尝试时,预警系统能够根据系统安全策略快速反应,如报警、跟踪、封堵和隔离等。目前出现了基于过程推理的预警系统、代理型防火墙预警系统、IDS与FW联动预警系统等;安全防护(P)、动态检测(D)和实时响应(R)中融入线性层级纵深防御的技术手段,在检测到网络入侵攻击之后能包括做好实时响应方案中的一切准备工作,从而把系统调整到安全状态;灾难恢复(R)是由灾难评估、安全恢复、修补漏洞、重构系统等诸多提升网络系统生存能力的技术手段组成;精确反击(C)是通过修复系统、封堵漏洞、追踪并精确定位攻击源,迅速组织力量,采用网络僚机技术、告警与取证技术、攻击源追踪技术、网络攻击诱骗技术等展开快速反击。

在APR-WPDRRC模型中,外围是依次连接的6种技术手段环节构成的同心六边形,内层是依据、策略、资源构成的六边形的核。依据是前提,策略是核心,资源是保证,3者紧密协作,6种技术手段有机联动将预期的安全防御策略变为安全现实。通过组织网络攻防仿真试验,验证了该模型在对抗大规模、分布式、瞬时万变的网络攻击时具有良好的适应性、应变性和耐攻击、强生存的能力,不仅能有力地抵御多种已知的网络攻击,而且也能主动地防御新型的未知的入侵攻击。

结束语 本文提出的纵深防御模型对建立一个全方位的军事网络安全体系具有一定的理论研究和现实意义。从系统整体性出发,进一步的研究需要完善模型整体功能,如融入基于蜜网的网络诱骗防御技术、基于免疫的动态检测技术和基于网格的协同联动防御技术等,建立起平战结合、技术管理一体、综合完善的多层次、多级别、多手段纵深防御的军事网络系统安全体系。

参考文献

[1] 卢昱,等. 协同式网络对抗[M]. 北京:国防工业出版社,2003

[2] 肖军模. 网络信息安全与对抗[M]. 北京:解放军出版社,1999

[3] 陈亚东. 网络攻击与防御[M]. 北京:国防大学出版社,2007

[4] 刘升俭. 网络对抗技术[M]. 长沙:国防科技大学出版社,2008

[5] 樊莉. 军事信息系统安全防御体系建设探讨[J]. 计算机安全,2009(2)

(上接第91页)

其流程如图8所示。

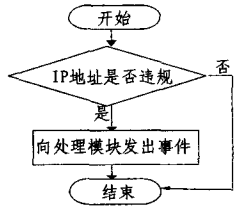

图8 NotifyAddrChange函数的调用及其相关流程

结束语 本文就特殊专网中的网络访问控制进行了探讨,设计并实现了一个网络访问控制软件。所设计的软件经过测试,其稳定性保证7*24小时工作,达到了既定的网络控制管理的功能,并在实际运用中达到一定的效果。但该软件任存在不足,如网络传输部分可以改为带宽占用更少的UDP协议进行传输,在对IPv6的兼容方面仍需改进以适应将来的网络环境,以及服务器端的界面设计可以更人性化等。

参考文献

[1] 中国互联网络信息中心(CNNIC). 第27次中国互联网络发展状况统计报告[R]. 2011

[2] 网易. 科技板块[OL]. http://tech.163.com/09/1120/07/5OH-VMPTU000915BE.html

[3] 封富君,李俊山. 新型网络环境下的访问控制技术,2007.04:17

[4] 中国业界资讯站[OL]. http://www.cnbeta.com/articles/129265.htm

[5] Faria D B, Cheriton D R. DoS and authentication in wireless public access networks[C]//Proc. of the 3rd ACM Workshop on Wireless Security. New York:ACM Press,2002:47-56

[6] 汪涛. 无线网卡驱动程序设计与实现技术研究[D]. 西安:西北工业大学,2005

[7] MSDN(Microsoft Developer Network)[OL]. http://msdn.microsoft.com/