军事网络对抗安全预警技术研究

刘升俭 孙虎元 王金宝

(解放军边防学院教研部 西安 710108)

摘 要 随着军事网络对抗技术的发展,网络安全预警管理已成为构建军事网络对抗纵深防御体系的关键环节。针对军事网络对抗现实环境,运用军事网络纵深防御策略及其安全预警机制,提出了构建一个实时态势感知、技术与管理协同、平时与战时无缝衔接的军事网络安全预警系统的设计原则、研发目标及其功能结构,并对目前预警系统的实现原理与技术进行了探究。

关键词 军事网络,网络对抗,纵深防御,安全预警,预警系统

中图法分类号 TP393.0 **文献标识码** A

Study on Security Early Warning Technology of Military Network Countermeasure

LIU Sheng-jian SUN Hu-yuan WANG Jin-bao

(Department of Teaching and Research, PLA Border Defense Academy, Xi'an 710108, China)

Abstract With the development of military networks countermeasure technology, network security early warning management has become an essential part of constructing military networks defense in depth system. This paper focused on military networks countermeasure real environment, use of security early warning mechanism in the military network defense-in-depth strategy, proposed the design ideas, reaching goals and function structures of military network security early warning system which is built into a real time situation awareness, technical and management coordination, peacetime and wartime seamless connection. Finally, the current implementation principle and technology of early warning system were summarized.

Keywords Military network, Network countermeasure, Defense-in-depth, Security early warning, Early warning systems

军事网络是军事信息系统的基础支撑,军事网络对抗是军事信息对抗的主要样式。随着网络攻防对抗的博弈,人们发现多年来基本上由防火墙、杀毒和入侵检测的"老三样"产品形成的网络对抗模型,已经面临极大的挑战。尤其对于军事网络防御而言,还要面对一个"在网络的内外两侧同时作战"的特殊环境。因而,人们就开始把目光转向安全审计、态势感知、证书认证、可信模块等其它技术领域,希望寻找到第四种、第五种以至于第N种技术元素,以达到"防患于未然"——网络安全防御预警技术应运而生。近年来,面对大规模、分布式、瞬时万变的军事网络攻击,以新的思路、新的方法和新的策略加强网络安全预警技术研究,构建具有良好的主动性、耐攻击、强生存能力的网络对抗体系,提升军事网络安全预警能力,是当前军事网络对抗面临的紧迫课题。

1 网络纵深防御策略与预警机制

由于军事信息网络带有核心军事机密,确立军事网络多层纵深防御战略就显得尤为重要。分析现有网络防御模型存在的缺陷,虽然它能通过检测和响应手段完成动态防御,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。依据军队信息安全保障体系建设需求,融合防御体系层级架构的技术手段,提出了一个基于纵深防御策略的军事网络防御模型APR-WPDRRC,如图1所示。在APR-WPDRRC模型中,外围是依次连接的六种技术手段环节构成的闭环六边形,内层是依据、策略、资源构成的六边形的核。A(分析)是前提,P(策)略是核心,R(资源)是保证,三者紧密协作,6种技术手段W(预警)P(防护)D(检测)R(响应)R(恢复)C(反击)有机联动,将预期的安全防御策略变为安全现实。

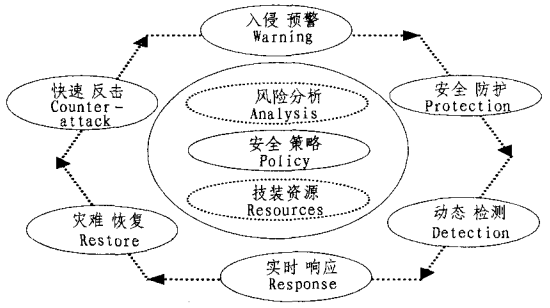

图1 军事网络纵深防御APR-WPDRRC模型

从逻辑层次上,WPDRRC以WPD实现积极主动防御,以RRC实现系统整固防御,以6种技术手段轮式往复,构成

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。

了一个具有闭环控制机制的纵深防御模型。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(W)，在其后增加了恢复(R)和反击(C)，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＋精确反击三方面全程考虑，强调在加强安全防护的同时，还要形成对攻击威胁的态势感知；强调在闭环控制下提高网络系统抗击能力的同时，要突出攻击入侵的快速预警能力，更要注重系统防御能力的动态提升。

在 WPDRRCW 模型中，入侵预警(W)不仅是纵深防御六个行动的第一步，也是构建网络纵深防御体系的关键环节。分析入侵预警的运行机制，就是利用网络中部署的安全系统和安全部件，监视网络中的节点状态并检测跟踪入侵异常行为，立足于信息跟踪的“提前量判断”，可称之为“预”的能力；基于当前的网络状态和已监测到的入侵判断，通过预警体系预报疑似对象的特征，预测未来时刻可能发生的入侵行为，实时发出警报；当发现特定进程发展到某一预设阶段，就采取“中止”、“隔离”或“清除”等措施，以制止入侵事态继续蔓延。

2 网络安全预警系统的设计原则与目标

目前，网络攻击的目标对象在基本理念、攻击模式、技术能力、组织形式和运行速度方面都已经大大突破了传统方式，呈现出快速多变海量的特点。一个主动有效、反应灵敏的军事网络纵深防御预警系统不仅需要识别已知的入侵攻击模式，还要有能力准确预知未知入侵攻击的可能性，并且也能具体指证将要发生的入侵行为和产生的后果。而目前在预警中常常连续运行的入侵检测系统(IDS)报警量常常达到 G 数量级，最多时有 99%以上是无关报警。报警量大、不相关报警多，使安全防御面对大量报警信息，很难实时了解网络系统的安全威胁状况，不能及时采取合适的响应措施。为使网络预警系统具有弹性化组织形态及超常规反应能力，应突出硬件与软件建设的紧密结合，强化以下设计原则：(1)系统性原则。预警管理系统的软硬件指标应使预警管理体系层次清晰、结构合理，软硬件相互联系、相互补充，能全面反映预警任务内容的综合情况，以保证预警管理体系的全面性和可信度；(2)高效能原则。要构建以扁平化矩阵式指挥控制硬件系统为核心、以标准化数据和应用软件资源为基础、以先进理论、高素质人才队伍、法规制度和技术装备为支撑的高效的信息网络安全预警体系；(3)生存性原则。信息网络攻防对抗的过程始终渗透于网络全纵深、多方位，既涉及硬件管理平台，又威胁软件技术系统。要未雨绸缪做到硬件与软件标本兼治，确保预警管理系统能够经受住各种网络攻击行为的考验；(4)预防性原则。构建一个硬件与软件相互配合、能够“发现隐患、制定对策、提升强度、效果认证”的闭环式、反馈型、非线性的预警系统，以提高预判能力，完善预报机制，加强应急响应；(5)多元性原则。加强网络安全预警管理硬件和软件系统协同发展，不但要具有实时性，而且还要具备全局性和前瞻性；不但应有基于传统的被动提升模式，而且还应发展以主动演变为基础的广谱、立体化的安全预警能力，具备与信息化发展水平相匹配的“快速变轨”能力；不但应有面向单一网络的安全预警能力，而且还应具备面向多种网络的安全预警能力。

面对无孔不入、无时不在的军事网络入侵攻击，构建一个相对完备的网络安全预警系统，至少应实现以下多层次目标：(1)对网络信息基础设施的安全状况及威胁的来源和程度能迅速全面系统地做出风险评估；(2)以网络入侵威胁来源为对象，按时间顺序、入侵序列、动作意图、威胁范围和程度能实时地进行统计、分析及审计；(3)对来自外部网络的恶意代码和违规操作能快速地通过入侵事件归约、融合关联分析进行识别、跟踪、记录、分类和报警，提高系统及时、主动发现入侵攻击事件的能力；(4)建立一套有效的“预警响应”运行机制，为遭到破坏的网络及信息系统的恢复提供技术性支持，任何时候都不能区分闲时、忙时而松懈和疏忽，不能有平战转换的结合部和过渡期，做到平时与战时无缝衔接，使网络安全预警管理无懈可击。

3 网络安全预警系统的功能结构设计

为构建一个基于主动实时发现、具备多维协同机制的网络预警管理的“闭合环链”，将系统调整到“最安全”和“风险最低”的状态，实现“防患于未然”的网络预警效果，预警系统至少具有以下功能：

1)数据挖掘，生成态势信息。运用 Web 挖掘技术，从运行网络的海量信息数据中，检测、审计并提取病毒、木马、蠕虫等特征代码，将其汇总生成网络系统预警态势信息。

2)信息融合，形成决策信息。对提取和汇总出来的态势信息进行多级别、多方面、多层次的实时决策信息处理，从而形成完整性、实时性、统一性的预警决策信息。

3)态势感知，运行报警机制。依据未来可感知的一段时间内网络安全态势的预设指标，以及当前形成的预警决策信息进行定量与定性评估，主动地运行报警程序，动态地提升网络系统的预警频率和强度。

4)快速反应，启动应急预案。在得到网络安全预警信息后迅速通知网络管理者。在辅助决策工具的协助下，管理者能快速地做出是否启动应急处理预案的决定。

为有效地实现军事网络纵深防御预警的目标与功能，一个网络安全预警系统设计由网络监控、入侵检测、运行预警和信息追踪 4 大功能模块组成，如图 2 所示。

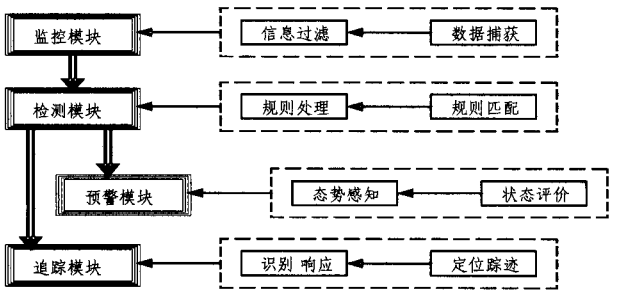

图 2 网络预警系统功能结构

3.1 监控模块

通过监听流入网络的各种信息，控制进出网络的数据流量，实现基于 IP 地址的访问控制和对常用高层协议的信息收集过滤；通过基于端口的流量统计可以知道网络的基本使用情况；通过对日志记录的分析可以收集到网络内部用户非法行为等。

3.2 检测模块

通过对监控收集的数据流进行规则匹配，对入侵攻击行为及用户误操作进行识别检测和规则处理，发现系统的威胁

和弱点，甄别入侵者和不同的入侵行为。此模块实现了数据的搜集和归纳，行为的分析和分类，它能将捕获的数据传入预警模块，为预警机制服务，同时也将捕获的数据传入追踪模块，为追踪响应服务。

3.3 预警模块

通过动态地检测识别入侵访问及操作，当发现网络违规模式和未授权的网络访问尝试时，预警系统能根据系统安全策略实时地进行网络系统态势感知，即确定威胁来源，对威胁事件进行分类、统计分析等，快速地确定预警级别，运行多种报警程序。

3.4 追踪模块

采用信息追踪技术，判断攻击入侵者的踪迹，定位攻击源的位置，推断出攻击者在网络中的穿行路由等，从而为事后的风险审计及取证工作提供充足的证据，为系统的应急响应提供有价值的信息。

上述4个模块中，检测和预警是系统功能实现的核心，部署在网络核心节点，二者协作使得系统由静态的防护转化为动态的预警，同时也是强制执行安全防御策略、及时准确地做出预警防范的有力工具。

4 网络安全预警系统的实现原理与技术

面对复杂的网络入侵活动，网络预警技术的研究不仅仅包括入侵技术的研究，而且更需要开展入侵检测策略与模型、审计分析策略研究等，并将这些技术组合起来，形成一个功能互补、技术协同、互动发展的预警机制，包括风险识别和风险控制、误操作与弱点漏洞检测等事前管理手段，当发现网络违规模式和未授权的网络访问尝试时，预警系统能够做出快速反应，如报警、跟踪、封堵和隔离等。

4.1 基于攻击过程推理的预警系统

基于攻击过程推理的预警系统，其实现原理就是在攻击过程识别中，对不断收到的警报，根据相关规则，首先形成相关的警报序列，然后将这些警报序列和完整攻击过程的参考序列相比较，得到当前攻击序列下可能的攻击行为和步骤。由于在预测时，检测的警报还不能构成一个完整的入侵过程，采用不完全序列匹配，可能会有多个匹配结果。警报序列之间相似程度与警报序列的组成、长度和警报在序列中不同的位置有关，为定量表示和衡量这些差别，使用序列匹配相似度计算当前序列和所有参考序列的匹配相似度；选取发生概率最大的那个参考序列作为可能发生的入侵过程；根据已发生的入侵序列，识别出最有可能的攻击计划和入侵过程，然后依据相应的计划和过程，对下一时刻的入侵行为和步骤进行推理预测。因此，基于警报数据的入侵过程的识别和可能目标的判断是实现预警的关键。

4.2 基于代理型防火墙的预警系统

利用人工智能技术，网络预警系统首先对防火墙日志数据以及若干个反映用户行为特点的变量进行实时分析，每隔一定的时间对用户的所有网络行为进行采样审计，然后运用用户网络行为习惯模型对该采样值进行统计，判定是否为该用户的正常行为，同时把采样值加入用户特征数据样本集合中。网络安全专家系统定时地对每个用户的数据库进行推理，在发现可疑活动后，根据推理结果来确定相应的躲避措施，如可将该用户列入系统黑名单中，以备重点观察，或向安全管理员发送报警信息，或安全管理员将该用户封锁一定的时间来确认该用户。这样能够在攻击者实施攻击前发现其企图，并采取必要的躲避措施，同时通知系统安全管理员。

4.3 基于IDS与FW联动的预警系统

入侵检测系统(IDS)能够对网络未经授权的访问进行报警，但检测本身不能提供安全保护的作用，有时还需要通过防火墙(FW)预防这种非法网络行为。IDS与FW之间通过请求与响应的方式实现联动预警功能，即IDS发现入侵行为，自动报警发送给FW，FW加载动态规则拦截入侵，阻止后续的攻击流。FW可以通过IDS及时发现其策略之外的攻击行为，IDS也可以通过防火墙对来自外部网络的攻击行为进行阻断，这就可以大大提高整体预警防护能力。

4.4 基于DIDS与DFW协作的预警系统

针对网络攻击日益呈现的相互协作入侵的特征，协作互动预警功能也日趋实用化。利用多个检测主体协作，采用分布式入侵检测(DIDS)，可以更全面、更准确地检测预警入侵事件。然而，DIDS的防御能力有限，通常对检测到的入侵事件仅能提示报警。分布式防火墙(DFW)自身是一个静态防御系统，主要完成访问控制，而在入侵检测方面的能力薄弱，单一DFW在网络防御上能力很有限。针对网络协作攻击的复杂性，结合DFW与DIDS的各自技术优长，实时、智能地设置DIDS、DFW各部件的安全策略，形成一种新型的网络防御协作预警系统，即根据事实库中的入侵事件，利用知识库中的知识进行推理，以确定对入侵事件的响应，再积极防御并追踪入侵源，利用专家系统，结合动态更新的专家知识，实现对已检测的入侵或攻击行为的自动响应。

结束语 网络安全预警系统及其管理是一个多层次的复杂的社会系统工程。尽管网络安全预警系统总免不了误警、漏警和虚警的困扰，但从目前看来，仍不失为从网络安全层面最大程度降低危害的重要举措。网络安全预警是技术防范和管理建设相结合的产物，要坚持“规范制度、技管并重”的建设思路，真正增强网络防御系统主动发现、实时感知和自我防御的能力，从先感染后免疫的“亡羊补牢”的被动态势向全域的实时预警补网的主动设防形态转变；必须进一步规范制度，强化管理，健全管理机制，通过严格制度，促成管理与技术高度融合以形成合力，在很大程度上弥补网络安全预警建设的“漏洞”和“短板”，建立起平战结合、内外兼顾、技术管理融合的多层次、多级别、多手段的具有弹性化组织预警形态及超常规反应能力的军事网络纵深防御预警体系；同时加强网络安全文化建设，真正使“预防为主”的理念深入人心，使主动报告安全隐患、主动保护网络安全成为网络社会的行为规范。

参考文献

[1] 刘升俭. 军事网络纵深防御模型研究[J]. 计算机科学，2011(10)：164

[2] 刘升俭. 网络对抗技术[M]. 长沙：国防科技大学出版社，2008：01

[3] 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)：86

[4] 苗青. 网络安全战略预警系统的攻击检测技术研究[J]. 计算机工程与科学，2002(18)：34

[5] 张险峰. 网络安全分布式预警体系结构研究[J]. 计算机应用，2004(6)：123

[6] 王志刚. 浅谈信息网络安全预警管理的几点策略[J]. 魅力中国，2010(27)：56