防空信息网络纵深防御体系研究

黄仁全[1,2] 李为民[1] 张荣江[3] 贺泽维[1]
(空军工程大学导弹学院 三原 713800)[1] (中国人民解放军93942部队 咸阳 712000)[2]
(中国人民解放军94188部队 西安 710077)[3]

摘 要 防空信息网络安全是对信息化条件下的防空作战提出的新课题。从信息网络硬件、操作系统和网络协议的脆弱性出发,分析了防空信息网络安全存在的巨大隐患,并研究了防空信息网络面临的外部威胁和内部威胁。为维护防空信息网络安全,提出了纵深防御策略,建立了防空信息网络纵深防御的广度和深度模型,并探索了防空信息网络纵深防御技术体系,研究了其关键技术。

关键词 防空信息网络,纵深防御,"舒特"系统,网络攻击
中图法分类号 TP393 **文献标识码** A

Research on the Defense in Depth System of Air Defense Information Network

HUANG Ren-quan[1,2] LI Wei-min[1] ZHANG Rong-jiang[3] HE Ze-wei[1]
(The Missile Institute of AFEU, Sanyuan 713800, China)[1] (PLA, No. 93942 Troop, Xianyang 712000, China)[2]
(PLA, No. 94188 Troop, Xi'an 710077, China)[3]

Abstract In the information age, the security of air defense information network is a new challenging problem to the air defense system. According to the frangibility of the hardware, operation system and the network protocol, there was a great danger hidden in the air defense information network, and both of the outside and inside threats were studied. For keeping the security of the air defense information network, the defense in depth strategy was proposed, and then the defense models were constructed both in length and depth. At last, the technology framework was analyzed, and the key technology was studied.

Keywords Air defense information network, Defense in depth, Suter project, Cyber attack

1 引言

信息化条件下,防空信息网络面临严峻的威胁[1]。海湾战争中,美国特工把携带计算机"病毒"的芯片安装到伊拉克的打印机中,并通过无线遥控将病毒激活,致使伊方防空指挥系统陷入瘫痪[2];2007年9月6日傍晚,以色列空军运用美军研制的"舒特"系统,成功入侵叙利亚防空雷达网并成功"接管"了网络的操控权,使叙方防空体系处于失效状态,从而躲过叙利亚军队苦心经营多年的防空体系,对叙方纵深100公里内的所谓"核设施"目标实施了毁灭性突击[3];据有关媒体报道,2011年3月19日法国、美国、英国等西方国家对利比亚发动的"奥德赛黎明"军事打击中,美军使用了"舒特"系统压制利比亚防空火力。此外,美军通过一项"小企业创新研究"计划,正在研制更有效的、能通过有线/无线方式注入敌方计算机系统的计算机病毒,其中包括通过天线电磁波辐射注入病毒和利用卫星进行辐射式注入病毒等;美军还在研究能远程注入计算机病毒的"病毒炮",计划用10年的时间研制出"病毒炮弹"[4]等。防空信息网络将成为空袭方实施网电攻击的首要目标,通过对防空信息网络的攻击,达到瘫痪整个防空体系的目的。因此,防空信息网络将面临空前威胁,研究其防御体系具有重要的理论和现实意义。

2 防空信息网络安全分析

防空信息网络安全性主要体现在以下两个方面,一是信息网络本身具有的脆弱性,二是防空信息网络所面临的安全威胁。

2.1 防空信息网络安全脆弱性

由于我国信息技术基础较薄弱,使得许多硬件、软件都依赖于进口,并广泛应用于国防与军队信息化建设过程中,从而为防空信息网络安全埋下了巨大隐患。防空信息网络安全的脆弱性主要体现在以下几个方面:

硬件设备的脆弱性。实现防空体系网络化的技术基础是计算机及网络技术的飞速发展,而计算机硬件在制造和使用过程中,由于设计或人为的原因存在一些安全漏洞。制造计算机硬件的国家,在计算机硬件及其外围设备的生产或运输过程中有意识地在硬件芯片中固化病毒或其他恶意代码,在战时通过遥控手段激活,从而让计算机病毒等恶意代码在网络中迅速传播,瘫痪整个信息网络系统,或为网络入侵提供后

本文受国家科技重点实验室基金项目(9140XXXXXX110)资助。
黄仁全(1983—),男,博士生,主要研究方向为防空作战建模与仿真,E-mail:huangrenquan@126.com;李为民(1964—),男,博士,教授,博士生导师,主要研究方向为防空反导作战运筹分析。

门。

操作系统的脆弱性。从操作系统发展角度看，多用户操作系统的主要目标是为用户提供基于主机的多用户分时管理、资源共享，系统安全技术特别是安全内核技术并没有得到充分考虑。如常见的 Windows、Unix、Linux、VxWork 等操作系统，其脆弱性主要体现在[5]：操作系统为提高运行效率，把设备驱动、文件系统等实现在操作系统内核中，导致内核庞大，降低了系统的稳定性和安全性；存在特权主体，目前大多数操作系统都是基于用户的访问控制，若以操作权限较高的用户账号登录系统将会对信息系统的安全构成更大范围的潜在威胁；缺乏安全的系统扩展机制，为满足不同用户的需求，操作系统一般都具有较好的可扩展性，但另一方面由于内核扩展程序运行于特权状态，可以访问全部系统资源，如果这些程序存在漏洞或本身就是恶意代码，将对系统构成严峻威胁。

网络协议的脆弱性。从网络协议的角度分析，TCP/IP 协议是当今使用最为广泛的网络协议，它的主要设计目标是互联、互通与互操作，主要是为了沟通，而不是安全。TCP/IP 协议制定有其特定环境的历史局限性，它是在资源及网络技术均不十分成熟的情况下设计的，因此协议中已有许多人所共知的安全漏洞和隐患，如 IP 地址的易欺骗性、源路选项漏洞及数据报重组漏洞等。

在防空信息网络构建过程中，国外硬件产品的大量引入，如 CPU、芯片等，商业化操作系统的普遍应用，如 Windows、Unix、Linux、VxWork 等操作系统，以及通用通信结构和通信协议的广泛使用，如 IEEE 802.3 通用以太网结构、TCP/IP 协议等，为空袭方实施网络攻击提供了便利条件，从而对防空信息网络安全构成严峻威胁。

2.2 防空信息网络安全威胁

从防空信息网络安全威胁产生的原因分析，主要包括两方面内容：一是外部威胁，即空袭方对防空信息网络攻击产生的威胁；二是内部威胁，由于防空信息网络管理不当或操作失误等原因产生的威胁。

(1)外部威胁。目前，我国防空信息网络遭受的外部威胁主要包括："舒特"系统攻击、恶意代码攻击、网络攻击和预置陷阱等。"舒特"系统是美国空军代号为"庞大远征狩猎(Big Safari)"绝密计划的重要组成部分，目前已经发展到了第五代[6,7]，其技术能力如表 1 所列。病毒是破坏防空信息系统的一种有效方式，早在海湾战争中美军已经使用过病毒攻击伊防空系统，并正在研制通过有线/无线方式注入敌方计算机系统的计算机病毒，其中包括通过天线电磁波辐射注入病毒和利用卫星进行辐射式注入病毒；此外，还在研究能远程注入计算机病毒的"病毒炮"，计划用 10 年的时间研制出"病毒炮弹"。预置陷阱是防空信息网络安全中最可怕、最难防的一种威胁，通过人为在信息网络中预设一些具有特殊功能的"陷阱"来破坏和干扰信息网络的正常运行，通常分为硬件陷阱和软件陷阱；硬件陷阱，如对芯片采取特定措施，在一段时间或接收到某种特定信号后自毁；常见软件陷阱，如特洛伊木马、逻辑炸弹和陷阱门等。若能够通过有线/无线或其他方式进入防空信息网络，则可以对整个网络系统实施攻击。就防空雷达网络而言，国外公开报道的进入途径有多种，例如使用辐射信号直接进入雷达接收机；通过指挥控制中心和雷达或武器平台之间的通信链路，特别是无线通信链路进入防空雷达网络；还可以通过防空雷达网络中的信息处理设备进入。一旦进入防空信息网络，攻击方可采用协议攻击、缓冲区溢出攻击以及拒绝服务攻击等攻击手段攻击防空信息网络。

表 1 "舒特"系统技术能力

发展阶段	时间	技术特点
"舒特"Ⅰ	2000	实现了"从传感器到射手"的集成，能看到防空雷达的探测结果
"舒特"Ⅱ	2002	攻击者作为管理员接管网络，并开始控制网络节点上的雷达，使防空雷达探测不到飞机目标
"舒特"Ⅲ	2004-2005	增加了入侵时敏目标链路(TCT)能力，将作战对象扩展到战场弹道导弹发射系统、移动地空导弹发射系统及通信系统
"舒特"Ⅳ	2006-2007	提升了战略防空导弹指挥控制网络的作战能力，检验了由地面、航空和航天节点组成的通信网络对地面传感器的远程监控能力，验证了针对相控阵雷达的信息作战能力
"舒特"Ⅴ	2008	将作战对象扩展到国家级指挥控制系统、一体化战略防空系统、反导反卫和大规模杀伤武器系统等网络化战略目标的关键信息节点和通信链路，提高了识别和定位指挥控制系统能力，对移动式、组网式系统可提供非传统情报、监视与侦察以及空间信息的联合战场态势情报，并能融合多个情报源以生成通用作战态势图

(2)内部威胁。虽然病毒、"舒特"系统、黑客等外部威胁对防空信息网络安全构成巨大挑战，但是内部威胁也是构成其安全隐患的重要要素，甚至可能成为造成信息网络安全问题的主要原因。据美国联邦调查局资料显示，约 70%的网络安全事件来自于内部，内部人员由于熟悉内部网络的情况，从而更容易入侵网络[8]。网络管理人员对于技术不精或责任心不强，对信息网络系统未进行必要的安全配置和管理，对网络信息缺乏严密的监控；操作人员违反安全操作规定，不注意对系统进行口令保护，不设口令或使用很容易破解的口令，从而使入侵者冒充合法用户进入系统等等。

3 防空信息网络纵深防御体系模型

3.1 防空信息网络纵深防御的基本涵义

纵深防御思想首先在美国"信息保障技术框架"(IATF)中提出，并应用于美国国防部(DoD)的《全球信息栅格(GIG)信息保障政策与实施指南》中指导美军 GIG 的建设[5]。纵深防御的基本思想是采用多层防护防范信息网络威胁，使能够攻破一层或一类保护的攻击行为无法破坏整个信息基础设施和应用系统。

纵深防御强调 3 个主要层面[9]：人员、技术和操作。纵深防御人员要求，从组织的最高管理者开始对安全威胁具有明确的认识，并且建立有效的保障策略和程序，指定角色和责任，培训包括系统管理员和用户在内的关键人员，强制关键人员履行义务。纵深防御强调技术，并提供一个框架提供多层保护。为了提供信息保障服务和检测入侵，存在很大范围的可用技术，为保证得到和部署正确的技术，组织将建立有效的技术获取策略和过程，这些策略和过程将包括安全策略、信息保障原理系统、信息保障体系结构和标准、需要信息保障的产品准则、已经被有名的第三方确认的产品的获取、配备指南以及评估集成系统风险评估的过程。纵深防御的操作要素集中在所有的活动上，这些活动维持组织每天的安全事态。纵深

防御有关的运行领域包括：安全策略、认证和认可、安全管理、密钥管理、可用性评估和重构等。按照纵深防御思想，要达到信息网络安全保障的目的，就要求达到人员、技术和运行 3 要素的平衡。

将纵深防御思想引入到防空信息网络安全体系中，对维护防空体系网络安全具有重要的意义，并具有其具体的含义。一是在防御广度上，防空体系中的广域网、局域网以及主机之间采取不同的防护策略；二是在防御深度上，防空信息网络应当形成“预警→保护→检测→响应→恢复→反击→预警”的闭环结构。

3.2 防空信息网络纵深防御广度模型

分析网络信息安全产生原因可知，针对防空信息网络的攻击主要体现在数据层、应用程序层、主机层、内部网络层、外围网络层、物理安全层及策略、过程和意识层。正是由于安全威胁来自于各个方面，微软提出了其“纵深防御”模型，其具体防御措施如表 2 所列[10]。在防御广度上分析，防空信息网络主要包括广域网、局域网和主机 3 类防御对象。为此，防空信息网络纵深防御广度模型如图 1 所示[11]。防空信息网络纵深防御模型在广度上必须体现异构性，即不同的网络、防御主体之间应当采取不同的防御策略。若采用同构的网络防御策略，一旦一个防御网络或防御主体被攻破，则等于攻破了所有相同防御系统；采取不同的防御结构，从而迫使攻击方必须突破多个防御层才能进入，达到降低其攻击成功概率。

表 2 “纵深防御”模型具体防御措施

防御层次	具体措施
数据层	强密码、ACL、加密、EFS、备份与还原策略
应用程序层	应用程序强化
主机层	操作系统加固、身份验证、更新管理、防病毒更新和审核
内部网络层	网段、IPSec、NIDS
外围网络层	防火墙、边界路由器、窗罐(网)和具有隔离过程的 VPN
物理安全层	警卫、锁、监视设备
策略、过程和意识层	规章制度、教育

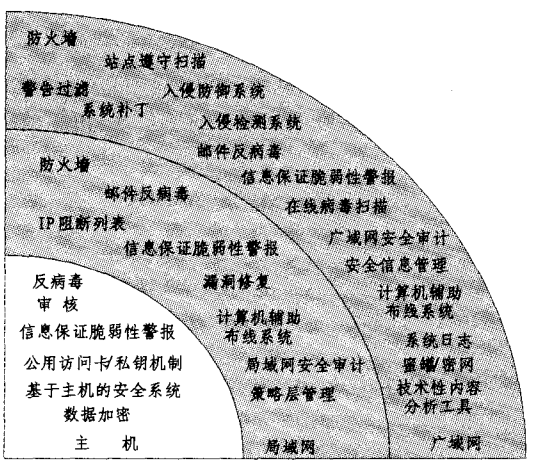

图 1 防空信息网络纵深防御广度模型

3.3 防空信息网络纵深防御深度模型

防空信息网络纵深防御在深度上的含义，主要体现在网络主动防御过程中。我国 863 信息安全专家推出了适合中国国情的信息系统安全保障体系建设模型——WPDRRC 模型[5]，是对传统 PDRR 模型的继承与发展。WPDRRC 模型主要包括：预警（Warning）、保护（Protection）、检测（Detection）、响应（Response）、恢复（Recovery）和反击（Counterattack）6 个环节。在深度上，防空信息网络的纵深防御将上述 6 个过程“预警→保护→检测→响应→恢复→反击→预警”形成闭环结构，即从第 1 层的“预警”到最后的“反击”，形成一个完整的防御过程，为以后的“预警”提供帮助，它是一种动态的主动防御过程，如图 2 所示。

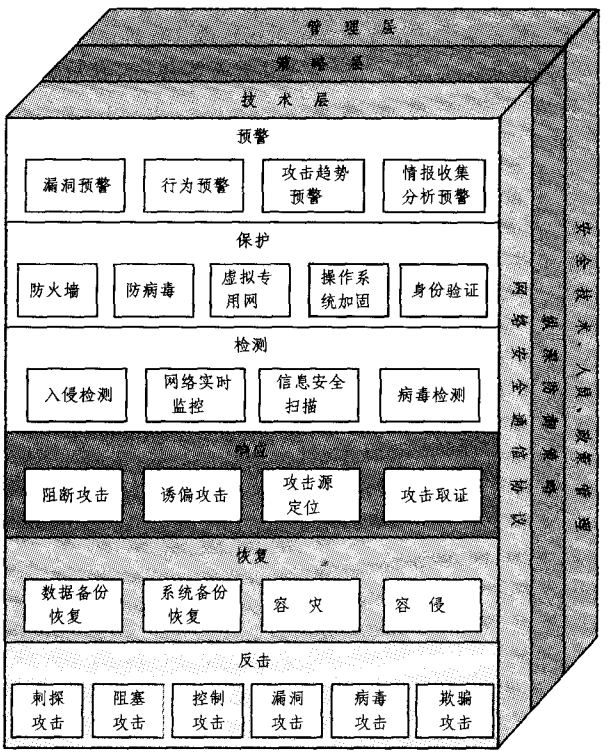

图 2 防空信息网络纵深防御深度模型

防空信息网络纵深防御深度模型包含 3 个层面：技术层、策略层和管理层。技术层包括 WPDRRC 模型的 6 个层次和一个网络安全通信协议层；策略层是指采取纵深防御策略，使得 WPDRRC 模型各层的技术在统一的安全策略下协调工作，共同构筑一个多层次纵深的防御体系；管理层主要功能是针对 WPDRRC 模型的技术、人员、策略及其它方面进行管理。

4 防空信息网纵深防御技术体系

在防空信息网络安全中引入纵深防御体系，是对防空网络安全从主机、网络、系统边界、支撑性基础设施等层面出发，将信息与信息系统的安全根据要求保障的不同层次保障起来，并实现预警、保护、检测、响应、恢复和反击的全过程防御。防空信息网络纵深防御体系，将分散系统整合为一个异构网络系统，基于联动联防和网络集中管理、监控技术，将所有信息安全和数据安全产品有机地结合在一起，在漏洞预防、攻击处理、破坏修复等方面提供整体的解决方案，从而极大地提高系统防护效果，降低网络管理的风险和复杂性。防空信息网络纵深防御体系需要应对各种内部及外部威胁，从而对纵深防御技术体系提出严格要求，其中部分关键技术如表 3 所列[5,9,10]。

（下转第 58 页）

protocol for wireless sensor networks[J]. IEEE,2003:335-340

[2] Nguyen H T T, Guizani M, Jo M, et al. An Efficient Signal-Range-Based Probabilistic Key Predistribution Scheme in a Wireless Sensor Network[J]. IEEE Transactions on Vehicular Technology,2009,58(5)

[3] Eltoweisy M, Heydari H, Morales L, et al. Combinatorial optimization of key management in group communications[J]. Journal ol Network and Systems Management,2004,12(1):33-50

[4] 孔繁瑞,李春丈,丁青青,等. 一种基于 EBS 的无线传感器网络动态密钥管理方法[J]. 电子与信息学报,2009,31(5)

[5] 孔繁瑞,李春文,焦飞,等. 基于 EBS 的动态密钥管理方法共谋问题[J]. 软件学报,2009,20(9)

[6] 黄少清,李继国. 基于二元对称多项式的 WSN 密钥管理方案[J]. 计算机工程,2010,36(16):145-147

[7] 肖德贵,杨金,罗娟. 基于多项式和分组的无线传感器网络密钥管理方案[J]. 计算机应用研究,2009,26(2)

[8] Cheng Y, Agrawal D P. A improved key distribution mechanism for large-scale hierarchical wireless sensor networks[J]. Journal of Ad Hoc Networks,2007,5(1):35-48

[9] Shen A-N, Guo Song, Chien H Y, et al. A scalable key pre-distribution mechanism for large-scale wireless sensor networks [Z]. Wiley InterScience. DOI:10.1002/cpe.142, April 2009

(上接第 55 页)

表 3 纵深防御关键技术

类型	名称	技术说明
信息加密技术	加密算法	采用加密算法包括:对称/非对称密码算法、公开密钥数字签名算法、数字签名与数字信封、数字证书等
	公钥基础设施(PKI)	由公开密钥密码技术、数字证书、证书发放机构(CA)和关于公开密钥的安全策略等基本成分共同组成,主要包括:X.509 格式证书和证书废止列表 CEL、CA/RA 操作协议、CA 管理协议和 CA 政策制定四个部分
	数据库加密	主要通过操作系统(OS)、数据库管理系统(DBMS)内核层和外层实现对数据库数据的加密
	虚拟专用网(VPN)	VPN 的重要意义在于"虚拟"与"专用",实现其技术的要点包括:隧道、相关隧道协议(PPTP、L2F、L2TF、VTP)和数据安全协议
网络隔离技术	物理隔离	实现物理隔离的常见技术包括:双网机隔离与交换技术、单主板安全隔离计算机技术、网络安全隔离卡技术和物理隔离集成器技术等
	防火墙	主要包括:包过滤、应用级网关、电路级网关和规则检测防火墙四种类型,需要依据实际需求具体使用
主动防御技术	入侵检测系统(IDS)	入侵检测系统分为:基于主机的 IDS(HIDS)和基于网络的 IDS(NIDS)。HIDS 主要用于防止对单机节点的入侵,检测目标主要是主机系统和本机用户;NIDS 主要用于防止对网络的入侵,从防火墙内部或外部监视整个网络运行
	入侵防御系统(IPS)	入侵防御系统分为:基于主机的 IPS(HIPS)和基于网络的 IPS(NIPS),实现功能包括:识别非授权业务流;主动阻断或降低对所识别的非授权业务流的服务;实时记录业务流状况,并及时向网络管理员发出警报;提供与异常数据包相关的分析数据等
	蜜罐	蜜罐可分为产品型蜜罐和研究型蜜罐,产品型蜜罐的目的在于为网络提供安全保护,包括检测攻击、防止攻击造成破坏及帮助管理员对攻击做出正确的响应;研究型蜜罐则是专门用于对黑客攻击的捕获和分析,分析和追踪黑客攻击能捕获黑客的键击记录,从而掌握其攻击目的、心理状态等信息
	蜜网	蜜网是在蜜罐技术基础上发展起来的,又称为诱捕网络,构成一个黑客诱捕网络体系架构
	安全审计	主要对操作系统、数据库、网络设备、防火墙等项目的安全审计,从而有针对性地对网络运行状态和过程进行记录、跟踪和审查
	信息取证	其目的为阻止和减小攻击事件带来的影响,根据攻击者行动留下的痕迹寻找到攻击证据,最终找到攻击者,主要包括现场保护、数据分析、结果提交、数据恢复等过程
系统抗毁技术	容灾	利用地理上的分散性,在异地建立和维护一个备份系统以保证数据对"灾难"事件的抵御能力,可分为数据容灾和应用容灾两个层次
	容侵	目的是保证系统在遭受入侵攻击发生故障时也能正常工作,或以一种无害的、非灾难性的方式停止,主要包括入侵容忍和错误触发两方面

结束语 防空信息网络安全问题事关整个防空体系作战效能的发挥,因此是信息化条件下空防对抗作战对防空体系提出的新挑战与新课题。论文分析了防空信息网络安全的脆弱性,以及所面临威胁的严峻性,从而提出了构建防空信息网络纵深防御体系,建立了纵深防御广度模型和深度模型,并对纵深防御技术体系进行了初步探索,研究了相关关键技术。论文仅抛砖引玉,防空信息网络安全问题是一个复杂的系统问题,将随着攻防对抗技术和对抗手段的发展而不断发展,因此需要不断地探索与完善。

参 考 文 献

[1] 王凤山,王福田. 防空信息战概论[M]. 北京:航空工业出版社,2002

[2] 吕登明. 信息化战争与信息化军队[M]. 北京:解放军出版社,2004

[3] 姚红星,温柏华. 美军网络战研究[M]. 北京:国防大学出版社,2010

[4] 李雄伟. 网络对抗系统及其关键技术研究[D]. 北京:北京邮电大学,2005

[5] 吴晓平,陈泽茂,等. 信息对抗理论与防御[M]. 武汉:武汉大学出版社,2008

[6] 张菊荣,周俊佑. 美国"舒特"机载战场网络攻击系统透视[R]. 西安:空军工程大学,2010

[7] 郭庆丰. 透过美国空军"舒特"计划探析战场网络战[J]. 空军装备研究,2010,4(2):58-61

[8] 秦立军. 信息安全保密系列谈[M]. 北京:金城出版社,2002

[9] 赵磊. 校园网纵深防御体系的研究与实现[D]. 北京:北京交通大学,2009

[10] 张世永. 网络安全原理与应用[M]. 北京:科学出版社,2003

[11] 李建. 美国海军计算机网络防御体系分析及启示[C]//知远战略与防务研究所,《网络战研讨会》论文集. 盐城,2010:50-67