

安全保护模型与等级保护 安全要求关系的研究

马力, 毕马宁, 任卫红

(公安部信息安全等级保护评估中心, 北京 100036)

摘要: 该文指出等级保护安全建设整改需要依据技术标准落实各项技术和管理措施, 建立信息系统安全防护体系将会借鉴各种流行的安全保护模型, 进而分析和说明了各种流行的安全保护模型与等级保护安全要求之间的关系, 给出了基于等级保护安全要求结合流行安全保护模型形成信息系统安全防护体系的思路。

关键字: 安全等级保护; 安全保护要求; 安全保护措施; 安全保护模型

中图分类号: TP393.08 **文献标识码:** A **文章编号:** 1671-1122 (2011) 06-0001-04

Research of the Relationship Between Popular Security Protection Model and Security Protection Requirements for Classified Protection of Information System Security

MA Li, BI Ma-ning, REN Wei-hong

(MPS Information Security Classified Protection Evaluation Center, Beijing 100036, china)

Abstract: Construction and correction of Security protection system in classified protection of information system security need to implement various technology and management measures according to technical standard, establishing security protection system of the information system will reference to various popular security protection model. This paper analyzed and explained the relations between various popular security protection model and security protection requirements for classified protection of information system security, given the thought of forming security protection system of information system based on the security protection requirements for classified protection and the popular security protection models.

Key words: information security classified protection; security protection requirements; security protection measures; security protection models

0 引言

随着信息安全等级保护工作的深入开展, 全国范围内重要信息系统定级工作已基本完成, 各地区、各部门工作的重点转到了已定级备案信息系统的安全建设整改工作上来。等级保护工作中的安全建设整改是按照国家出台的一系列有关等级保护标准规范, 从管理和技术两方面开展信息系统安全建设整改工作, 将技术和管理措施有机结合, 建立信息系统安全防护体系, 提高信息系统整体安全保护能力。

近些年来, 国家先后发布了《计算机信息安全保护等级划分准则》(GB 17859-1999)、《信息系统等级保护安全设计技术要求》(GB/T 25070-2010) 和《信息系统安全等级保护基本要求》(GB/T 22239-2008, 以下简称《基本要求》) 等有关信息安全等级保护方面的技术标准, 并要求按照上述技术标准落实各项技术和管理措施。信息系统的安全建设整改是一项涉及信息系统运行使用单位、安全服务商和产品提供商等的复杂系统工程, 安全建设整改的参与各方正确理解和使用等级保护的标准规范是有效开展等级保护安全建设整改工作的关键。

随着信息安全技术的发展, 信息安全行业流行着各种信息安全体系模型, 比如 OSI 安全体系结构、PDR 安全保护模型、IATF 信息保障技术框架和 WPDRRC 信息安全模型等, 如何正确理解等级保护标准规范中的安全要求(以下以《基本要求》为例说明)和

● 收稿时间: 2011-05-10

作者简介: 马力(1963-), 男, 江苏, 副研究员, 硕士, 主要研究方向: 信息安全、等级保护; 毕马宁(1960-), 男, 江苏, 副研究员, 硕士, 主要研究方向: 信息安全管理、信息安全等级保护; 任卫红(1963-), 河北, 副研究员, 硕士, 主要研究方向: 信息安全。

流行安全保护模型之间的关系,如何基于等级保护安全要求针对特定的信息系统量身定做合适的安全防护体系,是制定信息安全解决方案和开展等级保护安全建设整改的基础。

1 流行的安全保护模型

1.1 OSI安全体系结构

国际标准化组织(ISO)在对开放系统互联环境的安全性进行了深入研究后,提出了OSI安全体系结构(Open System Interconnection Reference Model),即《信息处理系统——开放系统互连——基本参考模型——第二部分:安全体系结构》(ISO 7498-2:1989),该标准被我国等同采用,即GB/T 9387.2-1995。该标准是基于OSI参考模型针对通信网络提出的安全体系架构模型。

该模型提出了安全服务、安全机制、安全管理和安全层次的概念。需要实现的5类安全服务,包括鉴别服务、访问控制、数据保密性、数据完整性和抗抵赖性,用来支持安全服务的8种安全机制,包括加密机制、数字签名、访问控制、数据完整性、数据交换、业务流填充、路由控制和公证,实施的安全管理分为系统安全管理、安全服务管理和安全机制管理,实现安全服务和安全机制的层面包括物理层、链路层、网络层、传输层、会话层、表示层和应用层。

1.2 PDR安全防护体系

早期,为了解决信息安全问题,技术上主要采取防护手段为主,比如采用数据加密防止数据被窃取,采用防火墙技术防止系统被侵入。随着信息安全技术的发展,又提出了新的安全防护思想,具有代表性的是ISS公司提出的PDR安全模型。该模型认为安全应从防护(protection)、检测(detection)、响应(reaction)三个方面考虑形成安全防护体系。

按照PDR模型的思想,一个完整的安全防护体系,不仅需要防护机制(比如防火墙、加密等),而且需要检测机制(比如入侵检测、漏洞扫描等),在发现问题时还需要及时做出响应。同时PDR模型是建立在基于时间的理论基础之上的,该理论的基本思想是认为信息安全相关的所有活动,无论是攻击行为、防护行为、检测行为还是响应行为,都要消耗时间,因而可以用时间尺度来衡量一个体系的能力。

假设被攻破保护的时间为 P_t ,检测到攻击的时间为 D_t ,响应并反击的时间为 R_t ,系统被暴露的时间为 E_t ,则系统安全状态的表示为 $E_t = D_t + R_t - P_t$,当 $E_t > 0$ 时,说明系统处于安全状态;当 $E_t < 0$ 时,说明系统已受到危害,处于不安全状态;当 $E_t = 0$ 时,说明系统安全处于临界状态。

PDR模型虽然考虑了防护、检测和响应三个要素,但在实际使用中依然存在不足,该模型总体来说还是局限于从技术上考虑信息安全问题,但是随着信息化的发展,人们越来越意识到信息安全涉及面非常广,除了技术外还应考虑人员、管理、制度和法律等方面要素。为此,安全行业的研究者们

对这一模型进行了补充和完善,先后提出了PPDR、PDRR、PPDRM、WPDRRC等改进模型。

1.3 IATF信息保障技术框架

与PDR模型一样被人们重视的另一个模型是IATF。信息保障技术框架(Information Assurance Technical Framework, IATF)是由美国国家安全局组织专家编写的一个全面描述信息安全保障体系的框架,它提出了信息保障时代信息安全需要考虑的要素。正是因为人们在信息安全工作中人们意识到,构建信息安全保障体系必须将技术、管理、策略、工程和运维等各个方面的要素紧密结合,安全保障体系才能真正完善和发挥作用,IATF成为一个流行的信息安全保障体系模型。

IATF首次提出了信息保障需要通过人(People)、技术(Technology)和操作(Operation)来共同实现组织职能和业务运作的思想,同时针对信息系统的构成特点,从外到内定义了四个主要的技术关注层次,包括网络基础设施、网络边界、计算环境和支撑基础设施,完整的信息保障体系在技术层面上应实现保护网络基础设施、保护网络边界、保护计算环境和保护支撑基础设施形成“深度防护战略(Defense-in-Depth Strategy)”。

1.4 WPDRRC信息安全模型

WPDRRC信息安全模型是我国“八六三”信息安全专家组提出的适合中国国情的信息系统安全保障体系建设模型,它在PDR模型的前后增加了预警和反击功能,它吸取了IATF需要通过人、技术和操作来共同实现组织职能和业务运作的思想。WPDRRC模型有6个环节和3大要素。6个环节包括预警(W)、保护(P)、检测(D)、响应(R)、恢复(R)和反击(C),它们具有较强的时序性和动态性,能够较好地反映出信息系统安全保障体系的预警能力、保护能力、检测能力、响应能力、恢复能力和反击能力。3大要素包括人员、策略和技术,人员是核心,策略是桥梁,技术是保证,落实在WPDRRC 6个环节的各个方面,将安全策略变为安全现实。

各类安全保护模型各有优缺点,OSI安全体系结构和PDR安全保护模型是早期提出的安全保护模型,其过于关注安全保护的技术要素,忽略了重要的管理要素,存在一定的局限性。IATF信息保障技术框架和WPDRRC信息安全模型融入了人员、技术和管理要素,并且分别从信息系统的构成角度和安全防护的层次角度提出了安全防护体系的构成思想,因此,成为最为流行的安全保护模型被广泛应用。

2 等级保护安全要求与流行保护模型的关系

2.1 等级保护的技术要求和管理要求

《基本要求》提出的等级保护安全要求由安全层面、技术要求和和管理要求三个要素构成。安全层面对应等级保护安全要求的实施层次,技术要求和和管理要求对应等级保护技术类要求和和管理类要求两个方面。技术类安全要求通常与信息系统提供的各类技术安全机制有关,主要是通过信息系统

部署软硬件并正确的配置其安全功能来实现；管理类安全要求通常与信息系统中各种人员参与的活动有关，主要是通过控制各种人员的活动，从政策、制度、规范、流程以及记录等方面做出规定来实现。

《基本要求》提出的安全要求与其它技术标准提出的安全要求有所不同，其从物理、网络、系统、应用、数据和管理等几个层面针对不同级别的信息系统提出了不同的要求，无论信息系统的级别如何，该标准认为信息系统的安全技术体系架构应包含物理、网络、系统、应用和数据等几个层面。技术要求与安全层面存在一定的对应关系，某些安全要求只适用于特定的安全层面，例如防雷、防火等针对物理层面的安全，边界防护、区域划分等针对网络层面的安全。而某些安全要求可以在多个层面实现，例如身份鉴别、访问控制等，可以分别针对网络层面、主机层面和应用层面的安全。等级保护安全技术体系架构如图1所示。

虽然安全管理要求与安全层面也存在一定的对应关系，比如设备管理、介质管理等主要适用于物理层面的安全，网络配置管理、网络漏洞扫描等适用于网络层面的安全，但是为了方便使用和理解，等级保护安全管理要求采用了三个要素、二个过程的组织方式提出。要素分为安全管理机构、安全管理制度、人员安全管理三个实施安全管理的要件，过程上强调对系统建设过程和系统运维过程的管理和控制。

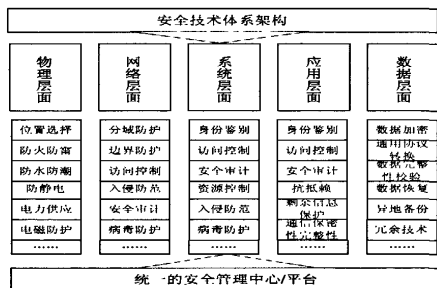


图1 安全技术体系架构

2.2 安全要求和保护模型的关系

等级保护安全要求的组织形式借鉴了OSI安全体系结构中安全机制、安全服务和安全层次的分类思想和要素关系，即不同安全层次实现相应的安全机制以提供不同的安全服务。等级保护安全要求的安全层次根据信息系统的构成特点扩展为物理层、网络层、系统层、应用层和数据层，鉴于信息系统中不同层面提供的安全服务主要是通过向信息系统中部署具有相关安全功能或安全机制的软硬件产品来实现的特点，等级保护安全要求中没有采用安全服务的概念，而是采用物理层、网络层、系统层、应用层和数据层应该实现的“安全控制”来表征。

“安全控制”的实现可能需要在信息系统中部署具有相关安全功能或安全机制的软硬件产品来实现，或通过人员的一定管理手段来实现（如通过对软硬件产品的参数配置），上述

内容称为“安全要求”。安全层次、安全控制和安全要求的关系如图2所示。等级保护安全要求的核心思想是通过在不同层面实施不同强度的安全控制，来保障信息系统具有相应的安全保护能力，安全控制主要通过向信息系统中部署或采取满足等级保护安全要求的措施来实现。

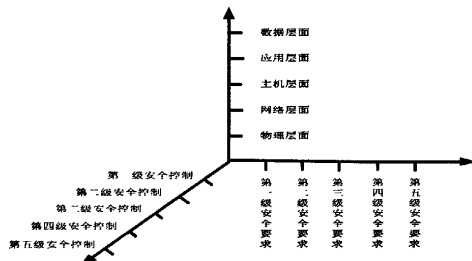


图2 安全层次、安全控制和安全要求之间关系

目前流行的几种安全保护模型，无论是IATF信息保障技术框架还是WPDRRC信息安全模型均强调了在技术基础上“人”的作用。如前所述，IATF强调了需要通过人、技术和操作来共同实现组织职能和业务运作的思想，WPDRRC强调了人员是核心、策略是桥梁、技术是保证的思想，等级保护安全要求没有用图示模型表述人员、策略、制度、管理或操作所起到的作用和相互关系，但是在安全管理要求中强调了这些内容。

在等级保护安全管理要求中，明确了人员、策略、操作等要素所起到的作用和控制要求，信息系统的保护除安全技术体系框架外（见图1），还需要控制信息系统中各种人员参与的活动，包括对安全活动进行管理的机构和人员、对安全活动进行控制的策略、制度和规程，对信息系统建设过程和运维过程进行安全管理的安全要求等。

等级保护安全要求在技术上进一步细分为物理安全、网络安全、系统安全、应用安全和数据安全五个层面，从层次与IATF模型的网络基础设施、网络边界、计算环境和支撑基础设施的划分存在一定差异，但是上述分类是看待信息系统的视角不同，等级保护安全技术要求中的网络安全对应着网络基础设施和网络边界的保护，系统安全、应用安全和数据安全对应着计算环境的保护。整个关系示意图如图2所示。

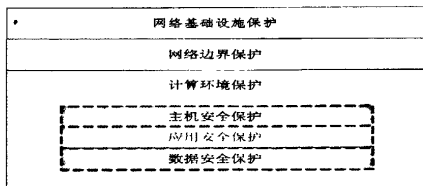


图3 等级保护安全层面与IATF模型要素的关系

有关网络基础设施和网络边界保护的安全要求，包括通信线路的安全、网络边界的安全、网络区域的划分、区域边界的安全和网络设备的安全等均在网络安全中提出，有关计算环境保护的安全要求，包括服务器安全、终端安全、应用系

统安全和计算环境中的数据安全在系统安全、应用安全和数据安全中分别提出，有关支撑基础设施的相关要求在安全管理中心或平台中提出。

信息安全等级保护的主要思想是“突出重点、保护重点”。信息系统的级别不同意味着信息系统的重要程度不同，国家对不同级别的信息系统有不同的安全保护能力要求，如第三级信息系统应能在统一的安全保护策略下具有抵御大规模、较强恶意攻击的能力，抵抗较为严重的自然灾害的能力，防范计算机病毒和恶意代码危害的能力；具有检测、发现、报警、记录入侵行为的能力；具有对安全事件进行响应处置，并能够追踪安全责任的能力；在系统遭到损害后，具有能够较快恢复正常运行状态的能力；对于服务保障性要求高的系统，应能快速恢复正常运行状态；具有对系统资源、用户、安全机制等进行集中控管的能力。

不同级别的信息系统具备不同的安全保护能力，意味着不同级别的信息系统并不需要全部实现 WPDRRC 模型中的预警能力、保护能力、检测能力、响应能力、恢复能力和反击能力，只有较高级别的系统应该能够应对更多的威胁，考虑更为周密的应对措施，实现 WPDRRC 模型提出的预警能力、保护能力、监测能力、响应能力、恢复能力和反击能力的大部分内容。不同级别的信息系统的安全要求与 WPDRRC 模型的关系如表 1 所示。

系统级别	实现 WPDRRC 模型要素					
	预警 (W)	保护 (P)	监测 (D)	响应 (R)	恢复 (R)	反击 (C)
第一级	---	Y	---	---	---	---
第二级	---	Y	Y	---	---	---
第三级	---	Y	Y	Y	Y	---
第四级	Y	Y	Y	Y	Y	---
第五级	不详	不详	不详	不详	不详	不详

2.3 安全要求和保护模型结合使用的一种方法

信息系统可以从不同的视角去观察，典型的信息系统从外

到内分析可以认为是由通信网络、交换网络和各个网络区域构成，每个网络区域内部可能有各类主机、应用和数据；从下到上分析可以认为信息系统是由物理、网络、主机、应用和数据几个逻辑层面构成。

对信息系统的安全保护可以首先采用 IATF 的思想，通过合理区分通信网络、交换网络和各个网络区域，形成网络基础设施保护、网络（区域）边界保护、计算环境（区域内部）保护的 IATF 总体构思，然后将等级保护安全要求中网络层面的要求落实到网络基础设施、网络（区域）边界保护处，主机、应用和数据层面的安全要求落实到计算环境（区域内部）的保护处。即先从网络架构上考虑从外到内的保护，再从内部层次上考虑从下到上的保护，形成纵深防御战略。

最后，由于不同级别的信息系统对预警能力、保护能力、监测能力、响应能力、恢复能力和反击能力的要求是不一样的，在形成通信网络保护、网络边界保护和计算环境保护的纵深防御战略过程中，应对比不同级别的信息系统对预警能力、保护能力、监测能力、响应能力、恢复能力和反击能力的要求，从外到内、从各个层次实现相关能力的安全机制和措施，避免缺失某类安全机制和措施。

3 结束语

在等级保护安全建设整改工作中，对信息系统安全保护可以充分利用 IATF 信息保障技术框架和 WPDRRC 信息安全模型的思想，考虑人员、技术和管理三个重要要素，分别从网络基础设施、网络边界和计算环境，从物理、网络、主机、应用和数据几个层面，根据信息系统的级别，有区别地实现预警、保护、检测、响应、恢复和反击等有关的安全机制和措施。●（责编 岳道远）

国家广电总局《广播电视相关信息系统安全等级保护定级指南》通过专家评审

2011 年 4 月 19 日，国家广电总局科技司在北京组织召开了《广播电视相关信息系统安全等级保护定级指南》行业暂行技术文件审定会。国家广电总局科技司、公安部网络安全保卫局、公安部信息安全等级保护评估中心、证监会信息中心、中央人民广播电台、中央电视台、中国国际广播电台、国家广电总局无线局、国家广播电视安全播出调度中心、广播电视规划院、中国有线电视网络公司、北京歌华有线电视网络公司等单位的专家参加了评审会。参加评审的各位专家听取了起草小组关于行业暂行技术文件编制情况的介绍，经认真讨论，提出了修改意见。与会专家一致认为，该暂行技术文件起草小组结合国家信息安全相关政策，分析研究了我国广电行业制作、播出、传输、覆盖等生产业务相关信息系统受到破坏时侵害的客体以及对客体的侵害程度，提出了适用于广播电视相关信息系统安全等级保护定级方法，并提出了相应的定级建议。定级方法科学、定级建议合理。该文件的制定，对推动我国广电行业信息安全等级保护工作、提高全行业信息安全水平，提升安全播出保障能力具有重要意义。与会专家建议尽快推广试用，并逐步完善。审定会一致同意通过对该暂行技术文件的审定。（记者 程斌）

浙江省、陕西省、宁夏自治区、江西省推动国有企业信息安全等级保护工作

近期，浙江省、陕西省、宁夏自治区、江西省为进一步加强本地国有企业的信息安全工作，保障和促进企业的信息化发展，根据公安部、国务院国有资产监督管理委员会《关于进一步推进中央企业信息安全等级保护工作的通知》（公通字[2010]70 号）精神，省（区）公安厅会同省（区）人民政府国有资产监督管理委员会联合下发了《关于加快推进我省国有企业信息安全等级保护工作的通知》。通知要求，全省（区）各级公安机关和国资监管机构要高度重视国有企业信息安全等级保护工作，各国有企业要将这项工作摆在重要位置，切实将等级保护工作纳入企业的信息化工作中，同步规划、同步实施、同步考核。为确保此项工作的顺利开展，公安机关、国资监管机构和国有企业进一步明确了职责分工，并在省级层面建立由省公安厅和省国资委共同参加的国有企业信息安全等级保护工作协调配合机制，各市也建立相应的工作机制。两部门加强协调配合，定期沟通和通报情况，联合开展监督检查，共同组织推动国有企业的等级保护工作。（记者 程斌）