

网络安全技术基础

周海刚 主编

邱正伦 石爱军 扶树刚 副主编

清华大学出版社

北京交通大学出版社

·北京·

内 容 提 要

网络信息系统将成为 21 世纪人类社会运转的基础, 网络信息安全将是信息社会正常运转的保证。本书在内容安排上首先介绍了信息安全和网络安全的基本概念和 3 层 4 域安全模型, 然后详细地论述网络信息安全的核心理论——密码技术及其应用。根据 3 层 4 域模型, 本书对网络防护的“保护”、“检测”、“响应”、“恢复”等几个方面进行了详细的论述, 包括服务器的安全管理、路由器和防火墙技术、数据库安全、入侵检测、应急响应和系统恢复以及网络安全增强的技术。最后, 从较为宏观的角度讨论信息保障和信息战, 这是网络安全发展的最新阶段。本书可以作为网络安全专业、计算机专业、信息工程专业或相近专业的大专、本科和研究生的教科书, 也可以作为从事网络安全领域的科技人员与信息系统安全管理员的参考书。

版权所有, 翻印必究。

本书封面贴有清华大学出版社激光防伪标签, 无标签者不得销售。

图书在版编目 (CIP) 数据

网络安全技术基础 王海刚主编 北京: 清华大学出版社; 北京交通大学出版社, 2005.12

ISBN 7-302-12400-3

(21 世纪高等学校电子信息类专业规划教材)

Ⅰ. 网... Ⅱ. 海... Ⅲ. 网... Ⅳ. 网...

I 援网... II 援周... III 援计算机网络安全技术 高等学校 教材 IV 援裁 474.4

中国版本图书馆 CIP 数据核字 (2005) 第 12400 号

责任编辑: 陈文诤

出版者: 清华大学出版社 邮编: 100084 电话: (010) 62770175

北京交通大学出版社 邮编: 100044 电话: (010) 62223000, 62226000

印刷者: 北京鑫海金澳胶印有限公司

发行者: 新华书店总店北京发行所

开本: 185mm×260mm 印张: 15.5 字数: 380千字

版次: 2005 年 12 月第 1 版 2005 年 12 月第 1 次印刷

书号: 7-302-12400-3

印数: 1-5000册 定价: 29.00 元

前 言

近年来，网络世界中发生的网络攻击事件越来越频繁，网络黑客的手段越来越高级，世界各国在网络攻击事件中的损失也越来越严重。为此，世界各国都投入了大量的资金和人员进行网络攻击和网络防护技术的研究。世界各国在积极开展网络攻击和防护技术研究的同时，网络黑客们也在不停地制造着网络入侵事件。1988年10月2日这一天被称为“黑色的星期四”，一个美国年轻人把一个“蠕虫”程序放到了网络上，导致了上千台网上机器瘫痪。这个称为“蠕虫”程序的出现改变了许多人对网络安全性的看法，引起人们对计算机网络安全问题的重视。20世纪90年代以来，网络安全走向商业化，上网计算机数量急剧增加，网络“黑客”与“入侵者”的非法活动呈猖獗趋势。人们发现网络安全问题无法仅用数据加密技术完全加以解决，还需要解决硬件系统、操作系统、网络、数据库系统和应用系统的整体安全问题，信息安全问题也就进入了网络信息安全阶段。进入21世纪后，各国对信息安全的重要性与作用有更高地认识，美国首先提出了信息保障的概念，提出了防护、检测、反应与恢复（PDRC）模型，使信息安全进入主动防御阶段。

最近几年来的网络攻击手段也开始从单一型向综合性转变：1999年10月发生的攻击再根、汉城、悦春等站点的分布式拒绝服务攻击就采用了缓冲区溢出、特洛伊木马、口令攻击及一般拒绝服务的综合性攻击；2001年出现的对整个网络世界造成恐慌的“红色代码”及其变种“红色代码II”网络病毒，以及2002年出现的“冲击波”和“震荡波”病毒则综合了蠕虫病毒、特洛伊木马和缓冲区溢出等攻击手段。网络攻击的方式和方法也经历了从早期的粗糙、单一的攻击方法发展到今天的精致、综合的攻击方法的过程。早期的攻击方法以口令破解、洪泛式拒绝服务和特洛伊木马为主；20世纪90年代开始兴起缓冲区溢出、网络信息探测和网络漏洞扫描攻击；近几年出现了综合各种网络攻击手段的网络欺骗攻击和分布式拒绝服务攻击。

面对网络攻击事件的频频发生和网络攻击手段的日益强大，我们需要了解网络攻击的方式和方法，更有必要对网络防护所涉及的网络安全技术进行深入研究，这样我们才能在当前这个不安全的网络中保护自己。

本书出版的目的是用作网络安全专业或相近专业的教材，通过对本课程的学习，将让学生全面了解网络安全的知识和网络空间中进行信息对抗的技术与知识。在内容选择上既考虑实时性（安全领域中的最新发展），也考虑系统性与理论性，同时还注重了实用性。

本书重点是讨论计算机网络中的信息安全问题与实现信息安全的措施。为了让读者了解各种安全威胁的严重性及各种安全防护措施的作用，也介绍了一些网络黑客与入侵者常用的网络攻击手段。了解这些攻击手段是为了更好进行防御。当然，一些好奇者可能会仿效黑客的某些手法去尝试网络攻击，我们劝说这些人应该学习法律，在未经许可的情况下这样做是违法的。对于那些别有用心的人来说，他们这样做总有一天会受到法律制裁。我

们编写本书的目的是提高读者的安全知识和安全管理的技术，管理好自己所在单位的网络信息系统，防止各种有意与无意的安全威胁，保证信息系统安全可靠的运行。

本书的内容安排如下。第 1 章介绍网络和信息安全以及网络安全模型的基本概念。第 2 章介绍密码技术及其应用。第 3 章主要讨论网络安全问题，包括网络安全机制、网络攻击手段、网络服务的安全问题、网络设备和网络的安全问题和安全机制。第 4 章以 UNIX 操作系统和 Windows 操作系统为对象介绍了服务器和网络设备的安全管理。第 5 章介绍路由器和防火墙的防护原理，还包括网络路由器的安全配置。第 6 章首先讨论数据库的一般安全问题，然后以 Oracle 数据库和 Microsoft SQL Server 为目标介绍数据库的安全管理。第 7 章介绍网络安全防护中重要的技术——入侵检测技术。第 8 章为应急响应与系统恢复，讨论在遭受到网络攻击后如何应对。第 9 章介绍其他的一些网络安全增强技术，如入侵检测、灾难恢复和信息隐藏等。第 10 章介绍信息保障的概念，并讨论信息战这个热点问题。

全书由周海刚主编，邱正伦、石爱军、扶树刚任副主编并参加了部分内容的编写和资料搜集工作，花春春女士也为本书的录入、校正和图表制作付出了辛勤的劳动，在此一并表示感谢！

本书可作为电子信息类专业高年级本科或研究生的教材，也可作为相关研究领域技术人员的参考资料。由于网络安全技术是一个新兴的研究领域，许多技术还处于完善与发展中，加上编写时间短，书中难免存在错误，非常欢迎广大读者和专家提出批评改进意见。

联系地址：北京岳各庄路

编者
2008年 8月

目 录

第 1 章 概述.....	员
1.1 信息安全与信息对抗	员
1.1.1 信息的安全需求	员
1.1.2 信息对抗的阶段性和特点	圆
1.2 信息安全概念与技术的发展	圆
1.2.1 单机系统的信息保密阶段	猿
1.2.2 网络信息安全阶段	猿
1.2.3 信息保障阶段	源
1.3 可信安全模型	远
习题 1	苑
第 2 章 密码技术.....	愿
2.1 密码技术简介	愿
2.1.1 密码学基本概念	愿
2.1.2 对称密钥密码系统	苑
2.1.3 公钥密码系统	苑
2.1.4 散列函数	愿
2.2 密码技术的应用	愿
2.2.1 数据加密	愿
2.2.2 鉴别协议	园
2.2.3 消息完整性协议	园
2.3 公开密钥分发	园
习题 2	园
第 3 章 网络安全问题	园
3.1 网络安全框架	园
3.2 网络安全机制	园
3.3 网络攻击原理与步骤	猿
3.3.1 网络攻击	猿
3.3.2 利用漏洞进行攻击	猿
3.3.3 网络攻击的一般过程	猿

源源 其他安全措施	源
源源 粤群集的安全管理	源
源源 粤群集中的模块	源
源源 根据客户来源进行限制	源
源源 根据用户标志进行限制	源
源源 计算机病毒攻击	源
源源 网络病毒特点	源
源源 常见网络病毒	源
源源 网络防毒措施	源
习题 源	源
第 缘章 路由器与防火墙	源
缘源 路由器的包过滤功能	源
缘源 包过滤路由器的操作方式与过滤规则	源
缘源 包过滤路由器的特点	源
缘源 应用协议的包过滤	源
缘源 路由器访问表原理与配置	源
缘源 扩展访问表基础	源
缘源 标准访问表举例	源
缘源 扩展访问表举例	源
缘源 安全路由器原理	源
缘源 安全路由器的设计原则	源
缘源 双协议栈结构	源
缘源 系统结构	源
缘源 构建 缘缘	源
缘源 防火墙系统的安全原理	源
缘源 防火墙的基本概念	源
缘源 防火墙的逻辑构造与安全策略	源
缘源 防火墙的安全技术	源
缘源 防火墙系统	源
缘源 网络层防火墙	源
缘源 应用层防火墙	源
缘源 基于 缘缘的防火墙	源
缘源 术语	源
缘源 工作原理	源
缘源 功能实现	源

习题 缘	缘
第 远章 数据库安全技术	缘
远 数据库的安全问题	缘
远 数据库特点概述	缘
远 数据库的安全威胁	缘
远 数据库的安全要求	缘
远 数据库的安全措施	园
远 数据库安全与数据库安全管理	缘
远 数据库安全概述	缘
远 验证方法	缘
远 数据库安全 : 登录	苑
远 数据库安全 : 用户	苑
远 数据库安全 : 角色	愿
远 管理 数据库登录	园
远 管理 数据库用户	园
远 管理 数据库角色	核
远 管理 数据库权限	缘
远 使用加密	苑
远 数据库安全管理	苑
远 用户管理	苑
远 权限和角色	员
远 资源限制	苑
远 数据审计	愿
远 标签安全	怨
习题 远	猿
第 苑章 入侵检测技术	源
苑 限的基本概念	源
苑 限检测的活动	缘
苑 入侵检测方法	远
苑 基本方法	远
苑 异常入侵检测方法	苑
苑 误用入侵检测方法	园
苑 其他检测方法	源
苑 入侵监测系统的设计	缘
苑 基于主机的 限系统	缘

苑题源	基于局域网的 混杂	苑题苑
苑题苑	分布式 混杂	苑题苑
习题 苑	苑题苑
第 愿章	应急响应与系统恢复	苑题苑
愿题	应急响应	苑题苑
愿题苑	概述	苑题苑
愿题苑	应急响应方法学	苑题苑
愿题苑	应急响应组	苑题苑
愿题苑	应急响应设计的关键技术	苑题苑
愿题苑	应急响应的发展方向	苑题苑
愿题	系统恢复	苑题苑
习题 愿	苑题苑
第 怨章	网络安全的增强技术	苑题苑
怨题	运奥系统	苑题苑
怨题苑	运奥系统的认证协议	苑题苑
怨题苑	运奥系统的密钥交换协议	苑题苑
怨题苑	运奥系统的不足	苑题苑
怨题	杂编安全协议	苑题苑
怨题苑	杂编简介	苑题苑
怨题苑	杂编协议的状态与状态变量	苑题苑
怨题苑	杂编握手协议	苑题苑
怨题苑	杂编记录协议	苑题苑
怨题苑	杂编使用的安全机制以及提供的安全服务	苑题苑
怨题	障灾	苑题苑
怨题	虚拟专用网	苑题苑
怨题苑	灾罩简介	苑题苑
怨题苑	灾罩的分类	苑题苑
怨题苑	隧道技术	苑题苑
怨题苑	国外主要厂商的 灾罩解决方案	苑题苑
怨题	网络多级安全技术	苑题苑
怨题苑	可信网络基	苑题苑
怨题苑	安全通信服务器	苑题苑
怨题苑	多级安全信道	苑题苑
怨题	信息隐藏技术	苑题苑
怨题苑	信息隐藏技术的分类	苑题苑

怨	隐写术及其通信模型	
怨	数字水印及其安全性分析	
	习题	
第 章	信息保障与信息战	
	信息保障	
	定义	
	信息保障技术框架	
	世纪的信息战争与信息安全	
	定义	
	网络信息战的主要手段	
	关于信息战的思考	
	安全防御体系	
	网络空间信息战	
	网络空间的构成与对抗模型	
	网络信息战的阶段与对抗样式	
	可用的网络信息战手段探讨	
	用于网络信息战的武器系列	
	习题	
附录 粤	计算机信息网络国际联网安全保护管理办法	
附录 月	中华人民共和国计算机信息系统安全保护条例	
参考文献	

第 1 章 概 述

人类已经进入信息化社会，随着网络在全世界日益普及，政府、军队、企业等部门越来越需要利用网络传输与管理信息。虽然计算机与网络技术为信息的获取、传输与处理利用提供了越来越先进的手段，但也为入侵者提供了方便之门，使得计算机与网络中的信息变得越来越不安全。由于网络“黑客”与“入侵者”的活动越来越频繁，人们对计算机与网络中信息的安全越来越担心。不仅金融、商业、政府部门担心，军事部门更为担心。信息技术发展到今天，迫切要求发展各种信息安全技术。怎样才能使计算机与网络中的信息更安全，必须研究网络与计算机本身的安全机制和措施，研究“黑客”与“入侵者”的攻击方法和对他们的防范措施，这也是编写本书的主要宗旨。

1.1 信息安全与信息对抗

在本书中，“信息”是一个广泛的概念，不仅包括计算机文件系统或数据库系统中存储的各种数据、正文、图形、图像、声音等形式的多媒体数据文件、软件或各种文档资料，也包括存放或管理这些信息的硬件信息，如计算机硬件及其网络地址、网络结构、网络服务等都属于本书中所涉及的“信息”。尽管在许多文献中都大量引用“数据”与“信息”两个术语，但却没有一个被公认的对数据和信息的定义。本书将不对信息与数据加以区分，信息安全与数据安全是指同一个概念。在字典中，“安全”一词是指“远离危险、威胁的状态或特性”和“为防范间谍活动或蓄意破坏、犯罪、攻击等而采取的措施。”信息安全则是指防止任何对数据进行未授权访问的措施，或者防止造成信息有意无意泄露、破坏、丢失等问题的发生，让数据处于远离危险、免于威胁的状态或特性。而网络安全则是指计算机网络环境下的信息安全。

“信息对抗”也是一个概念广泛的术语，其主要含义是指争斗的双方利用各种手段获取信息的控制权，进而使己方在争斗过程中处于主动地位。信息对抗的主要表现形式有：敌对双方或利益竞争的双方通过电视广播进行宣传战；对立的双方互相进行心理战；通过侦察、间谍等手段窃取对方的信息；双方通过计算机网络进行信息的对抗等等。信息战是信息对抗的另一种称呼，只不过军事气息更浓一些。在本书中对“信息战”和“信息对抗”这两个术语也将不做区分，而且只讨论争斗的双方通过计算机网络进行的信息对抗。

1.2 信息的安全需求

计算机系统的安全需求主要用三方面表征：保密性、完整性和可用性。

保密性表示对信息资源开放范围的控制，不让不应涉密的人涉及秘密信息。实现保密性的方法一般是通过信息的加密、对信息划分密级，并为访问者分配访问权限，系统根据用户的身份权限控制对不同密级信息的访问。除了考虑数据加密、访问控制外，还要考虑计算机电磁泄露可能造成的信息泄露。

完整性是指保证计算机系统中的信息处于“保持完整或一种未受损的状态”。任何对系统信息应有特性或状态的中断、窃取、篡改、伪造都是破坏系统信息完整性的行为。其中中断是指在某一段时间内因系统的软、硬件的故障或恶意的破坏、删除造成系统信息的受损、丢失或不可利用；窃取是指系统的信息被未经授权的访问者非法获取，造成信息不应有的泄露，使得信息的价值受到损失或者失去了存在的意义；篡改是指故意更改正确的数据，破坏了数据的真实性状态；伪造是指恶意的未经授权者故意在系统信息中添加假信息，造成真假信息难辨，破坏了信息的可信性。

可用性是指合法用户在需要的时候，可以正确使用所需的信息而不遭服务拒绝。系统为了控制非法访问可以采取许多安全措施，但系统不应该阻止合法用户对系统中信息的利用。信息的可用性与保密性之间存在一定的矛盾。

1.4.4 信息对抗的阶段性

信息生命期是指信息从产生到消亡的整个过程，可以划分为信息获取、信息传输、信息储存、决策处理、信息作用、信息废弃等若干个阶段。任何主体要想达到某种目的，比如某公司希望到某国开拓市场，那么首先应该派人到该国了解市场的需求信息，这叫信息获取；这些信息通过无线与有线信道传输到国内公司的计算机系统中存储到数据库中，这里经历了信息传输和信息存储两个阶段，当然在数据库中还存放着该公司的生产能力、销售网络、成本核算等信息。为了决策是否到国外开拓市场，需要利用决策软件对信息进行处理和做出相应的决策。信息作用则是把决策信息返回给前端的执行机构，由执行机构实现决策的意图。信息一般都具有时效性，过了某个时效后，信息也就失去了作用，失去效用的信息应该及时废弃。信息的时效可以根据需要决定，为了留作历史资料，需要对一些信息做长时间的存储保留。

利益冲突的双方进行的信息对抗遍布信息生命期的每个阶段，而且在不同的阶段采取不同的对抗形式。在信息获取阶段，对抗的一方需要获取对方真实完整的信息，而另一方则可以通过各种手段，如伪装、欺骗的方法使对方不能获取所需要的信息。在信息传输阶段，对抗的一方要设法让信息正确传输到目的地，而另一方则通过截获、弄假、干扰等手段妨碍信息的正确传输。在信息的存储阶段，对抗的双方围绕信息的完整性和保密性展开争斗。决策处理阶段的信息对抗体现为双方信息处理与决策支持系统之间的对抗。在信息作用阶段的信息对抗则体现为对双方信息执行机构控制权的争夺。网络黑客对信息的攻击一般都集中在信息的传输、存储和决策处理三个阶段中。针对不同阶段中信息所处的不同状态，研究不同的对抗手段更为有效。

1.5 信息安全概念与技术的发展

随着人类对信息的依赖程度越来越大，人们对信息的安全性越来越关注。随着应用与研究的深入，信息安全的概念与技术不断得到创新。早期在计算机网络广泛使用之前主要是开发各种信息保密技术，在 20 世纪 70 年代中期在全世界范围商业化应用之后，信息安全进入网络信息安全阶段。近几年又发展出了“信息保障（Information Assurance）”的新概念。本文以下部分将介绍信息安全的各个发展阶段的主要内涵与所开发的新概念与新技术。

点，还应标明支持用户完成使命所需的信息处理类型（交互通信、广播通信、信息存储、一般访问、受限访问等）。

(猿 要求：描述任务、行动及完成系统需求的活动等。

猿援系统的设计

(员 功能分配；

(圆 概要设计；

(猿 详细设计。

猿援系统的实现

(员 通过各种手段获取一切必要的资源，包括通过采办手段；

(圆 按照需求构建系统；

(猿 系统测试；

(源 评估性能。

猿援系统云过程

猿援作为上述系统工程过程的一个子过程，其重点是针对信息保护方面的需求，从理论上讲它是与上述系统工程平行出现的，分布在各个阶段。猿援的活动包括：

(员 描述信息保护的需求；

(圆 基于前述系统工程过程，形成信息安全方面的要求（安全要适度）。

(猿 根据这些要求构建功能性的信息安全体系结构；

(源 把信息保护功能分配给物理体系结构及逻辑体系结构；

(缘 在系统设计中实现信息保护体系结构；

(远 实现适度安全，在费用、进度及运作合适度与有效度的总体范围内平衡信息保护风险管理及猿援的其他方面的考虑。

(苑 参与和其他信息保护及系统工程条令有关平衡、折中的研究，以及使命、威胁、政策对信息保护要求的影响。

猿援系统猿援 信息安全的鲁棒性反制措施的强度

反制措施是一种防御网络攻击的专门技术、产品或程序。在有效的安全总体解决方案中，不管技术的还是非技术的反制措施都是非常重要的。但制定合适的技术反制措施需要遵循一些原则，其中包括对各种威胁、重要安全服务的鲁棒性（鲁棒性策略、互操作性框架、运行鲁棒性的评估。

敌对方信息攻击的目的可以归纳为三大类：非法访问、非法修改和阻止提供合法服务。安全总体解决方案就是为了不让敌方达到他们的目的。己方网络需要提供的五种基本安全服务是访问控制、保密性、完整性、可用性及不可否认性。这些安全服务需要利用以下安全机制完成：加密、鉴别或识别（鉴别和鉴别）、认证、访问控制、安全管理及可信赖技术，这些机制综合到一起可以构成防止攻击的壁垒。

鲁棒性策略针对某种信息价值和可能遭到的威胁水平，提供一种在确定信息安全机制强度的指导思想。这种策略还定义了对技术性反制措施的测量及评估其鲁棒性不同等级的策略。在鲁棒性策略中把信息的价值分为 缘级（灾员~灾缘，其价值依次递升；威胁分为 苑级（劫员~劫苑，其大小也依次递升。表 员缘根据待保护信息的价值及威胁程度，给出了对应安全强度的安全机制。

表 员圆 鲁棒性的等级分类表

信息价值	威胁程度						
	栽员	栽圆	栽猿	栽源	栽缘	栽远	栽苑
灾员	灾员栽员 灾员栽圆	灾员栽圆 灾员栽猿	灾员栽猿 灾员栽源	灾员栽源 灾员栽缘	灾员栽缘 灾员栽远	灾员栽远 灾员栽苑	灾员栽苑 灾员栽愿
灾圆	灾圆栽员 灾圆栽圆	灾圆栽圆 灾圆栽猿	灾圆栽猿 灾圆栽源	灾圆栽源 灾圆栽缘	灾圆栽缘 灾圆栽远	灾圆栽远 灾圆栽苑	灾圆栽苑 灾圆栽愿
灾猿	灾猿栽员 灾猿栽圆	灾猿栽圆 灾猿栽猿	灾猿栽猿 灾猿栽源	灾猿栽源 灾猿栽缘	灾猿栽缘 灾猿栽远	灾猿栽远 灾猿栽苑	灾猿栽苑 灾猿栽愿
灾源	灾源栽员 灾源栽圆	灾源栽圆 灾源栽猿	灾源栽猿 灾源栽源	灾源栽源 灾源栽缘	灾源栽缘 灾源栽远	灾源栽远 灾源栽苑	灾源栽苑 灾源栽愿
灾缘	灾缘栽员 灾缘栽圆	灾缘栽圆 灾缘栽猿	灾缘栽猿 灾缘栽源	灾缘栽源 灾缘栽缘	灾缘栽缘 灾缘栽远	灾缘栽远 灾缘栽苑	灾缘栽苑 灾缘栽愿

表中：灾员-灾苑——机制强度的等级；栽员-栽愿——保障评估的等级；

灾员栽员——基本强度，抗非复杂威胁（栽员-栽圆级）用以保护低价值数据；

灾圆栽圆——中等强度，抗复杂威胁（栽圆-栽猿级）用以保护中等价值数据；

灾猿栽猿——高等强度，抗国家级威胁（栽猿-栽源级）用以保护高等价值数据。

美国社会高度依赖信息，投入巨额经费研究信息安全的新技术，发展出许多信息安全的新概念。本文介绍的“信息保障”概念，就是由美国国防部提出的。随着我国现代化建设的进展，我国党、政、军、企各部门对信息的依赖程度越来越高，各单位领导对信息安全问题也越来越重视。美国对信息安全的新理论，如信息保障技术框架，是值得我国参与借鉴的。我们应该研究这些新概念与新理论，并结合我国自己的情况，提出符合我国国情的信息保障技术框架，作为指导我国各部门信息安全建设的参考。

员圆 孕砸砸安全模型

孕砸砸安全模型是从经典的孕砸砸模型基础上演变而来的，随同信息保障概念一起为大家所接收和重视。孕砸砸安全模型强调网络防护不再是单纯被动式的防护，而是保护（孕砸砸）、检测（孕砸砸）、响应（孕砸砸）、恢复（孕砸砸）的有机结合，如图 员圆 所示。因此 孕砸砸模型不仅包含安全防护的概念，更重要地是增加主动的和积极的防御观念。

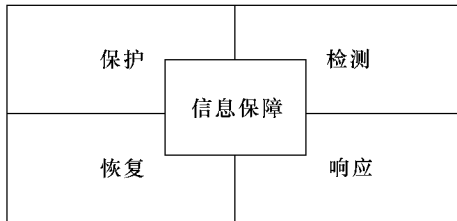


图 员圆 孕砸砸模型

员圆 员 保护

保护就是采用一切的手段保护我们信息系统的可用性、机密性、完整性、可控性和不

可否认性。这里的手段一般指静态的防护手段，包括：防火墙、防病毒、虚拟专用网(VPN)、路由器等。

入侵检测

在网络安全模型中，检测是非常重要的一个环节。检测的目的是发现网络攻击，检测本地网络存在的非法信息流，以及检测本地网络存在的安全漏洞，从而有效地阻止网络攻击。检测部分典型的技术有入侵检测技术和网络安全扫描技术等。

应急响应

响应就是对危及网络安全的事件和行为做出反应，阻止对信息系统的进一步破坏并使损失降到最低。这就要求在检测到网络攻击后及时地阻断网络攻击，或者将网络攻击引诱到其他的主机上去，使网络攻击不能对信息系统造成进一步的破坏。另外，还需要定位网络攻击源，并进行网络攻击取证，为诉诸法律和网络反击做准备。阻断网络攻击主要是和其他的技术配合，比如检测到网络攻击后，利用防火墙等系统来阻断网络攻击。

系统恢复

及时地恢复系统，使系统能尽快正常地对外提供服务，是降低网络攻击造成损失的有效途径。为了保证受到攻击后能够及时成功地恢复系统，必须在平时做好备份工作。这包括对信息系统所存储的有用数据进行备份恢复工作，还包括对信息系统本身进行备份恢复工作。备份技术有三种：现场内备份、现场外备份和冷热备份。

这几个阶段并不是孤立的，构建信息安全保障体系必须从安全的各个方面进行综合考虑，只有将技术、管理、策略、工程过程等方面紧密结合，安全保障体系才能真正成为指导安全方案设计和建设的有力依据。

习 题 员

员 什么是信息安全？什么是网络安全？

员 信息有哪些安全需求？

员 简述信息安全概念的发展阶段。

员 简述 入侵 的含义。

员 简述 网络安全模型的基本概念。