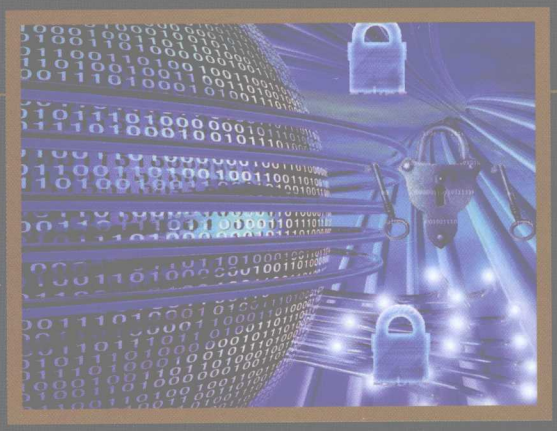
高等学校计算机科学与技术教材

计算机安全基础教程

□ 朱卫东　编著



- 原理与技术的完美结合
- 教学与科研的最新成果
- 语言精炼，实例丰富
- 可操作性强，实用性突出

清华大学出版社　●　北京交通大学出版社

高等学校计算机科学与技术教材

计算机安全基础教程

朱卫东　编著

清华大学出版社
北京交通大学出版社
·北京·

内 容 简 介

本书从计算机安全的基本概念出发，先对计算机安全的定义、安全威胁、安全规范与安全模型、风险管理、安全体系结构作了介绍，然后系统地阐述了包括实体安全与可靠性、密码学、身份认证与访问控制方面、公钥基础设施等计算机安全所涉及的基础理论知识。最后介绍了包括计算机病毒及恶意软件防治、黑客与网络攻击技术、防火墙技术、入侵检测技术、VPN 技术等安全防护方面的知识。

本书是作者在总结了多年教学经验的基础上写成的，适合用本科计算机专业、网络学院、高职高专等计算机专业的课程教材。

图书在版编目（CIP）数据

计算机安全基础教程 / 朱卫东编著. —北京：清华大学出版社；北京交通大学出版社，2009.8
（高等学校计算机科学与技术教材）
ISBN 978-7-81123-588-3

Ⅰ. 计… Ⅱ. 朱… Ⅲ. 电子计算机-安全技术-高等学校-教材 Ⅳ. TP309

中国版本图书馆 CIP 数据核字（2009）第 097073 号

责任编辑：谭文芳
出版发行：清 华 大 学 出 版 社　邮编：100084　电话：010-62776969　http://www.tup.com.cn
　　北京交通大学出版社　邮编：100044　电话：010-51686414　http://press.bjtu.edu.cn
印 刷 者：北京东光印刷厂
经　　销：全国新华书店
开　　本：185×260　印张：15.25　字数：378 千字
版　　次：2009 年 9 月第 1 版　2009 年 9 月第 1 次印刷
书　　号：ISBN 978-7-81123-588-3/TP・500
印　　数：1～4 000 册　定价：26.00 元

本书如有质量问题，请向北京交通大学出版社质监组反映。对您的意见和批评，我们表示欢迎和感谢。
投诉电话：010-51686043，51686008；传真：010-62225406；E-mail：press@bjtu.edu.cn。

前　言

随着信息技术的迅速发展，计算机与人类生活密不可分，人们对计算机的依赖程度越来越高，可是计算机并不安全，它存在着多种安全缺陷和漏洞。攻击者经常利用这些安全缺陷和漏洞对计算机实施攻击和入侵，窃取重要机密资料，导致计算机的瘫痪等，给社会造成巨大的经济损失，甚至危害到地区和国家的安全。因此，计算机的安全问题是一个关系到人类生活与生存的大事情，必须给予充分的重视并设法解决。我们每个使用计算机的人、特别是计算机专业的学生必须具备计算机安全方面的知识。

本书是作者在总结多年来教学经验的基础上，针对计算机专业、电子商务等专业的全日制本科生和网络学院学生编写的教材。教材编写的主导思想是使学生系统地学习计算机安全方面的基础知识和相关技术，提高对计算机安全重要性的认识，掌握计算机安全方面的基本理论、方法与技能，培养学生具有计算机安全分析与实施能力，初步具有计算机安全设计与安全产品使用和维护方面的能力，掌握计算机安全学科的发展动向，掌握实现计算机安全的相关理论与技术，能运用这些理论与技术构建安全基础平台与设施。

全书共 8 章。第 1 章主要介绍计算机安全的概念、安全威胁、安全规范与标准、安全模型、风险管理、安全体系结构。第 2 章从环境安全、设备安全和媒体安全三个方面系统地讲授与计算机系统的实体安全相关的理论及实用知识；可靠性与容错性方面的知识。第 3 章介绍密码学的知识，消息认证与 Hash 函数、数字签名等。第 4 章介绍身份认证与访问控制方面的内容。第 5 章在详细介绍公钥基础设施 PKI 的组成和功能的基础上，也对基于 PKI 的 SSL、SET、S/MIME 和 PGP 安全协议协作了介绍。第 6 章主要介绍计算机病毒防治及恶意软件的防范方面的内容。第 7 章首先对黑客和网络攻击技术作了介绍，然后对缓冲区溢出攻击、监听攻击、端口扫描、拒绝服务攻击、IP 欺骗、木马等常见的网络攻击的原理、预防措施进行介绍。第 8 章主要介绍防火墙技术、入侵检测技术、VPN 技术等安全防护技术。

本书编写过程中得到了北京交通大学计算机学院韩臻院长、远程与继续教育学院陈庚院长、信息中心贾卓生主任的支持和帮助。

陈杰博士、谢倩倩、冯静、邱瑛参与了本书的内容校对、习题编写等方面的工作。杜晔、袁中兰、张大伟博士为本书提供了部分参考资料，在此一并致谢。

作　者

2009 年 6 月

目　录

第 1 章　计算机安全综述

本章主要介绍计算机所面临的各种安全威胁，计算机安全的概念，国内外计算机系统安全规范与标准、安全威胁、安全模型、风险管理和安全体系结构。

1.1　计算机安全的概念与安全威胁

当今社会是科学技术高度发展的信息社会，人类的一切活动均离不开信息，而计算机是对信息进行收集、分析、加工、处理、存储传输等的主体部分。可是计算机并不安全，它潜伏着严重的不安全性、脆弱性和危险性。攻击者经常利用计算机存在的缺陷对其实施攻击和入侵，窃取重要机密资料，甚至导致计算机的瘫痪等，给社会造成巨大的经济损失，甚至危害到国家和地区的安全。因此计算机的安全问题是一个关系到人类生活与生存的大事情，必须给予充分重视并设法解决。

本节分别讲述计算机安全的基本概念、计算机安全的定义、安全威胁和国内外安全标准。

1.1.1　计算机安全的概念

“安全”作为现代汉语的一个基本语词，在各种现代汉语辞书中有着基本相同的解释。《现代汉语词典》对“安全”的解释是“没有危险，不受威胁，不出事故”。计算机安全中的“安全”一词对应的英文是“security”，含义有两方面，一方面是指安全的状态，即免于危险，没有恐惧；另一方面是指对安全的维护，指安全措施和安全机构。

国际标准化委员会有关计算机安全的定义是“为数据处理系统所采取的技术的和管理的安全保护，保护计算机硬件、软件、数据不因偶然的或恶意的原因而遭到破坏、更改、显露”。

美国国防部国家计算机安全中心的定义是“要讨论计算机安全首先必须讨论对安全需求的陈述。一般来说，安全的系统会利用一些专门的安全特性来控制对信息的访问，只有经过适当授权的人，或者以这些人的名义进行的进程可以读、写、创建和删除这些信息”。

我国公安部计算机管理监察司的定义是“计算机安全是指计算机资产安全，即计算机信息系统资源和信息资源不受自然和人为有害因素的威胁和危害”。

从上述定义中可看出，计算机安全不仅涉及技术问题、管理问题，还涉及有关法学、犯罪学、心理学等问题。可以用四部分来描述计算机安全这一概念，即实体安全、软件安全、数据安全和运行安全。而从内容来看，包括计算机安全技术、计算机安全管理、计算机安全评价与安全产品、计算机犯罪与侦查、计算机安全法律、计算机安全监察，以及计算机安全理论与政策。

1.1.2　计算机面临的威胁

计算机面临的威胁主要有：电磁泄露、雷击等环境安全构成的威胁，软硬件故障和工作

人员误操作等人为或偶然事故构成的威胁，利用计算机实施盗窃、诈骗等违法犯罪活动的威胁，网络攻击和计算机病毒构成的威胁，以及信息战的威胁等。

1. 环境安全构成的威胁

计算机的所在环境主要是场地与机房，会受到下述各种不安全因素的威胁。

电磁波辐射：计算机设备本身就有电磁辐射问题，也怕外界电磁波的辐射和干扰，特别是自身辐射带有信息，容易被别人接收，造成信息泄露。

辅助保障系统：水、电、空调中断或不正常会影响系统运行。

自然因素：火、电、水、静电、灰尘、有害气体、地震、雷电、强磁场和电磁脉冲等带来的危害。这些危害有的会损害系统设备，有的则会破坏数据，甚至毁掉整个系统和数据。

2. 计算机的软硬件故障

电子技术的发展使电子设备出故障的概率在几十年里一降再降，许多设备在它们的使用期内根本不会出错。但是由于计算机和网络的电子设备往往极多，故障还是时有发生。由于器件老化、电源不稳、设备环境等很多问题会使计算机或网络的部分设备暂时或者永久失效。这些故障一般都具有突发的特点。

软件是计算机的重要组成部分，由于软件自身的庞大和复杂性，错误和漏洞的出现是不可避免的。软件故障不仅会导致计算机工作异常甚至死机，所存在的漏洞会被黑客利用攻击计算机系统。

3. 人为的无意失误

人为的无意失误包括：程序设计错误、误操作、无意中损坏和无意中泄密等。例如，操作员安全配置不当造成的安全漏洞、用户安全意识不强、用户口令选择不慎、用户将自己的账号随意转借他人或与别人共享等都会对计算机安全带来威胁。

4. 人为的恶意攻击

人为的恶意攻击包括：主动攻击和被动攻击。主动攻击是指以各种方式有选择地破坏信息（如修改、删除、伪造、添加、重放、乱序、冒充等）。被动攻击是指在不干扰网络信息系统正常工作的情况下进行侦收、截获、窃取、破译和业务流量分析及电磁泄露等。这些人为的恶意攻击属于计算机犯罪行为，实施攻击者的主要有以下几种。

（1）雇员

人数最多的计算机罪犯类型由那些最容易接近计算机的人，即雇员构成。有时，雇员只是设法从雇主那里盗窃某种东西——设备、软件、电子资金、专有信息或计算机时间。有时，雇员可能出于怨恨而行动，试图“报复”公司。

（2）外部用户

除雇员外，有些供应商或客户也可能有机会访问公司的计算机系统。使用自动柜员机的银行客户就是一例。像雇员一样，这些授权的用户可能获取秘密口令，或者找到进行计算机犯罪的其他途径。

（3）“黑客”与“非法侵入者”

有些人认为这两类人相同，其实不然。黑客获取对计算机系统未经授权的访问，是因为这种行为有趣和具有挑战性。非法侵入者行为相同，但往往出于恶意。他们可能企图窃取技术信息，或者往系统里放置他们所谓的“炸弹”——一种破坏性计算机程序。

（4）犯罪团伙

犯罪团伙可以像合法的商业人员一样使用计算机，但是为了达到非法的目的。例如，计算机可用于跟踪赃物或非法赌债。另外，伪造者使用计算机和打印机伪造支票、驾驶证等看起来很复杂的证件。

5．计算机病毒与恶意软件

计算机病毒（Computer Virus）在《中华人民共和国计算机信息系统安全保护条例》中被明确定义：“指编制或者在计算机程序中插入的破坏计算机功能或者破坏数据，影响计算机使用并且能够自我复制的一组计算机指令或者程序代码。”计算机病毒是一种高技术犯罪，具有瞬时性、动态性和随机性；不易取证，风险小破坏大，从而刺激了犯罪意识和犯罪活动；是某些人恶作剧和报复心态在计算机应用领域的表现，也是目前对计算机（尤其是个人计算机）的主要威胁之一。

恶意软件（见图 1-1）是恶意植入系统破坏和盗取系统信息的程序。恶意软件的泛滥是继病毒、垃圾邮件后互联网世界的又一个全球性问题。恶意软件的传播严重影响了互联网用户的正常上网，侵犯了互联网用户的正当权益，给互联网带来了严重的安全隐患，妨碍了互联网的应用，侵蚀了互联网的诚信。特洛伊木马就是一种恶意软件。该程序看上去有用或无害，但却包含了旨在利用或损坏运行该程序的系统的隐藏代码。特洛伊木马和蠕虫都是典型的恶意软件。

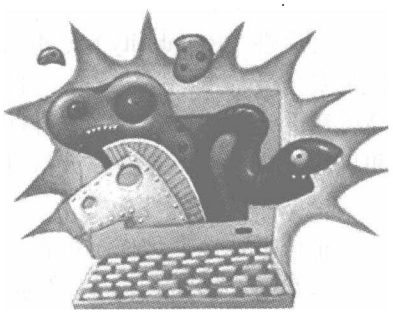


图 1-1　恶意软件

1.1.3　安全目标

计算机的安全目标就是要保证系统资源的保密性（Confidentiality）、完整性（Integrity）和可用性（Availability），这就是通常强调所谓 CIA 三元组的目标。CIA 概念的阐述源自信息技术安全评价准则（Information Technology Security Evaluation Criteria，ITSEC），它也是信息安全的基本要素和安全建设所应遵循的基本原则。除此之外还有不可抵赖性、可鉴别性、真实性、可靠性、可控性等。它们之间是相互联系的。

1．计算机安全的五个属性

在美国国家信息基础设施（National Information Infrastrachure，NII）的文献中，给出了安全的五个属性：保密性、完整性、可用性、可靠性和不可抵赖性。这五个属性适用于国家信息基础设施的教育、娱乐、医疗、运输、国家安全、电力供给及分配、通信等广泛领域。

（1）保密性

保密性是指确保信息不暴露给未授权的实体或进程。即信息的内容不会被未授权的第三

方所知。这里所指的信息不但包括国家秘密，而且包括各种社会团体、企业组织的工作秘密及商业秘密，个人的秘密和个人私密（如浏览习惯、购物习惯）。防止信息失窃和泄露的保障技术称为保密技术。

（2）完整性

完整性是指信息不被偶然或蓄意地删除、修改、伪造、乱序、重放、插入等的特性。只有得到允许的人才能修改实体或进程，并且能够判别出实体或进程是否已被篡改。即信息的内容不能被未授权的第三方修改；信息在存储或传输时不被修改、破坏，不出现信息包的丢失、乱序等。

（3）可用性

可用性是指无论何时，只要用户需要，信息系统必须是可用的，也就是说信息系统不能拒绝服务。网络最基本的功能是向用户提供所需的信息和通信服务，而用户的通信要求是随机的，多方面的（语音、数据、文字和图像等），有时还要求时效性。网络必须随时满足用户通信的要求。攻击者通常采用占用资源的手段阻碍授权者的工作。可以使用访问控制机制，阻止非授权用户进入网络，从而保证网络系统的可用性。增强可用性还包括如何有效地避免因各种灾害（战争、地震等）造成的系统失效。

（4）可靠性

可靠性（Reliability）是指系统在规定条件下和规定时间内、完成规定功能的概率。可靠性是安全最基本的要求之一。目前，对于可靠性的研究基本上偏重于硬件可靠性方面。研制高可靠性元器件设备，采取合理的冗余备份措施仍是最基本的可靠性对策，然而，许多故障和事故则与软件可靠性、人员可靠性和环境可靠性有关。

（5）不可抵赖性

不可抵赖性也称作不可否认性（Non-Repudiation），它是面向通信双方（人、实体或进程）信息真实同一的安全要求，包括收、发双方均具有不可抵赖性。一是源发证明，它提供证据给信息接收者，使发送者不能否认未发送过这些信息及其内容；二是交付证明，它提供证明给信息发送者，使接收者不能否认未接收过这些信息及其内容。

2. 可信计算机系统评价准则

美国国防部的可信计算机系统评价准则（Trusted Computer System Evaluation Criteria TCSEC，橘皮书）是计算机信息安全评估的第一个正式标准，具有划时代的意义。该准则于1970年由美国国防科学委员会提出，并于1985年12月由美国国防部公布。TCSEC将安全分为4个方面：安全政策、可说明性、安全保障和文档。该标准将以上4个方面分为7个安全级别，按安全程度从最低到最高依次是D、C1、C2、B1、B2、B3、A1。

D类：最低保护。无须任何安全措施。属于这个级别的操作系统有：DOS、Windows、Apple的Macintosh System7.1。

C1类：自决的安全保护。系统能够把用户和数据隔开，用户可以根据需要采用系统提供的访问控制措施来保护自己的数据，系统中必有一个防止破坏的区域，其中包含安全功能。用户拥有注册账号和口令，系统通过账号和口令来识别用户是否合法，并决定用户对程序和信息拥有什么样的访问权。

C2类：访问控制保护。控制粒度更细使得允许或拒绝任何用户访问单个文件成为

可能。系统必须对所有的注册、文件的打开、建立和删除进行记录。审计跟踪必须追踪到每个用户对每个目标的访问。能够达到 C2 级的常见操作系统有：UNIX 系统、Windows NT。

B1 类：有标签的安全保护。系统中的每个对象都有一个敏感性标签而每个用户都有一个许可级别。许可级别定义了用户可处理的敏感性标签。系统中的每个文件都按内容分类并标有敏感性标签，任何对用户许可级别和成员分类的更改都受到严格控制。较流行的 B1 级操作系统是 OSF/1。

B2 类：结构化保护。系统的设计和实现要经过彻底的测试和审查。系统应结构化为明确而独立的模块，实施最少特权原则。必须对所有目标和实体实施访问控制。政策要有专职人员负责实施，要进行隐蔽信道分析。系统必须维护一个保护域，保护系统的完整性，防止外部干扰。目前，UnixWare 2.1/ES 作为国内独立开发的具有自主版权的高安全性 UNIX 系统，其安全等级为 B2 级。

B3 类：安全域。系统的关键安全部件必须理解所有客体到主体的访问，必须是防窜扰的，而且必须足够小以便分析与测试。

A1 类：系统保护。系统的设计者必须按照一个正式的设计规范来分析系统。对系统分析后，设计者必须运用核对技术来确保系统符合设计规范。A1 系统必须满足下列要求：系统管理员必须从开发者那里接收到一个安全策略的正式模型；所有的安装操作都必须由系统管理员进行；系统管理员进行的每一步安装操作都必须有正式文档。

3. 国际安全评价标准的发展及其联系

1991 年，欧共体发布了 ITSEC。1993 年，加拿大发布了加拿大可信计算机产品评价准则（Canadian Trusted Computer Product Evaluation Criteria，CTCPEC），CTCPEC 综合了 TCSEC 和 ITSEC 两个准则的优点。同年，美国在对 TCSEC 进行修改补充并吸收 ITSEC 优点的基础上，发布了美国信息技术安全评价联邦准则（Federal Criteria，FC）。ITSEC 与 TCSEC 不同，其观点是应当分别衡量安全的功能和安全的保障，而不应像 TCSEC 那样混合考虑安全的功能和安全的保障。因此，ITSEC 对每个系统赋予两种等级：“F”（Functionality）即安全功能等级，“E”（European Assurance）即安全保障等级。另外，TCSEC 把保密作为安全的重点，而 ITSEC 则把完整性、可用性与保密性作为同等重要的因素。CTCPEC 标准将安全需求分为 4 个层次：机密性、完整性、可靠性和可说明性。FC 参照了 CTCPEC 及 TCSEC，在美国的政府、民间和商业领域得到广泛应用。1993 年 6 月，上述国家共同起草了一份通用准则 CC（Common Criteria for Information Technology Security Evaluation），并将该准则推广为国际标准。1999 年 10 月 CC v2.1 版发布，并且成为 ISO 标准。该准则结合了 FC 及 ITSEC 的主要特征，它强调将安全的功能与保障分离，并将功能需求分为 9 类 63 族，将保障分为 7 类 29 族。

国际安全评价标准的发展及其联系如图 1-2 所示。

ISO 在安全体系结构方面制定了国际标准 ISO 7498-2：1989《信息处理系统开放系统互连基本参考模型第 2 部分安全体系结构》。该标准提供了安全服务与有关机制的一般描述，确定在参考模型内部可以提供这些服务与机制的位置。

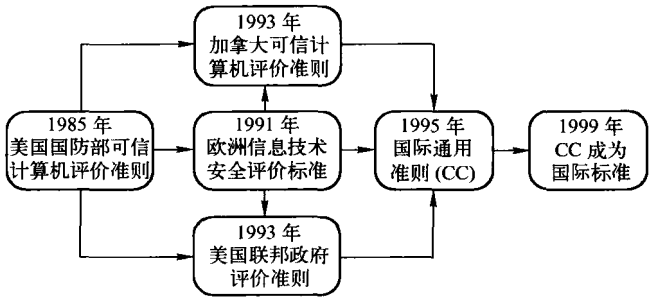


图 1-2 国际安全评价标准的发展及其联系

我国由公安部主持制定、国家技术标准局发布了国家标准 GB 17895—1999《计算机信息系统安全保护等级划分准则》。该准则将信息系统安全分为 5 个等级，分别是：自主保护级、系统审计保护级、安全标记保护级、结构化保护级和访问验证保护级。主要的安全考核指标有身份认证、自主访问控制、数据完整性、审计、隐蔽信道分析、客体重用、强制访问控制、安全标记、可信路径和可信恢复等，这些指标涵盖了不同级别的安全要求。我国红旗安全操作系统 2.0 版本已通过公安部计算机信息系统产品质量监督检验中心的认证，达到信息安全第三级的要求。

1.2 安全模型

可信计算机系统评价准则（TCSEC）的发布对操作系统、数据库等方面的安全发展起到了很大的推动作用，被称为信息安全的里程碑。但是，TCSEC 是基于主机/终端环境的静态安全模型建立起来的标准，是在当时的网络发展水平下被提出来的。随着网络的深入发展，这个标准已经不能完全适应当前的技术需要，无法完全反应分布式、动态变化、发展迅速的 Internet 安全问题。针对日益严重的网络安全问题和越来越突出的安全需求，“动态安全模型”应运而生。最早的动态安全模型是 PDR，模型包含 Protection（保护）、Detectioon（检测）、Response（响应）三个过程，对三者的时间要求满足：Dt + Rt < Pt，其中，Dt 是系统能够检测到网络攻击或入侵所花费的时间，Rt 是从发现对信息系统的入侵开始到系统做出足够反应的时间，Pt 是系统设置各种保护措施的有效防护时间，也就是外界入侵实现对安全目标侵害目的所需要的时间。此模型着重强调 PDR 行为的时间要求，可以不包含风险分析及相关安全策略的制定。在 PDR 模型的基础上，通过增加安全策略，形成策略、防护、检测、响应的动态安全模型 PPDR 和增加恢复策略的保护 PDRR 安全模型。

1.2.1 PPDR 模型

PPDR 模型是可适应网络安全理论或称为动态信息安全理论的主要模型。PPDR 模型包含四个主要部分：Policy（安全策略）、Protection（防护）、Detection（检测）和 Response （响应）。防护、检测和响应组成了一个所谓的“完整的、动态的”安全循环，在安全策略的整体指导下保证信息系统的安全。PPDR 模型如图 1-3 所示。

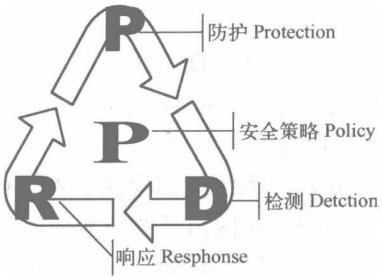


图 1-3　PPDR 模型

1. PPDR 模型的安全策略

PPDR 模型是在整体的安全策略的控制和指导下，在综合运用防护工具（如防火墙、操作系统身份认证、加密等手段）的同时，利用检测工具（如漏洞评估、入侵检测等系统）了解和评估系统的安全状态，将系统调整到“最安全”和“风险最低”的状态 。

根据 PPDR 模型的理论，安全策略是整个网络安全的依据。不同的网络需要不同的策略，在制定策略以前，需要全面考虑局域网络中如何在网络层实现安全性，如何控制远程用户访问的安全性、在广域网上的数据传输实现安全加密传输和用户的认证等问题。对这些问题做出详细回答，并确定相应的防护手段和实施办法，就是针对企业网络的一份完整的安全策略。策略一旦制定，应当作为整个企业安全行为的准则。

2. PPDR 模型的理论体系

PPDR 模型有自己的理论体系，有数学模型作为其论述基础——基于时间的安全理论（Time Based Security）。该理论的最基本原理就是认为，信息安全相关的所有活动，不管是攻击行为、防护行为、检测行为和响应行为等都要消耗时间。因此可以用时间来衡量一个体系的安全性和安全能力。

作为一个防护体系，当入侵者要发起攻击时，每一步都需要花费时间。当然攻击成功花费的时间就是安全体系提供的防护时间 Pt。在入侵发生的同时，检测系统也在发挥作用，检测到入侵行为也要花费时间——检测时间 Dt；在检测到入侵后，系统会做出应有的响应动作，这也要花费时间——响应时间 Rt。

PPDR 模型（如图 1-4 所示）可以用一些典型的数学公式来表达安全的要求。

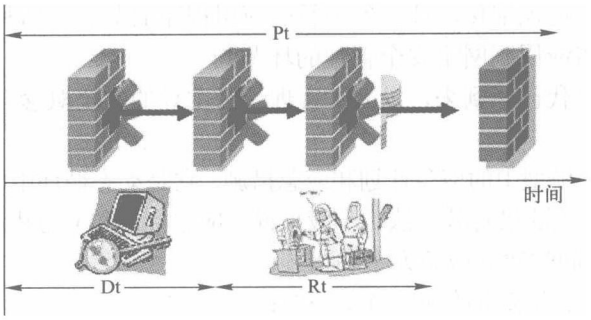


图 1-4　PPDR 时间关系

公式 1：

$$Pt > Dt + Rt$$

Pt 是系统为了保护安全目标设置各种保护后的防护时间；或者理解为在这样的保护方式下，黑客（入侵者）攻击安全目标所花费的时间。

Dt 是从入侵者开始发动入侵开始，系统能够检测到入侵行为所花费的时间。

Rt 是从发现入侵行为开始，系统能够做出足够的响应，将系统调整到正常状态的时间。那么，针对于需要保护的安全目标，如果上述数学公式满足，即防护时间大于检测时间加上响应时间，也就是在入侵者危害安全目标之前就能够被检测到并及时处理。

公式 2：

$$Et = Dt + Rt, \text{ 如果 } Pt=0$$

公式的前提是假设防护时间为 0。这种假设对 Web Server 这样的系统可以成立。

Dt 是从入侵者破坏了安全目标系统开始，系统能够检测到破坏行为所花费的时间。

Rt 是从发现遭到破坏开始，系统能够做出足够的响应，将系统调整到正常状态的时间。比如，对 Web Server 被破坏的页面进行恢复。

那么，Dt 与 Rt 的和就是该安全目标系统的暴露时间 Et。针对于需要保护的安全目标，如果 Et 越小系统就越安全。

通过上面两个公式的描述，实际上给出了安全一个全新的定义："及时的检测和响应就是安全"，"及时的检测和恢复就是安全"。

而且，这样的定义为安全问题的解决给出了明确的方向：提高系统的防护时间 Pt，降低检测时间 Dt 和响应时间 Rt。

3．PPDR 的应用

PPDR 理论给人们提出了全新的安全概念，安全不能依靠单纯的静态防护，也不能依靠单纯的技术手段来解决。网络安全理论和技术还将随着网络技术、应用技术的发展而发展。未来的网络安全会有以下趋势：

一方面，高度灵活和自动化的网络安全管理辅助工具将成为企业信息安全主管的首选，它能帮助管理相当庞大的网络，通过对安全数据进行自动的多维分析和汇总，使人从海量的安全数据中解脱出来，根据它提交的决策报告进行安全策略的制定和安全决策。

另一方面，由于网络安全问题的复杂性，网络安全管理将与已经较成熟的网络管理集成，在统一的平台上实现网络管理和安全管理。

另外，检测技术将更加细化，针对各种新的应用程序的漏洞评估和入侵监控技术将会产生，攻击追踪技术也将应用到网络安全管理的环节当中。

因此，网络安全时代已经到来，以 PPDR 理论为主导的安全概念必将随着技术的发展而不断丰富和完善。

在这里要特别强调模型中的应急计划和应急措施，它是动态循环中的一个关键，也是在发生事件后减轻损失和灾难的最有效方法。一般来说，应急计划和应急措施包括以下三个方面：

① 建立系统时需同时建立应急方案和措施；

② 成立专门的、专人负责的应急行动小组；

③ 入侵发生后迅速有效地控制局面（对入侵者的鉴定和跟踪、分析结果、启动应急方