

网络信息安全

战福瑞

izfree@dlmu.edu.cn

- 教材

- 《信息安全技术（第2版）》，俞承杭，科学出版社，2012.

- 参考书

- 《信息安全技术与应用》，张辉、郭昊、朱晓军、彭新光，人民邮电出版社，2013.

- 考核方式

- 30% 平时成绩
- 70% 期末考试

第一章 计算机网络安全概述

本章知识点

网络安全

NETWORK SECURITY

- 1. 网络安全基本概念
 - (1) 网络安全定义
 - (2) 网络安全目标
 - (3) 网络安全模型
 - (4) 网络安全策略

本章知识点

网络安全

NETWORK SECURITY

- 2.网络安全漏洞与威胁
 - (1) 软件漏洞
 - (2) 网络协议漏洞
 - (3) 安全管理漏洞
 - (4) 网络安全威胁

本章知识点

- 3.信息安全评价标准
 - (1) 美国可信计算机系统评价标准
 - (2) 其他国家信息安全评价标准
 - (3) 国际通用信息安全评价标准
 - (4) 国家信息安全评价标准

第一章 计算机网络安全概述

网络安全

NETWORK SECURITY

Internet迅猛发展以及网络社会化，网络无所不在地影响着社会的政治、经济、文化、军事、意识形态和社会生活各个方面

全球范围内，针对重要信息资源和网络基础设施的入侵行为的数量在持续不断增加，网络攻击与入侵行为对国家安全、经济和社会生活造成了极大的威胁

网络安全已成为世界各国当今共同关注的焦点

第一章 计算机网络安全概述

网络安全

NETWORK SECURITY



中国新闻网 V

【注意！网络安全专家称#拍照比剪刀手会泄露指纹信息#】15日，上海，2019年国家网络安全宣传周全民体验日活动上，专家介绍，拍照比“剪刀手”很容易泄露身份信息。基本上1.5米内拍的剪刀手照片能100%还原指纹，1.5-3米内能还原50%的指纹，超3米拍的照片才难以提取指纹。（澎湃新闻）你觉得比剪刀手危险吗？你觉得比剪刀手危险吗？收起全文^

09月15日 20:53 来自 微博 weibo.com

1.1 网络安全基本概念

1.1.1 网络安全定义

网络安全

NETWORK SECURITY

安全在字典中的定义是为防范间谍活动或蓄意破坏、犯罪、攻击而采取的措施

网络安全就是为防范计算机网络硬件、软件、数据偶然或蓄意破坏、篡改、窃听、假冒、泄露、非法访问和保护网络系统持续有效工作的措施总和

1. 网络安全保护范围

网络安全

NETWORK SECURITY

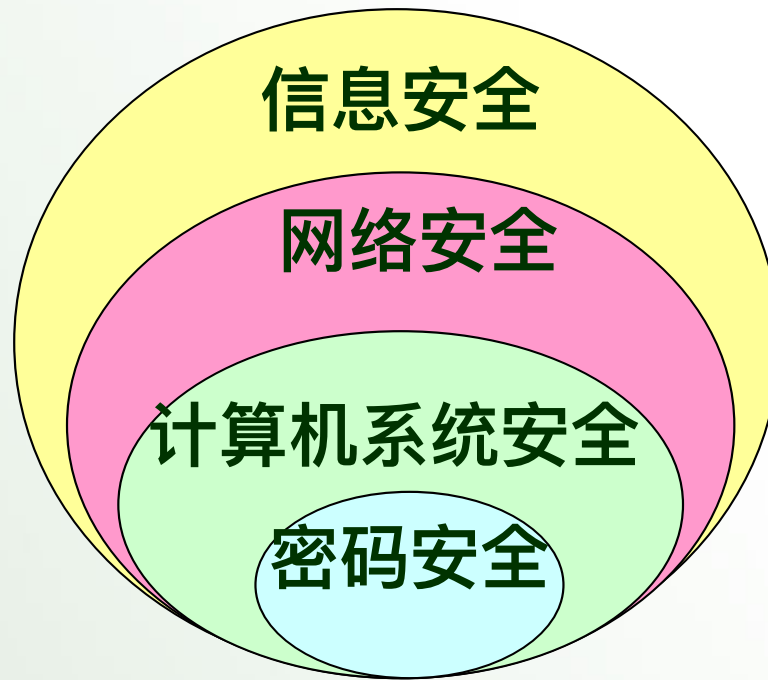


图1.1 网络安全保护范围

2. 网络安全侧重点

网络安全

NETWORK SECURITY



研究人员更关注从理论上采用数学方法精确描述安全属性

工程人员从实际应用角度对成熟的网络安全解决方案和新型网络安全产品更感兴趣

评估人员较多关注的是网络安全评价标准、安全等级划分、安全产品测评方法与工具、网络信息采集以及网络攻击技术

网络管理或网络安全管理人员通常更关心网络安全管理策略、身份认证、访问控制、入侵检测、网络安全审计、网络安全应急响应和计算机病毒防治等安全技术

2. 网络安全侧重点

网络安全

NETWORK SECURITY

对国家安全保密部门来说，必须了解网络信息泄露、窃听和过滤的各种技术手段，避免涉及国家政治、军事、经济等重要机密信息的无意或有意泄露；抑制和过滤威胁国家安全的反动与邪教等意识形态信息传播

对公共安全部门而言，应当熟悉国家和行业部门颁布的常用网络安全监察法律法规、网络安全取证、网络安全审计、知识产权保护、社会文化安全等技术，一旦发现窃取或破坏商业秘密信息、软件盗版、电子出版物侵权、色情与暴力信息传播等各种网络违法犯罪行为，能够取得可信的、完整的、准确的、符合国家法律法规的诉讼证据

军事人员则更关心信息对抗、信息加密、安全通信协议、无线网络安全、入侵攻击和网络病毒传播等网络安全综合技术，通过综合利用网络安全技术夺取网络信息优势；扰乱敌方指挥系统；摧毁敌方网络基础设施，以便赢得未来信息战争的决胜权

保密归

1.1.2 网络安全目标

网络安全
NETWORK SECURITY

完整性
有效性

可控性 (controllability) 是指信息系统对信息内容和传输具有控制能力的特性。

可靠性 (reliability) 是所有信息系统正常运行的基本前提, 通常指信息系统能够在规定的条件与时间内完成规定功能的特性。

拒绝否认性(no-repudiation) 也称为不可抵赖性或不可否认性, 拒绝否认性是指通信双方不能抵赖或否认已完成的操作和承诺, 利用数字签名能够防止通信双方否认曾经发送和接收信息的事实。

最终目标就是通过各种技术与管理手段实现网络信息系统的可靠性、保密性、完整性、有效性、可控性和拒绝否认性。

1. 保密性

网络安全

NETWORK SECURITY

保密性 (confidentiality)

信息系统防止信息非法泄露的特性，信息只限于授权用户使用，保密性主要通过信息加密、身份认证、访问控制、安全通信协议等技术实现，信息加密是防止信息非法泄露的最基本手段

2. 完整性

完整性 (integrity)

信息未经授权不能改变的特性，完整性与保密性强调的侧重点不同。保密性强调信息不能非法泄露，而完整性强调信息在存储和传输过程中不能被偶然或蓄意修改、删除、伪造、添加、破坏或丢失，信息在存储和传输过程中必须保持原样。信息完整性表明了信息的可靠性、正确性、有效性和一致性，只有完整的信息才是可信任的信息

3. 有效性

有效性 (Availability)

信息资源容许授权用户按需访问的特性，有效性是信息系统面向用户服务的安全特性。信息系统只有持续有效，授权用户才能随时、随地根据自己的需要访问信息系统提供的服务。

1.1.3 网络安全模型

网络安全

NETWORK SECURITY

早期的网络安全模型主要从安全操作系统、信息加密、身份认证、访问控制和服务安全访问等方面来保障网络系统的安全性

网络安全解决方案是一个涉及法律、法规、管理、技术和教育等多个因素的复杂系统工程，单凭几个安全技术不可能保障网络系统的安全性

事实上，安全只具有相对意义，绝对的安全只是一个理念，任何安全模型都不可能将所有的安全隐患都考虑周全。因此，理想的网络安全模型永远不会存在

1.1.3 网络安全模型

网络安全

NETWORK SECURITY

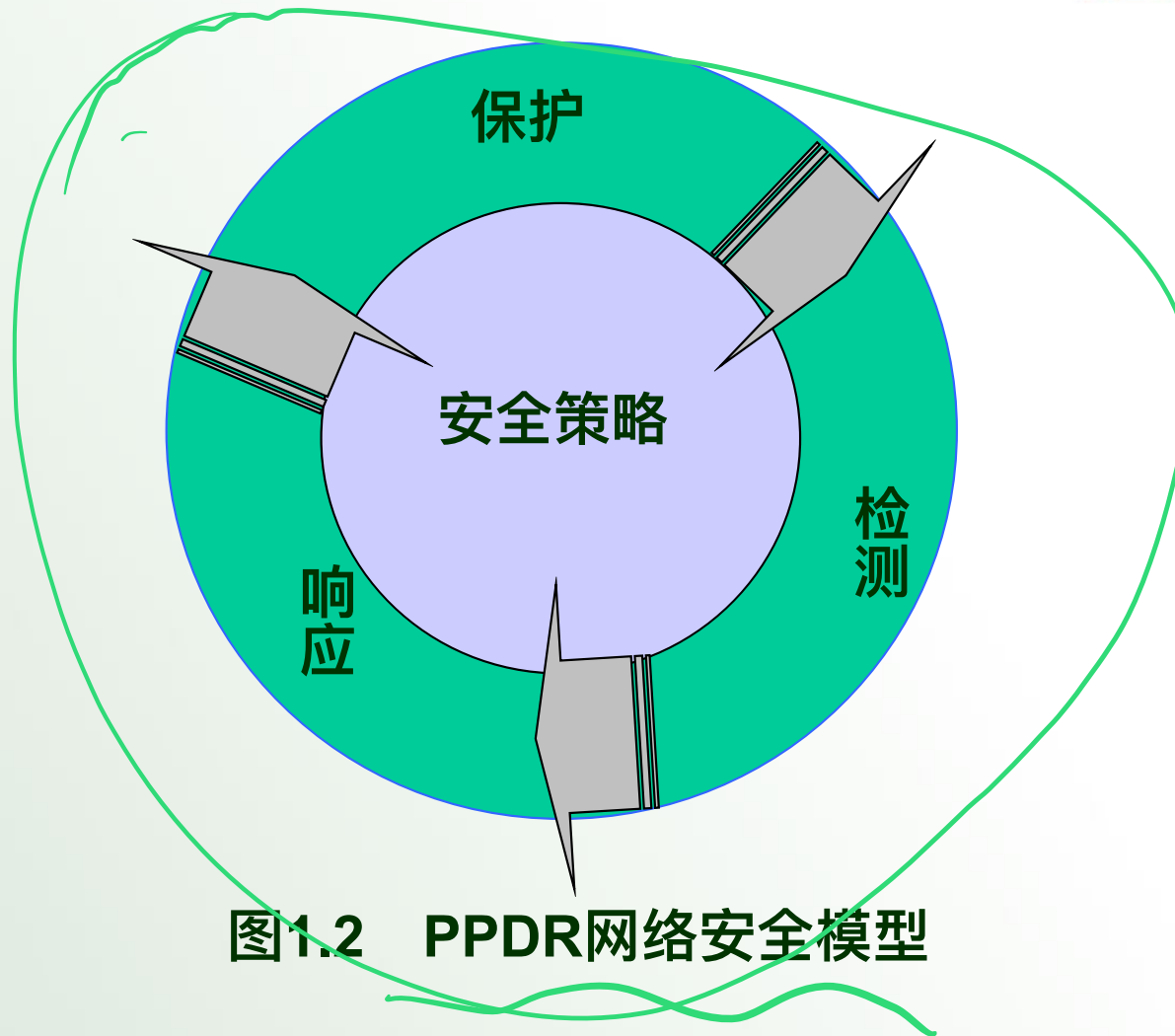



图1.2 PPDR网络安全模型

1.1.3 网络安全模型

网络安全

NETWORK SECURITY



安全保护是网络安全的第一道防线，包括安全细则、安全配置和各种安全防御措施，能够阻止绝大多数网络入侵和危害行为

The diagram illustrates the Network Security Model. It features a large blue double arrow pointing from left to right. On the left side of the arrow, there is a cluster of blue circles of various sizes. On the right side, there is a blue rounded rectangle containing text. The text on the left describes the first line of defense (Security Protection), and the text on the right describes the second line of defense (Intrusion Detection).

入侵检测是第二道防线，目的是采用主动出击方式实时检测合法用户滥用特权、第一道防线遗漏的攻击、未知攻击和各种威胁网络安全的异常行为，通过安全监控中心掌握整个网络的运行状态，采用与安全防御措施联动方式尽可能降低威胁网络安全的风险

1.1.4 网络安全策略

网络安全

NETWORK SECURITY

网络安全策略是保障机构 网络安全的指导文件

总体安全策略

- 总体安全策略用于构建机构网络安全框架和战略指导方针，包括分析安全需求、分析安全威胁、定义安全目标、确定安全保护范围、分配部门责任、配备人力物力、确认违反策略的行为和相应的制裁措施

具体安全管理实施细则

- 总体安全策略只是一个安全指导思想，还不能具体实施，在总体安全策略框架下针对特定应用制定的安全管理细则才规定了具体的实施方法和内容

1. 安全策略总则

网络安全

NETWORK SECURITY

均衡性原则

- 网络安全策略需要在安全需求、易用性、效能和安全成本之间保持相对平衡，科学制定均衡的网络安全策略是提高投资回报和充分发挥网络效能的关键

时效性原则

- 由于影响网络安全的因素随时间有所变化，导致网络安全问题具有显著的时效性

最小化原则

- 网络系统提供的服务越多，安全漏洞和威胁也就越多。因此，应当关闭网络安全策略中没有规定的网络服务；以最小限度原则配置满足安全策略定义的用户权限；及时删除无用账号和主机信任关系，将威胁网络安全的风险降至最低

2. 安全策略内容

网络安全

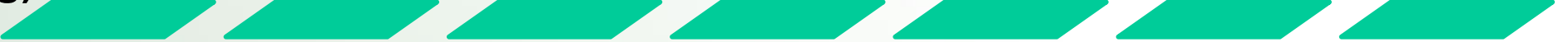
NETWORK SECURITY




1.2 网络安全漏洞与威胁

1.2.1 软件漏洞

软件漏洞(flaw)是指在设计与编制软件时没有考虑对非正常输入进行处理或错误代码而造成的安全隐患，软件漏洞也称为软件脆弱性(vulnerability)或软件隐错(bug)



软件漏洞产生的主要原因是**软件设计人员不可能将所有输入都考虑周全**。软件漏洞是任何软件存在的客观事实。软件产品通常在正式发布之前，一般都要相继发布α版本、β版本和γ版本供反复测试使用，目的就是尽可能减少软件漏洞



1.2.1 软件漏洞

网络安全

NETWORK SECURITY

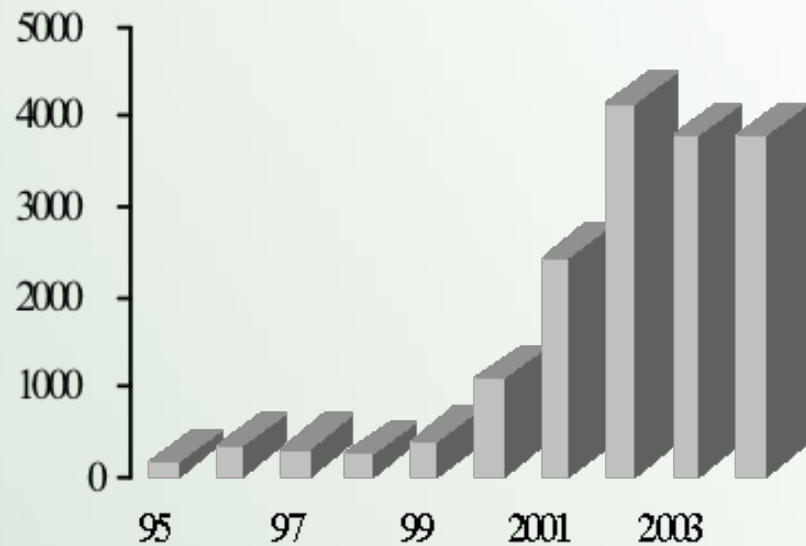


图1.3 软件漏洞趋势图

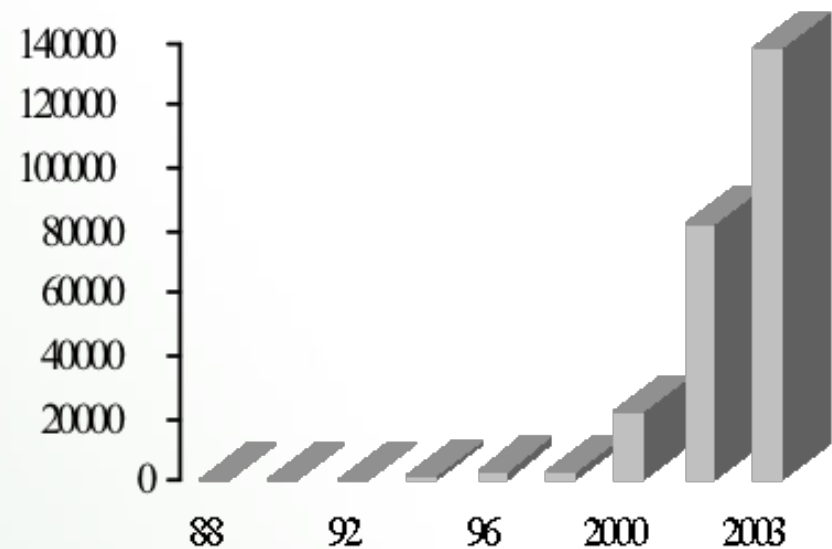


图1.4 攻击事件趋势图

1.2.2 网络协议漏洞

网络安全

NETWORK SECURITY

网络 协议 漏洞

类似于软件漏洞，是指网络通信协议不完善而导致的安全隐患。截止到目前，Internet上广泛使用的TCP/IP协议族几乎所有协议都发现存在安全隐患

1.2.3 安全管理漏洞

网络安全

NETWORK SECURITY

网络安全技术只是保证网络安全的基础，网络安全管理才是发挥网络安全技术的根本保证。因此，网络安全问题并不是一个纯技术问题，从网络安全管理角度看，网络安全首先应当是管理问题

许多安全管理漏洞只要提高安全管理意识完全可以避免，如常见的系统缺省配置、脆弱性口令等。系统缺省配置主要考虑的是用户友好性，但方便使用的同时也就意味着更多的安全隐患

1.2.3 安全管理漏洞(续)

网络安全管理是在网络安全策略指导下为保护网络不受内外各种威胁而采取的一系列网络安全措施，网络安全策略则是根据网络安全目标和网络应用环境，为提供特定安全级别保护而必须遵守的规则。

网络安全是相对的，是建立在信任基础之上的，绝对的网络安全永远不存在。

1.2.4 网络威胁来源(续)

网络安全

NETWORK SECURITY



图1.5 网络安全威胁分类及破坏目标

1.2.4 网络威胁来源(续)

网络安全

NETWORK SECURITY

依据网络安全威胁来自网络边界内部或外部，蓄意攻击还可以分为内部攻击和外部攻击，由于内部人员位于信任范围内，熟悉敏感数据的存放位置、存取方法、网络拓扑结构、安全漏洞及防御措施，而且多数机构的安全保护措施都是“防外不防内”，因此，决大多数蓄意攻击来自内部而不是外部

以窃取网络信息为目的的外部攻击一般称为被动攻击，其他外部攻击统称为主动攻击。被动攻击主要破坏信息的保密性，而主动攻击主要破坏信息的完整性和有效性

被动 → 保密性

主动 → 完整性和有效性

1.2.4 网络威胁来源(续)

网络安全

NETWORK SECURITY

主动攻击

主要来自网络黑客(hacker)、敌对势力、网络金融犯罪分子和商业竞争对手，早期黑客一词并无贬义，指独立思考、智力超群、精力充沛、热衷于探索软件奥秘和显示个人才干的计算机迷。国内多数将黑客作为贬义词使用，泛指利用网络安全漏洞蓄意破坏信息资源保密性、完整性和有效性的恶意攻击者

1.3 信息安全评价标准

网络安全

NETWORK SECURITY

典型的信息安全评价标准

美国国防部《可信计算机系统评价标准》

德国、法国、英国、荷兰
《信息技术安全评价标准》

加拿大《可信计算机产品评价标准》

美国、加拿大、德国、法国、英国
《信息技术安全评价通用标准》

中国国家质量技术监督局
《计算机信息系统安全保护等级划分准则》

1.3.1 信息安全评价标准简介

网络安全

NETWORK SECURITY

• 表1.1 信息安全评价标准发展历程

信息安全标准名称	颁布国家	颁布年份
美国可信计算机系统评价标准TCSEC	美国国防部	1985
美国TCSEC修订版	美国国防部	1987
德国计算机安全评价标准	德国信息安全部	1988
英国计算机安全评价标准	英国贸易部和国防部	1989
信息技术安全评价标准ITSEC	欧洲德、法、英、荷四国	1991
加拿大可信计算机产品评价标准CTCPEC	加拿大政府	1993
信息技术安全评价联邦标准草案FC	美国标准技术委员会和安全局	1993
信息技术安全评价公共标准CC	美、加、德、法、英、荷六国	1996
国家军用标准军用计算机安全评估准则	中国国防科学技术委员会	1996
国际标准ISO/IEC 15408 (CC)	国际标准化组织	1999
计算机信息系统安全保护等级划分准则	中国国家质量技术监督局	1999
信息技术-安全技术-信息技术安全评估准则	中国国家质量技术监督局	2001

1.3.2 美国可信计算机系统评价标准

网络安全

NETWORK SECURITY

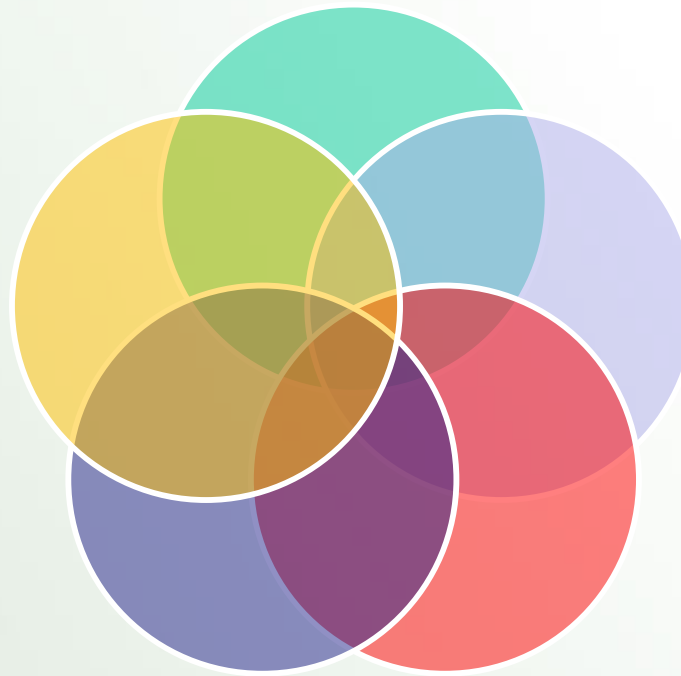
TCSEC根据计算机系统采用的安全策略、提供的安全功能和安全功能保障的可信度将安全级别划分为D、C、B、A四大类七个等级，其中D类安全级别最低，A类安全级别最高

验证安全保护A类

无安全保护D类

强制安全保护B类

自主安全保护C类



1.3.2 美国可信计算机系统评价标准(续)

网络安全

NETWORK SECURITY

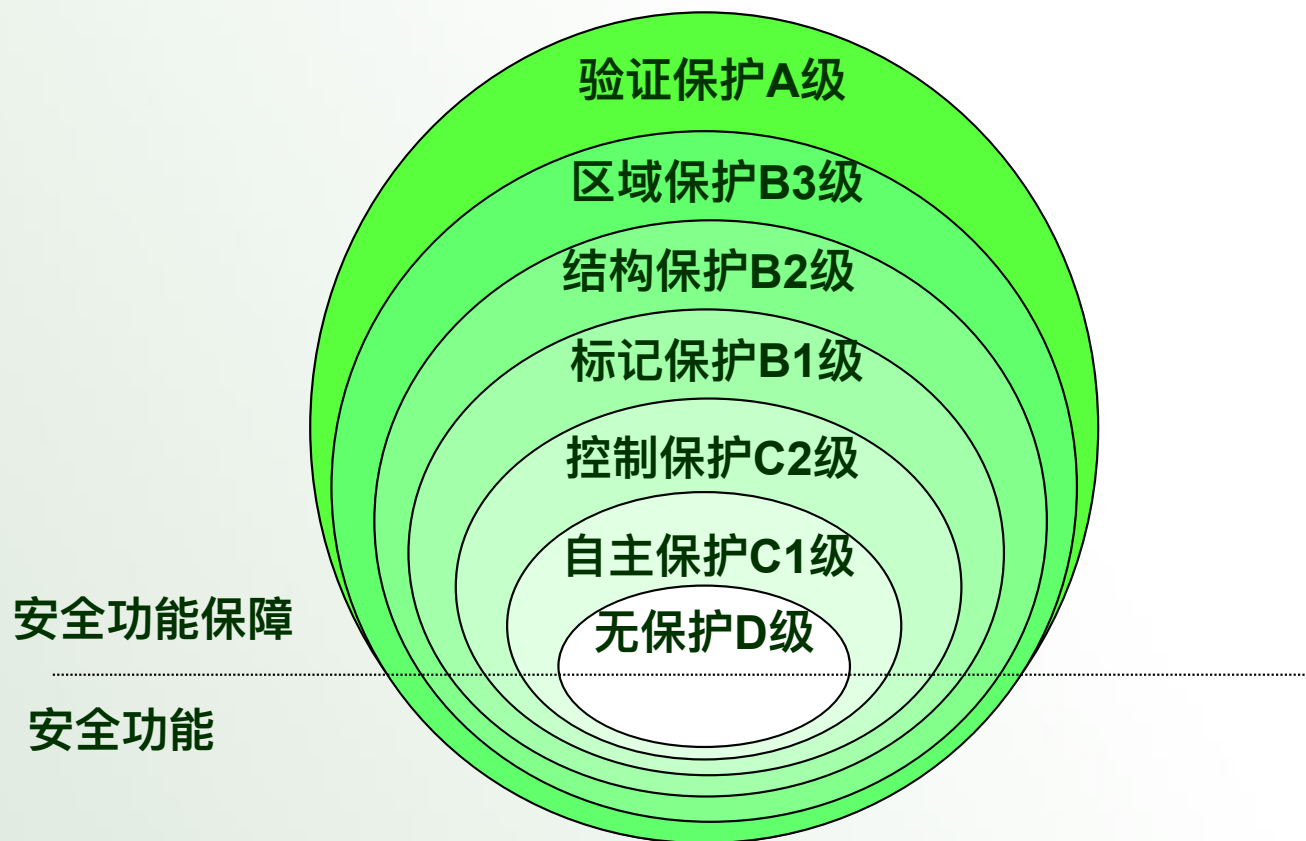


图1.6 TCSEC标准各安全等级关系

1.3.3 其他国家信息安全评价标准

网络安全

NETWORK SECURITY

1.德国计算机安全评价标准

- 《计算机安全评价标准》绿皮书在TCSEC的基础上增加了系统有效性和数据完整性要求，共定义了10个安全功能类别和8个实现安全功能的质量保障等级，安全功能类别用F1~F10表示，安全质量保障等级用Q0~Q7表示

2.欧共体信息技术安全评价标准

- 德国、法国、英国、荷兰联合制定的《信息技术安全评价标准》ITSEC在吸收TCSEC、英国标准和德国绿皮书经验的基础上，首次提出了信息保密性、完整性和有效性安全目标概念

3.加拿大可信计算机产品评价标准

- 加拿大制定的《可信计算机产品评价标准》CTCPEC也将产品的安全要求分成安全功能和功能保障可依赖性两个方面，安全功能根据系统保密性、完整性、有效性和可计算性定义了6个不同等级0~5

1.3.3 其他国家信息安全评价标准(续)

网络安全

NETWORK SECURITY

表1.2 安全评价标准之间的大致对应关系

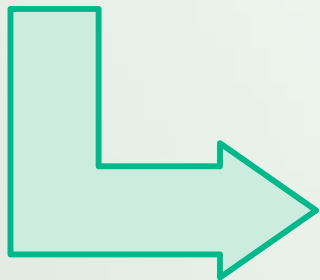
德国绿皮书标准		ITSEC标准		CTCPEC标准		TCSEC标准
功能等级	可信等级	功能等级	可信等级	功能等级	可信等级	安全等级
	Q0		E0		T0	D
F1	Q1	F1	E1		T1	C1
F2	Q2	F2	E2	0	T2	C2
F3	Q3	F3	E3	1	T3	B1
F4	Q4	F4	E4	2	T4	B2
F5	Q5	F5	E5	3	T5	B3
	Q6	F6	E6	4	T6	A
	Q7			5	T7	超A

1.3.4 国际通用信息安全评价标准

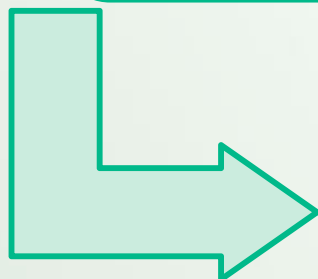
网络安全

NETWORK SECURITY

《信息技术安全评价公共标准》CC能够对信息技术领域中的各种安全措施进行安全评价，重点考虑人为因素导致的安全威胁。评价的信息系统或技术产品及其相关文档在CC中称为评价目标TOE(target of evaluation)



CC标准采用类(class)、族(family)、组件(component)层次结构化方式定义TOE的安全功能



CC标准定义安全保证(security assurance)同样采用了类、族和组件层次结构，保证类包含保证族，保证族又包含保证组件，保证组件由多个保证元素组成

1.3.4 国际通用信息安全评价标准(续)

网络安全

NETWORK SECURITY

表1.3 CC标准定义的安全功能类

序号	类名	类功能
1	FAU	安全审计 (security audit)
2	FCO	通信 (communication)
3	FCS	密码支持 (cryptographic support)
4	FDP	用户数据保护 (user data protection)
5	FIA	身份认证 (identification and authentication)
6	FMT	安全管理 (security management)
7	FPR	隐私 (privacy)
8	FPT	TOE安全功能保护 (protection of TOE security function)
9	FRU	资源利用 (resource utilization)
10	FTA	TOE访问 (TOE access)
11	FTP	可信通路 (trusted path)

1.3.4 国际通用信息安全评价标准(续)

网络安全

NETWORK SECURITY

表1.4 CC标准定义的安全保证类

序号	类名	类功能
1	ACM	配置管理 (configuration management)
2	ADO	提交与操作 (delivery and operation)
3	ADV	开发 (development)
4	AGD	指导文档 (guidance documents)
5	ALC	生命周期支持 (life cycle support)
6	ATE	测试 (tests)
7	AVA	脆弱性评估 (vulnerability assessment)
8	AMA	保证维护 (maintenance of assurance)
9	APE	资源利用 (protection profile evaluation)
10	ASE	安全对象评价 (security target evaluation)

1.3.5 国家信息安全评价标准

网络安全

NETWORK SECURITY

表1.5 CC及国家标准与TCSEC标准的对应关系

CC标准	国家GB17859-1999	国家GB/T 18336-2001	美国TCSEC
			D
EAL1		EAL1	
EAL2	用户自主保护	EAL2	C1
EAL3	系统审计保护	EAL3	C2
EAL4	安全标记保护	EAL4	B1
EAL5	结构化保护	EAL5	B2
EAL6	访问验证保护	EAL6	B3
EAL7		EAL7	A

1.4 国家信息安全保护制度

网络安全

NETWORK SECURITY

信息安全技术标准只是度量信息系统或产品安全性的技术规范，但信息安全技术标准的实施必须通过信息安全法规来保障。为了保护计算机信息系统的安全，促进计算机的应用和发展，保障社会主义现代化建设的顺利进行，1994年2月18日，中华人民共和国国务院发布了第147号令 **《中华人民共和国计算机信息系统安全保护条例》** (以下简称《安全保护条例》)，为计算机信息系统提供了安全保护制度。

1.4.1 信息系统建设和应用制度

- 安全保护制度第八条规定：计算机信息系统的建设和应用，应当遵守法律、行政法规和国家其他有关规定。无论是扩建、改建或新建信息系统，还是设计、施工和验收，都应当符合国家、行业部门或地方政府制定的相关法律、法规和技术标准。
- 军用信息系统建设和应用需符合国家军用标准。

1.4.2 信息安全等级保护制度

网络安全

NETWORK SECURITY



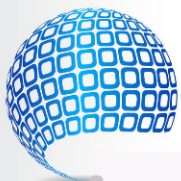
安全等级保护的关键是确定不同安全等级的边界，只有对不同安全等级的信息系统采用相应等级的安全保护措施，才能保障国家安全、维护社会稳定和促进信息化建设健康发展



信息保密等级是划分信息系统安全等级的关键要素，《中华人民共和国保守国家秘密法》明确指出：国家秘密是关系国家的安全和利益，依照法定程序确定，在一定时间内只限一定范围的人员知悉的事项



由于国家秘密信息只限局部范围人员知晓，根据用户应知晓范围赋予不同的访问权限，将用户划分成不同安全等级



国家公安部依据《安全保护条例》、GB17859-1999和GB/T18336-2001陆续颁布了一系列计算机信息系统安全等级保护公共安全行业标准，这些行业标准也是信息系统安全等级保护的重要依据

1.4.3 国际联网备案与媒体进出境制度

网络安全

NETWORK SECURITY



国际联网备案与媒体进出境制度是保障国家安全与利益的重要手段之一，《安全保护条例》第十一条规定：进行国际联网的计算机信息系统，由计算机信息系统的使用单位报省级以上人民政府公安机关备案。第十二条规定：运输、携带、邮寄计算机信息媒体进出境的，应当如实向海关申报



中国互联网络协会和各地公安机关相继建立了不良信息公众举报网站，例如，公安部公共信息网络安全举报网站

<http://www.cyberpolice.cn>

中国互联网络协会主办的违法和不良信息举报中心

<http://net.china.cn>

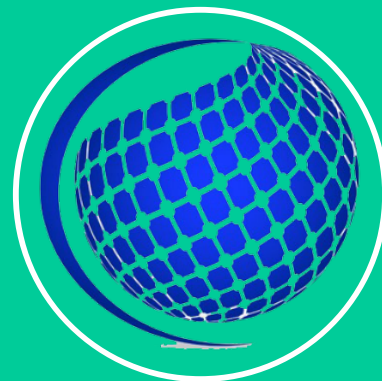
1.4.4 安全管理与计算机犯罪报告制度

网络安全

NETWORK SECURITY



《安全保护条例》第十三条和第十四条分别规定：计算机信息系统的使用单位应当建立健全安全管理制度，负责本单位计算机信息系统的安全保护工作。对计算机信息系统中发生的案件，有关使用单位应当在24小时内向当地县级以上人民政府公安机关报告



我国1997年全面修订《中华人民共和国刑法》时，分别加进了第二百八十五条非法侵入计算机信息系统罪、第二百八十六条破坏计算机信息系统罪和第二百八十七条利用计算机实施的各类犯罪条款



1.4.4 安全管理与计算机犯罪报告制度(续)

网络安全

NETWORK SECURITY

打击计算机犯罪的关键是获取真实、可靠、完整和符合法律规定的电子证据，由于计算机犯罪具有无时间与地点限制、高技术手段、犯罪主体与对象复杂、跨地区和跨国界作案、匿名登录或冒名顶替等特点，使电子证据本身和取证过程不同于传统物证和取证方法，给网络安全和司法调查提出了新的挑战。计算机取证(computer forensics)技术属于网络安全和司法调查领域交叉学科，目前已成为网络安全领域中的研究热点

1.4.5 计算机病毒与有害数据防治制度

网络安全

有害数据是指计算机信息系统及其存储介质中存在、出现的，以计算机程序、图象、文字、声音等多种形式表示的，含有攻击人民民主专政、社会主义制度，攻击党和国家领导人，破坏民族团结等危害国家安全内容的信息；含有宣扬封建迷信、淫秽色情、凶杀、教唆犯罪等危害社会治安秩序内容的信息，以及危害计算机信息系统运行和功能发挥，应用软件、数据可靠性、完整性和保密性，用于违法活动的包含计算机病毒在内的计算机程序

中华人民共和国公安部第51号令《计算机病毒防治管理办法》对计算机病毒概念、计算机病毒主管部门、传播计算机病毒行为、计算机病毒疫情和违规责任等事项进行了详细说明

1.4.6 安全专用产品销售许可证制度

网络安全

NETWORK SECURITY

《安全保护条例》第十六条规定：国家对计算机信息系统安全专用产品的销售实行许可证制度，具体办法由公安部会同有关部门制定

由于信息系统和信息安全产品直接影响着国家的安全和经济利益，各个国家都有自己的测评认证体系。我国的测评认证体系由国家信息安全测评认证管理委员会、国家信息安全测评认证中心(<http://www.itsec.gov.cn>)和授权分支机构组成

为方便读者引用或参考信息安全相关法律法规，表1.6 给出了国家信息安全保护常用法律法规名称、颁布部门和年份。这些法律法规是实施国家信息安全保护制度的指导文件；是保护国家信息安全的坚强后盾；是打击计算机犯罪的有力武器；是公安机关和相关部门行使监督职权的执法依据；也是科学、规范管理信息安全的重要保证

1.4.6 安全专用产品销售许可证制度

网络安全

NETWORK SECURITY

表1.6 国家信息安全保护常用法律法规

法律法规名称	颁布部门	颁布年份
中华人民共和国计算机信息系统安全保护条例	国务院147号令	1994-2-18
中国公用计算机互联网国际联网管理办法	邮电部493号令	1996-4-3
专用网与公用网联网的暂行规定	邮电部	1996-7-24
计算机信息系统安全专用产品检测和销售许可证管理办法	公安部令第32号令	1997-12-12
计算机信息网络国际联网安全保护管理办法	国务院批准公安部发布	1997-12-30
金融机构计算机信息系统安全保护工作暂行规定	公安部 and 中国人民银行	1998-8-31
中华人民共和国保守国家秘密法	全国人大常委会	1988-9-5
计算机信息系统国际联网保密管理规定	国家保密局	2000-1-1
计算机病毒防治产品评级准则GA 243-2000	公安部公共安全行业标准	2000-3-20
计算机病毒防治管理办法	公安部第51号令	2000-4-26
互联网信息服务管理办法	国务院第292号令	2000-9-20

1.4.6 安全专用产品销售许可证制度(续)

网络安全

NETWORK SECURITY

(续表)

联网单位安全员管理办法	公安部	2000-9-29
互联网电子公告服务管理规定	信息产业部	2000-11-7
互联网站从事登载新闻业务管理暂行规定	国务院新闻办公室	2000-11-10
关于维护互联网安全的决定	全国人民代表大会常务委员会	2000-12-2
关于进一步加强互联网上网服务营业场所管理的通知	国务院办公厅	2001-4-3
中国互联网行业自律公约	中国互联网协会	2002-3-26
互联网出版管理暂行规定	新闻出版总署、信息产业部	2002-8-1
互联网上网服务营业场所管理条例	国务院第363号令	2002-9-29
反垃圾邮件规范	中国互联网协会	2003-2-26
互联网站禁止传播淫秽色情等不良信息自律规范	中国互联网协会	2004-6-10
中华人民共和国电子签名法	全国人民代表大会常务委员会	2004-8-28

1.5 本章知识点小结

网络安全

NETWORK SECURITY

国家信息安全保护制度

- 《中华人民共和国计算机信息系统安全保护条例》是实施国家信息安全保护制度的法律文件，从计算机信息系统建设和应用、信息安全等级保护、国际联网备案、媒体进出境申报、建立健全安全管理、计算机犯罪案件报告、计算机病毒与有害数据防治、安全专用产品销售许可证9个方面规定了信息安全保护制度。全国人民代表大会常务委员会、国务院、公安部、国家保密局、信息产业部、邮电部、中国人民银行、中国互联网协会等部门先后颁布了多条配套的法律法规。这些法律法规和国家质量技术监督局颁布的信息安全技术标准为全面实施国家信息安全保护制度奠定了坚实的基础。

1. 概念

2. 目标

3. 安全模型

4. 软件漏洞

5. 蓄意攻击的变种