普通高等院校信息安全专业规划教材

Information Security Conspectus

信息安全概论

免费提供电子教案

电子教案下载网址
http://www.cmpedu.com

李剑 张然 等编著

由各院校从事一线教学工作的教师编写
反映信息安全领域的最新技术和发展方向
注重理论性与实践性相结合
提供完善的教学配套资源

机械工业出版社
CHINA MACHINE PRESS

普通高等院校信息安全专业规划教材

信息安全概论

李 剑 张 然 等编著

机 械 工 业 出 版 社

本书是一本信息安全专业知识的普及教材，以教育部高等学校信息安全类专业教学指导委员会所列知识点为基础，以帮助信息安全专业学生全面了解信息安全知识为目的而编写。全书共19章，第1章讲解信息安全概述；第2章讲解网络安全基础；第3章讲解网络扫描与网络监听；第4章讲解黑客攻击技术；第5章讲解网络后门与网络隐身；第6章讲解计算机病毒与恶意软件；第7章讲解物理环境与设备安全；第8章讲解防火墙技术；第9章讲解入侵检测技术；第10章讲解VPN技术；第11章讲解Windows操作系统安全；第12章讲解UNIX与Linux操作系统安全；第13章讲解密码学基础；第14章讲解PKI原理与应用；第15章讲解数据库系统安全；第16章讲解信息安全管理与法律法规；第17章讲解信息系统等级保护与风险管理；第18章讲解信息系统应急响应；第19章讲解数据备份与恢复。

图书在版编目(CIP)数据

信息安全概论/李剑，张然等编著. —北京：机械工业出版社，2009.1
(普通高等院校信息安全专业规划教材)
ISBN 978-7-111-26103-2

Ⅰ. 信… Ⅱ. ① 李… ② 张… Ⅲ. 信息系统-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010399号

机械工业出版社(北京市百万庄大街22号 邮政编码 100037)
责任编辑：唐德凯
责任印制：洪汉军
北京振兴源印务有限公司印刷厂印刷

2009年2月第1版·第1次印刷
184mm×260mm ·17.5印张·431千字
0001—3000册
标准书号：ISBN 978-7-111-26103-2
定价：28.00元

凡购本书，如有缺页、倒页、脱页，由本社发行部调换
销售服务热线电话：(010)68326294 68993821
购书热线电话：(010)88379639 88379641 88379643
编辑热线电话：(010)88379753 88379739

前　言

为了解决使用计算机所带来的安全问题，达到“普及信息安全知识”这一目的，作者编写了《信息安全概论》这本书。本教材包含了目前信息安全领域常用的攻击技术和防护技术，以及信息安全管理的知识，适合于大学本科专业的学生。

在授课时，教师可以根据授课对象来选择教学的内容以及讲述的深度。对于那些没有学过计算机网络课程的学生，可以在课前适当加一些计算机网络、信息安全方面的知识。本书共19章，第1章是信息安全概述，主要讲述了什么是信息安全、信息安全的历史、信息安全威胁等；第2章是网络安全基础，主要讲述了网络的OSI参考模型、TCP/IP参考模型、常用的网络服务以及常用的网络命令等；第3章是网络扫描与网络监听，主要讲述了黑客的概念、网络扫描技术、网络监听技术等；第4章是黑客攻击技术，主要讲述了黑客攻击的流程以及常见的8种攻击行为；第5章是网络后门与网络隐身，主要讲述了木马攻击、网络后门等；第6章是计算机病毒与恶意软件，主要讲述了计算机病毒的概念、原理、特征、常见的计算机病毒、恶意软件等；第7章是物理环境与设备安全，主要讲述了信息系统的物理层安全知识；第8章是防火墙技术，主要讲述了防火墙的概念、作用、结构等；第9章是入侵检测，主要讲述了入侵检测的概念、误用入侵检测、异常入侵检测、主机入侵检测、网络入侵检测等；第10章是VPN技术，主要讲述了VPN的概念、作用、原理、VPN技术以及VPN的发展趋势等；第11章是Windows操作系统安全，主要讲述了常见的Windows操作系统安全配置；第12章是UXIN与Linux操作系统安全，主要讲述UNIX和Linux操作系统安全配置；第13章是密码学基础，主要讲述什么是密码学、密码学的发展历史、古典密码学、对称密码学、公钥密码学、Hash函数等；第14章是PKI原理与应用，主要讲述什么是PKI、PKI的体系结构、CA证书等；第15章是数据库系统安全，主要讲述了针对数据库系统的攻击、数据库系统的防护等；第16章是信息安全管理与法律法规，主要讲述了信息安全管理的模式、意义、BS7799、常见信息安全法律法规等；第17章是信息系统风险管理与等级保护，主要讲述了信息系统的脆弱性、等级保护、风险管理、风险评估等；第18章是信息系统应急响应，主要讲述了信息系统应急响应的阶段、方法、组织、Windows操作系统下的应急响应、计算机犯罪取证等；第19章是备份与灾难恢复，主要讲述了数据备份和数据恢复。

本书第3、8、9、10章由北京工业大学软件学院张然老师编写，其余各章由北京邮电大学计算机学院李剑老师编写。

感谢北京邮电大学信息安全中心杨义先教授、钮心忻教授、罗群副教授，他们对本书的写作提出了宝贵的意见和建议。感谢我的博士导师北京理工大学的曹元大教授，曹老师对于本书的写作给予了极大的支持与帮助。

感谢中国电信研究院的赵阳博士、中科院计算技术研究所的谭建龙博士、北京交通大学的姚正林博士，它们对本书的写作给了很大的支持。其他参与本书编写和审阅工作的还有景博、李景加浩、景绍达、白小梅、李胜斌、陈彦侠、益德全、李美丽、李建龙、杨芬珍、李磊、马一帆等，这里一并谢过。

本教材也是国家信息产业部重点软课题项目“基于互联网内容安全的关键问题研究”（课题编号：2007 - R - 103）和国家 863 课题“IPS、IMS 关键技术研究”（课题编号：2005143040）的资助成果。

由于本书作者水平有限，书中疏漏与错误之处在所难免，恳请广大同行和读者指正。作者的电子邮箱是 lijian@ bupt. edu. cn。

李　剑
北京邮电大学

目　录

第1章　信息安全概述

本章从一些疑问和一个故事说起，进而讲述信息安全的定义、信息系统的安全威胁以及信息安全发展的过程，然后讲述了信息安全的需求和信息安全实现。

1.1　一些疑问

在使用计算机的时候，经常会遇到各种各样的安全疑问，比如：

1）现在市面上的杀毒软件这么多，国外的有诺顿、卡巴斯基、McAfee 等，国内的有江民、金山、瑞星等，究竟哪一款杀毒软件查杀病毒的效果会更好一些呢？

2）为什么 U 盘里经常会出现 Autorun. inf、RECYCLER、RavMonE. exe 等病毒文件呢？如何防止这些病毒的传染与发作呢？图 1-1 中所示为 U 盘病毒。

3）为什么计算机硬盘里经常会出现一个名为“runauto. .”的病毒文件夹，并且怎么删除都删除不掉呢？图 1-2 所示为 runauto. . 文件夹。

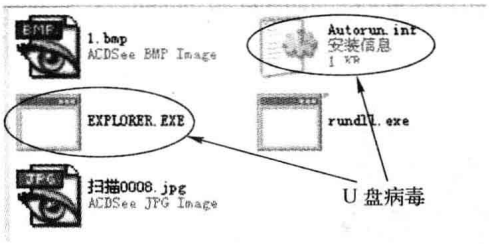

图 1-1　U 盘病毒

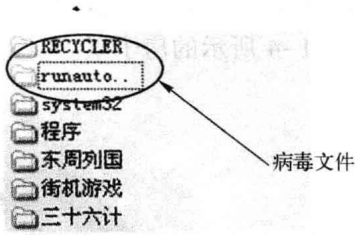

图 1-2　runauto. . 文件夹

4）为什么刚装好的 Windows 2000 专业版的计算机当中，C：盘、D：盘、E：盘等全是共享的，并且还有 IPC$ 空连接？如何去掉这些共享？图 1-3 为使用“net ␣ share”命令看到的操作系统中的共享信息（注：本书中所有的“␣”符号代表空格）。

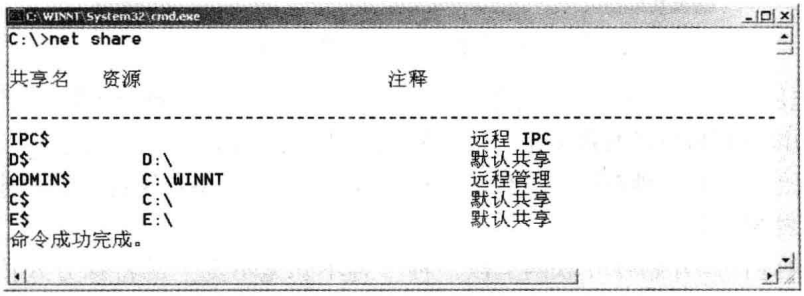

图 1-3　操作系统中的共享信息

5）如果有一天，发现自己的计算机运行很慢，鼠标乱动，并且硬盘灯在不停地闪动，这时会怀疑自己的计算机有病毒，那么应该怎样做应急处理？怎样找出病毒隐藏在什么地方？

6）如果有一天，自己的计算机在运行过程中死机了，重新启动不起来，安全模式也进不去，如果重新安装系统的话，会删除计算机里许多重要的文件（如桌面上的文件等），这时应该怎样处理？

7）如何安装一台新的计算机？安装哪些软件才能使它更安全一些？安装的步骤是什么？对计算机的操作系统应该做怎样的设置？

8）如何一次性将计算机所有补丁都安装上，而不是使用互联网慢慢下载，一个一个安装？

9）如何使用软件防火墙来封锁一个 IP 地址或一个端口？

10）当信息系统遭受攻击的时候，为什么经常会查到攻击人的 IP 地址在日本、美国或是在欧洲呢？难道真的有日本人、美国人、或是欧洲人在攻击信息系统吗？

诸如此类的一系列安全问题，经常困扰着使用计算机的人们。以上这些问题正是本书要解决的问题。

1.2 一个故事

1. 故事的开始

在讲述信息安全之前，这里先讲述一个故事。这个故事发生在 2004 年 4 月 29 日。地点是德国北部罗滕堡镇的一个名叫沃芬森（Waffensen）的小村，这个村仅有 920 人。其中一家人住在图 1-4 所示的房子里。

图 1-4 德国沃芬森村的一个房子

这个房子里住着一个孩子，名叫斯文·雅尚（Sven Jaschan），他的母亲叫维洛妮卡，开了一个门面不算大的以计算机维护修理为主的计算机服务部。4 月 29 日这一天是他 18 岁的生日。几天前，为了庆祝他的生日，他在网上下载了一些代码，修改之后将它放到了互联网上面。

2. 故事的发展

第二天，这些代码开始在互联网上以一种“神不知鬼不觉”的特殊方式传遍全球。“中招”后，计算机开始反复自动关机、重启，网络资源基本上被程序消耗，系统运行极其缓慢，如图 1-5 所示。同时可以看到，病毒占用了大量系统资源，如图 1-6 所示。

这就是全球著名的“震荡波”（Worm. Sasser）蠕虫病毒。据不完全统计，“震荡波”自 2004 年 5 月 1 日开始传播以来，全球已有约 1800 万台计算机感染了这一病毒。

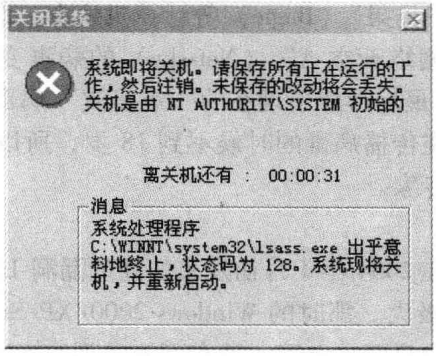

图 1-5　计算机反复自动关机

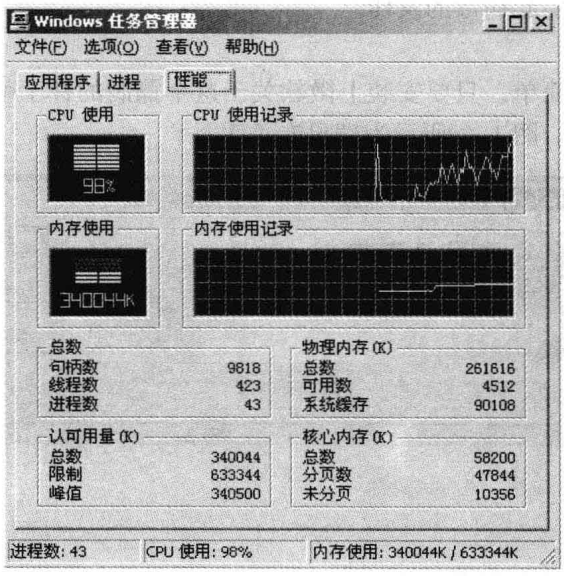

图 1-6　病毒占用大量系统资源

2004 年 5 月 3 日，“震荡波”病毒出现第一个发作高峰，当天先后出现了 B、C、D 三个变种，全中国已有数以十万计的计算机感染了这一病毒。微软公司悬赏 25 万美元查找元凶！

在我国，“五一”长假后的第一天，“震荡波”病毒的第二个高峰汹涌而来。仅 5 月 8 日上午 9 时到 10 时的短短一个小时内，瑞星公司就接到用户的求助电话 2815 个，且 30% 为企业局域网用户，其中不乏大型企业局域网、机场、政府部门、银行等重要单位。5 月 9 日，“震荡波”病毒疫情依然没有得到缓解。

五月份的第一个星期，也就是“震荡波”迅速传播的时候，微软公司德国总部的热线电话就从每周 400 个猛增到 3.5 万个。

3. 故事的结束

开始时，有报道说是一个俄罗斯人编写了这种病毒，因为病毒编定者在编写这个病毒的过程中，加了一段俄语。

5 月 7 日，斯文·雅尚的同学将其告发，斯文·雅尚被警察逮捕。

其实，这个孩子在最开始并不是为了编写出一种病毒来危害别人，而是为了清除和对付

“我的末日”（MyDoom）和“贝果”（Bagle）等计算机病毒。谁知，在编写杀病毒程序的过程中，他设计出一种名为“网络天空 A”（Net-sky）的病毒变体。在朋友的鼓动下，他对“网络天空 A”进行了改动，最后形成了现在的“震荡波”病毒程序。

最后，由于斯文·雅尚在传播病毒的时候不到 18 岁，所以没有受到过重的惩罚。再后来，据说他成了一名反病毒专家。

4. 病毒发作的原因

震荡波病毒是通过微软在 2004 年 4 月初发布的高危漏洞-LSASS 漏洞（微软 MS04 - 011 公告）进行传播的，危害性极大。那时的 Windows 2000/XP/Server 2003 等操作系统都存在该漏洞，这些操作系统的用户只要一上网，就有可能受到该病毒的攻击。

只是大多数用户，对于微软所发布的这些漏洞公告，没有注意，或没有引起高度重视，从而不去打补丁，进而引起病毒的发作。

5. 病毒的防治

这种病毒的防治很简单，只要安装上微软关于这个漏洞的补丁就行了。也可以使用流行的杀病毒软件进行查杀。图 1-7 所示为瑞星专杀工具。

图 1-7　瑞星专杀工具

1.3　信息与信息安全

1.3.1　信息的定义

信息是一种消息，通常以文字或声音、图像的形式来表现，是数据按有意义的关联排列的结果。信息由意义和符号组成。简单说，信息就是指以声音、语言、文字、图像、动画、气味等方式所表示的实际内容。信息是客观事物状态和运动特征的一种普遍形式，客观世界中大量地存在、产生和传递着以这些方式表示出来的各种各样的信息。在谈到信息的时候，

就不可避免地遇到信息的安全问题。

1.3.2 信息安全的定义

信息安全是指信息网络的硬件、软件及其系统中的数据受到保护，不受偶然的或者恶意的原因而遭到破坏、更改、泄露，系统连续可靠正常地运行，信息服务不中断。

信息安全是一门涉及计算机科学、网络技术、通信技术、密码技术、信息安全技术、应用数学、数论、信息论等多种学科的综合性学科。

从广义来说，凡是涉及信息的保密性、完整性、可用性等的相关技术和理论都是信息安全的研究领域。

信息安全本身包括的范围很广，大到国家军事政治等机密安全，小如防止商业机密泄露，防范青少年对不良信息的浏览以及个人信息的泄露等。网络环境下的信息安全体系是保证信息安全的关键，包括计算机安全操作系统、各种安全协议、安全机制（数字签名，信息认证，数据加密等），直至安全系统，其中任何一个安全漏洞都会威胁全局安全。

1.3.3 P^2DR^2 安全模型

基于闭环控制的动态信息安全理论模型在 1995 年开始逐渐形成并得到了迅速发展，学术界先后提出了 PDR、P^2DR 等多种动态风险模型，随着互联网技术的飞速发展，企业网的应用环境千变万化，现有模型存在诸多待发展之处。

P^2DR^2（Policy，Protection，Detection，Response，Restore）动态安全模型研究的是基于企业网对象、依时间及策略特征的动态安全模型结构，由策略、防护、检测、响应和恢复等要素构成，是一种基于闭环控制、主动防御的动态安全模型，通过区域网络的路由及安全策略分析与制定，在网络内部及边界建立实时检测、监测和审计机制，采取实时、快速动态响应的安全手段，应用多样性系统灾难备份恢复、关键系统冗余设计等方法，构造多层次、全方位和立体的区域网络安全环境，如图 1-8 所示。

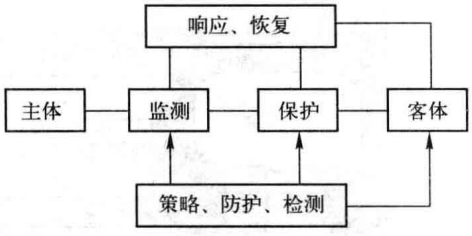

图 1-8 P^2DR^2 动态安全模型

一个良好的网络安全模型应在充分了解网络系统安全需求的基础上，通过安全模型表达安全体系架构，通常应具备以下性质：精确、无歧义、简单和抽象，具有一般性，充分体现安全策略。

该理论的最基本原理是：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 P_t；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 D_t；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 R_t。

P^2DR^2 模型可以用一些典型的数学公式来表达安全的要求：

公式 1：$P_t > D_t + R_t$。

P_t 代表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。D_t 代表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。R_t 代表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，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，就说明在入侵者危害安全目标之前就能被检测到并得到及时处理。

公式 2：$E_t = D_t + R_t$，如果 $P_t = 0$。

公式的前提是假设防护时间为 0。D_t 代表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。R_t 代表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，D_t 与 R_t 的和就是该安全目标系统的暴露时间 E_t。针对需要保护的安全目标，E_t 越小系统就越安全。

通过上面两个公式的描述，实际上给出了一个安全的全新定义：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：延长系统的防护时间 P_t，缩短检测时间 D_t 和响应时间 R_t。

1.3.4 信息安全体系结构

在考虑具体的网络信息安全体系时，把安全体系划分为一个多层面的结构，每个层面都是一个安全层次。根据信息系统的应用现状和网络结构，信息安全问题可以定位在五个层次：物理安全、网络安全、系统安全、应用安全和安全管理，图 1-9 所示为信息安全体系结构以及这些结构层次之间的关系。

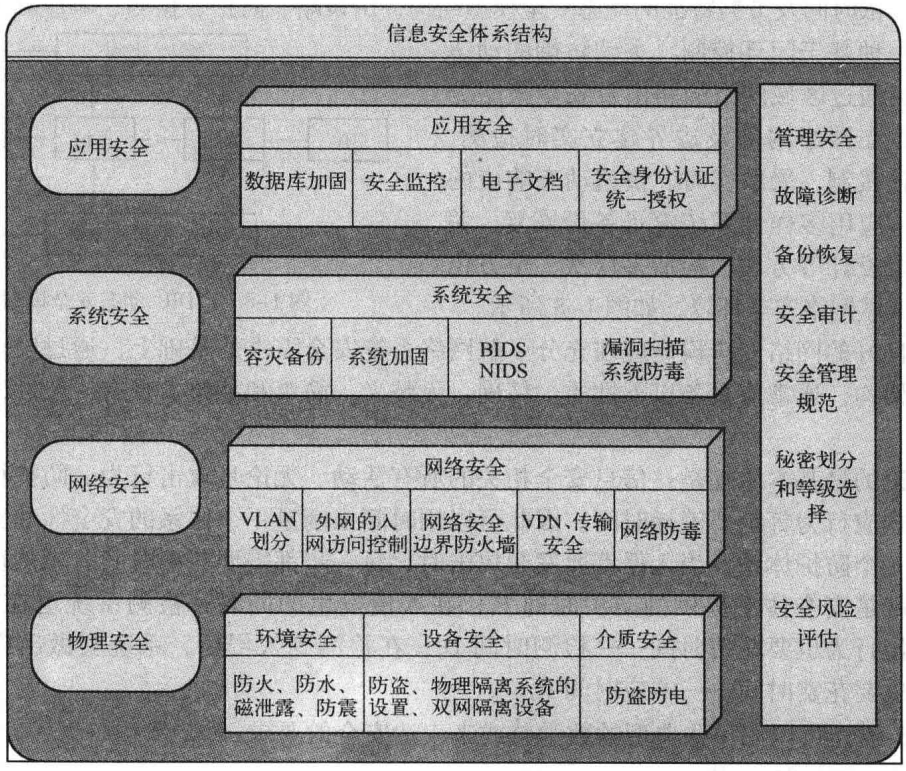

图 1-9 信息系统安全体系

1. 物理层安全

该层次的安全包括通信线路的安全、物理设备的安全、机房的安全等。物理层的安全主要体现在通信线路的可靠性（线路备份、网管软件、传输介质），软硬件设备安全性（替换设备、拆卸设备、增加设备），设备的备份，防灾害、防干扰能力，设备的运行环境（温度、湿度、烟尘），不间断电源保障，等等。

2. 网络层安全

该层次的安全问题主要体现在网络方面的安全性，包括网络层身份认证，网络资源的访问控制，数据传输的保密与完整性，远程接入的安全，域名系统的安全，路由系统的安全，入侵检测的手段，网络设施防病毒等。网络层常用的安全工具包括防火墙系统、入侵检测系统、VPN 系统、网络蜜罐等。

3. 系统层安全

该层次的安全问题来自网络内使用的操作系统，如 Windows NT，Windows 2000 等。系统层安全主要表现在三方面，一是操作系统本身的缺陷带来的不安全因素，主要包括身份认证、访问控制、系统漏洞等；二是对操作系统的安全配置问题；三是病毒对操作系统的威胁。

4. 应用层安全

应用层的安全主要考虑所采用的应用软件和业务数据的安全性，包括数据库软件、Web 服务、电子邮件系统等。此外，还包括病毒对系统的威胁，因此要使用防病毒软件。

5. 管理层安全

安全领域有句话叫“三分技术，七分管理”，管理层安全从某种意义上来说要比以上 4 个安全层次更重要。管理层安全包括安全技术和设备的管理、安全管理制度、部门与人员的组织规则等。管理的制度化程度极大地影响着整个网络的安全，严格的安全管理制度、明确的部门安全职责划分、合理的人员角色定义都可以在很大程度上弥补其他层次的安全漏洞。

1.3.5 信息安全的目标

开始的时候，信息安全具有三个目标：保密性、完整性和可用性（Confidentiality、Integrity、Availability，CIA）。后来，对信息安全的目标进行了扩展，将 CIA 三个目标扩展为：保密性、完整性、可用性、真实性、不可否认性、可追究性、可控性等 7 个信息安全技术目标。其中所增加的真实性、不可否认性、可追究性、可控性可以认为是完整性的扩展和细化。

1）保密性：保证机密信息不被窃听，或窃听者不能了解信息的真实含义。

2）完整性：保证数据的一致性，防止数据被非法用户篡改。

3）可用性：保证合法用户对信息和资源的使用不会被不正当地拒绝。

4）真实性：对信息的来源进行判断，能对伪造来源的信息予以鉴别。

5）不可否认性：建立有效的责任机制，防止用户否认其行为，这一点在电子商务中是极其重要的。

6）可控制性：对信息的传播及内容具有控制能力。

7）可追究性：对出现的网络安全问题提供调查的依据和手段。