

计算机系列教材

计算机系统安全

李章兵 编著

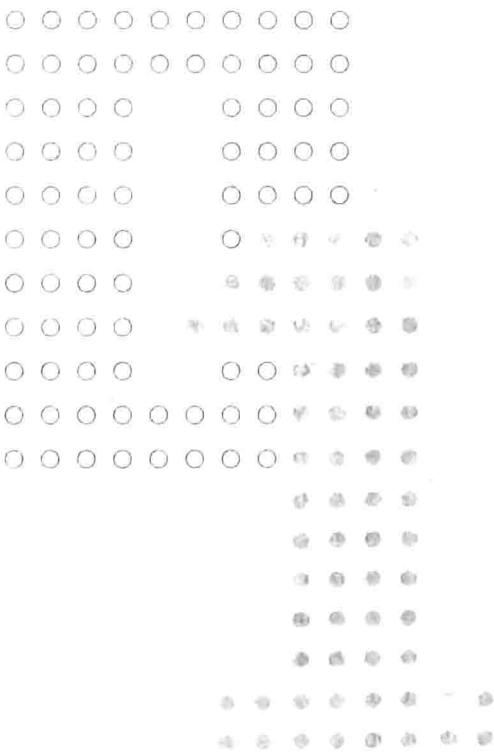


清华大学出版社

计算机系列教材

李章兵 编著

计算机系统安全



清华大学出版社
北京

内 容 简 介

计算机系统安全是信息安全的关键内容之一,它已成为计算机信息系统的核心技术,也是网络安全的重要基础和补充。本书是作者在长期信息安全教学和科研的基础上编写而成的,书中系统地阐述计算机安全理论、技术和方法,全面讲述计算机安全基础(信息系统及其威胁,安全体系结构与模型、标准)、恶意代码、数据加密与保护、访问控制、信息认证技术、操作系统安全、软件保护与数字版权管理、黑客、数据库安全、防火墙、入侵检测与防御、数字取证技术等方面的内容,涵盖了计算机技术与密码学理论。

本书概念清晰,表达深入浅出,内容新颖翔实,重点突出,理论与实践相结合,实用性强,易学易懂。

本书可作为信息安全、计算机、网络工程等相关专业的高年级本科生或研究生教材,也可供相关专业的教学、科研和工程从业人员参考。

本书封面贴有清华大学出版社防伪标签,无标签者不得销售。

版权所有,侵权必究。侵权举报电话:010-62782989 13701121933

图书在版编目(CIP)数据

计算机系统安全/李章兵编著. --北京:清华大学出版社,2014

计算机系列教材

ISBN 978-7-302-36552-5

I. ①计… II. ①李… III. ①计算机网络—安全技术—高等学校—教材 IV. ①TP393.08

中国版本图书馆 CIP 数据核字(2014)第 112343 号

责任编辑:张 玥 顾 冰

封面设计:常雪影

责任校对:时翠兰

责任印制:李红英

出版发行:清华大学出版社

网 址: <http://www.tup.com.cn>, <http://www.wqbook.com>

地 址:北京清华大学学研大厦 A 座 邮 编:100084

社 总 机:010-62770175 邮 购:010-62786544

投稿与读者服务:010-62776969, c-service@tup.tsinghua.edu.cn

质量反馈:010-62772015, zhiliang@tup.tsinghua.edu.cn

课件下载: <http://www.tup.com.cn>, 010-62795954

印 刷 者:清华大学印刷厂

装 订 者:三河市溧源装订厂

经 销:全国新华书店

开 本:185mm×260mm 印 张:31.75

字 数:773 千字

版 次:2014 年 9 月第 1 版

印 次:2014 年 9 月第 1 次印刷

印 数:1~2000

定 价:59.00 元

产品编号:058756-01

计算机在政治、军事、金融、商业等部门的应用越来越广泛,社会对计算机系统的依赖也越来越大,安全可靠的计算机系统应用已经成为支撑国民经济、关键性基础设施以及国防的支柱,信息安全在各国都受到了前所未有的重视。“信息安全+国土安全=国家安全”正逐渐得到社会的认同。我国成立了国家计算机网络应急处理协调中心 CNCERT(<http://www.cert.org.cn>)、国家计算机病毒应急处理中心 CVERC(<http://www.antivirus-china.org.cn>)、国家计算机网络入侵防范中心(<http://www.nipc.org.cn>)、信息安全国家重点实验室(<http://www.is.ac.cn>)等一批国家级信息安全机构。许多高校及科研院所开设了信息安全专业以及“信息安全导论”、“计算机系统安全”等相关课程。

计算机系统安全是信息安全的关键内容之一,它已成为计算机信息系统的核心技术,也是网络安全的重要基础和补充。学习计算机系统安全,密码学是理论基础,恶意代码和黑客是重要的威胁源,必须掌握其原理和技术,操作系统安全、数据库安全、软件保护和数字版权管理是核心,访问控制、防火墙、入侵检测与防御以及数字取证是实现计算机系统安全的重要技术和保障。

本教材从计算机系统安全的角度出发,结合多年来“信息安全导论”的教学经验,根据教学需要不断充实改进内容,突出了计算机系统安全的概念、原理、技术和应用实例,反映了信息安全的最新进展。第1章介绍计算机信息系统与所面临的威胁、计算机系统安全概念、体系结构、安全模型、安全等级标准、信息资产风险评估等基础知识。第2章介绍计算机病毒、蠕虫、后门、木马、僵尸网络、恶意移动代码等恶意代码的原理和防范,并对反病毒原理与技术加以介绍。第3章介绍密码学基础知识、对称密码、公钥密码、密钥管理、新型密码、信息隐藏与水印、数据与版权保护等。第4章详细介绍认证需要的杂凑函数、数字签名以及消息认证、身份认证和实用的认证系统和协议。第5章介绍访问控制的模型、策略和实现,以及授权与审计跟踪等知识。第6章从进程、内存、文件系统和应用程序的角度,介绍操作系统的安全、安全OS的设计理论、Windows安全、UNIX安全以及设备安全等。第7章介绍软件的保护、破解和逆向的原理和技术,以及数字版权管理(DRM)技术。第8章详细介绍黑客及其信息收集类、入侵类、欺骗类、拒绝服务类的攻击,以及木马植入和网络钓鱼技术。第9章简介数据库系统及其安全概念,阐述数据库的管理系统安全、数据安全(关联推理和隐私保护)和应用系统安全等原理和技术。第10章介绍防火墙的基本知识、体系结构、过滤原理与技术、网闸以及防火墙的配置与管理等。第11章介绍入侵检测的概念、原理、技术、实现和蜜罐技术以及IDS的部署和产品,并介绍和比较了入侵防御系统原理和技术。第12章从计算机犯罪和电子证据概念入手,介绍计算机数字取证的原理和技术、证据分析以及反取证技术等。

本书概念清晰,理论和实践并重,重点突出。偏重实践的书缺乏理论深度,而偏重理论的书很难提高学生进一步学习的兴趣。本书注重从原理和实践双重角度阐明计算机系统的知识,教会学生一些处理问题的原理和具体方法并用于实践中,帮助加深对比较抽象和枯燥的理论的理解。

本书选材合理,内容翔实、全面、新颖、深入浅出。重点阐述恶意代码、访问控制、信息认证、操作系统、数据库、软件保护与数字版权等计算机系统安全的基本概念,特别侧重阐述恶意代码这把“威胁之剑”的使用和铸造、黑客攻击等的原理和技术。在防御方面阐述防火墙、入侵检测、数字取证等理论和技术知识。密码学作为信息安全的基础,本书阐述其基本理论,摒弃过时和不过关的内容。总之,本书全面反映了近几年计算机系统安全领域的新发展。

作为“网络安全”的基础,交叉内容较少。密码学、黑客、防火墙和入侵检测等理论和技术也是计算机系统安全需要的知识,但侧重于方法、部署和管理,需要的网络专业知识较少。对于开设了密码学的学生,第3、4章的部分内容可以选择讲授。

本书参考了大量的RFC文档(<http://www.ietf.org/rfc.html>)、美国国家标准技术研究所出版物(<http://csrc.nist.gov/publications>),也希望读者在学习的过程中查阅参考。

虽然经过多次修改,鉴于水平有限,书中错漏难免,欢迎读者批评指正。本书参考了大量相关书籍,引用了许多来自于互联网的资料和PPT,但多数资料没有版权信息,无法一一列在参考文献中,敬请作者谅解。

本书不仅适合信息安全专业的本科高年级学生学习,也适合计算机相关专业的其他本科学生和工程技术人员学习和参考,可以作为“信息安全导论”、“信息安全基础”、“计算机系统安全”等相关课程的教材。

本书的编写过程受到湖南省科技计划(2011FJ4300、2012FJ3047)和湖南省教育厅科研项目(11C0533)的资助。感谢北京邮电大学杨义先教授、武汉大学彭国军、王丽娜教授在信息安全领域给予的指导和支持。感谢湖南科技大学计算机科学与工程学院徐建波教授、知识处理与网络化制造、湖南省重点实验室刘建勋教授的支持,感谢钟小勇、汪丰兰、娄宇、许梁茜、李佳、宋佳静、符婷、赖朝刚等人的资料整理和绘图。感谢清华大学出版社对本书出版的支持与帮助。

作 者

2014.2

F O R E W O R D

第 1 章	计算机系统安全概述	/1
1.1	信息系统与信息安全	/1
1.1.1	信息化及信息系统	/1
1.1.2	信息的安全威胁	/2
1.1.3	信息安全	/6
1.2	信息安全体系结构	/10
1.2.1	OSI 安全体系结构	/10
1.2.2	Internet 安全体系结构	/12
1.2.3	基于 TCP/IP 的网络安全 体系结构	/14
1.3	信息安全模型与策略	/15
1.3.1	信息安全模型	/15
1.3.2	信息安全策略	/19
1.4	计算机系统安全	/22
1.4.1	计算机系统安全概述	/22
1.4.2	计算机系统安全的目标与技术	/23
1.4.3	计算机系统安全标准	/25
1.4.4	信息系统安全保护等级划分	/26
1.4.5	计算机系统的风险评估	/29
1.4.6	全书内容安排	/35
	本章小结	/36
	习题 1	/37
第 2 章	恶意代码	/39
2.1	恶意代码概述	/39
2.2	计算机病毒	/40
2.2.1	计算机病毒概述	/40
2.2.2	传统的计算机病毒——DOS 病毒	/43
2.2.3	Windows 病毒	/47
2.3	网络蠕虫	/55
2.3.1	蠕虫程序的功能结构	/55
2.3.2	蠕虫程序的工作机制	/56

2.3.3	蠕虫的扫描机制与策略	/56
2.3.4	网络蠕虫特征	/57
2.3.5	网络蠕虫防御和清除	/58
2.3.6	网络蠕虫举例	/58
2.4	后门病毒	/59
2.4.1	后门病毒的类型与特点	/59
2.4.2	后门病毒的工作机制	/60
2.4.3	后门病毒的举例	/61
2.4.4	检测和防御后门启动技术	/62
2.5	木马	/63
2.5.1	木马概述	/63
2.5.2	木马控制原理与技术	/65
2.5.3	木马的防御	/70
2.5.4	木马举例	/71
2.6	特殊后门与僵尸网络	/71
2.6.1	Rootkit 后门	/71
2.6.2	僵尸网络	/73
2.7	恶意移动代码	/76
2.7.1	恶意浏览器脚本	/77
2.7.2	恶意插件	/77
2.7.3	恶意 ActiveX 控件	/77
2.7.4	间谍软件与恶意广告软件	/78
2.7.5	恶意移动代码的特点比较	/79
2.8	反病毒原理与技术	/80
2.8.1	病毒检测原理	/80
2.8.2	启发式扫描技术	/82
2.8.3	专业杀毒软件	/82
2.8.4	病毒防范措施	/83
	本章小结	/83
	习题 2	/84

第 3 章 数据加密基础 /85

3.1	密码学概述	/85
-----	-------	-----

- 3.1.1 密码体制 /85
- 3.1.2 密码系统分类 /86
- 3.1.3 序列密码与随机序列数 /87
- 3.1.4 密码分析与攻击 /89
- 3.1.5 密码协议 /91
- 3.2 对称密码 /91
 - 3.2.1 古典密码学 /92
 - 3.2.2 数据加密标准 /93
 - 3.2.3 高级加密标准 /100
 - 3.2.4 分组密码的工作模式 /108
- 3.3 公钥密码 /111
 - 3.3.1 公开密钥体制与单向陷门函数 /111
 - 3.3.2 RSA 算法 /112
 - 3.3.3 Elgamal 密码系统 /115
 - 3.3.4 椭圆曲线密码体制 /116
 - 3.3.5 对称加密体制与公开密钥体制比较 /118
- 3.4 密钥管理 /119
 - 3.4.1 密钥的分类与产生 /119
 - 3.4.2 密钥的管理 /120
 - 3.4.3 密钥分配 /121
 - 3.4.4 公钥加密体制密钥管理 /122
 - 3.4.5 Diffie-Hellman 密钥交换 /124
 - 3.4.6 密钥托管 /125
- 3.5 其他新型密码学 /126
 - 3.5.1 量子密码 /126
 - 3.5.2 DNA 密码 /130
 - 3.5.3 混沌密码 /131
 - 3.5.4 演化密码 /132
- 3.6 信息隐藏与水印 /133
 - 3.6.1 信息隐藏 /133
 - 3.6.2 数字水印 /134

本章小结 /137

习题 3 /138

第 4 章 信息认证技术 /140

4.1 概述 /140

4.2 杂凑函数 /141

4.2.1 杂凑函数概念 /141

4.2.2 Hash 函数的构造形式 /141

4.2.3 MD5 算法 /142

4.2.4 SHA 算法 /146

4.2.5 其他 Hash 算法 /148

4.2.6 对 Hash 函数的攻击 /149

4.2.7 消息认证码 /150

4.3 数字签名 /151

4.3.1 基本概念 /151

4.3.2 杂凑函数的数字签名 /154

4.3.3 RSA 数字签名算法 /155

4.3.4 ElGamal 数字签名 /156

4.3.5 DSS 签名 /158

4.3.6 椭圆曲线签名 /159

4.3.7 盲签名 /160

4.3.8 群签名 /162

4.3.9 其他数字签名方案 /163

4.4 消息认证 /165

4.4.1 消息的内容认证 /165

4.4.2 消息的其他特性认证 /169

4.5 身份认证 /170

4.5.1 身份认证概念 /170

4.5.2 身份标识 /171

4.5.3 身份认证分类与方式 /174

4.5.4 身份识别协议 /176

4.5.5 认证的口令机制 /178

4.5.6 认证的主体特征机制 /180

4.5.7	认证的数字证书机制	/183
4.5.8	认证的智能卡机制	/185
4.6	实用的认证系统	/187
4.6.1	一次性动态口令认证	/188
4.6.2	RADIUS 拨号认证	/189
4.6.3	Kerberos 认证系统	/190
4.6.4	单点登录	/193
	本章小结	/194
	习题 4	/195

第 5 章 访问控制 /197

5.1	访问控制概述	/197
5.2	访问控制模型	/200
5.2.1	自主访问控制模型	/200
5.2.2	强制访问控制模型	/203
5.2.3	基于角色的访问控制模型	/207
5.2.4	基于任务的访问控制模型	/212
5.2.5	基于对象的访问控制模型	/213
5.2.6	信息流模型	/214
5.3	访问控制的安全策略	/214
5.4	访问控制的实现	/216
5.5	授权	/219
5.6	审计跟踪	/220
	本章小结	/222
	习题 5	/223

第 6 章 操作系统安全 /224

6.1	操作系统安全概述	/224
6.1.1	操作系统构成	/224
6.1.2	安全操作系统功能	/225
6.1.3	操作系统的安全措施	/225
6.2	安全操作系统	/226
6.2.1	安全操作系统概念	/226

6.2.2	安全模型	/230
6.2.3	安全隔离设施	/233
6.2.4	操作系统的安全机制	/235
6.2.5	安全操作系统设计	/239
6.2.6	安全操作系统研究历史	/242
6.3	Windows 操作系统安全	/242
6.3.1	Windows 安全模型	/242
6.3.2	Windows 用户身份识别/ 验证机制	/245
6.3.3	存储保护	/246
6.3.4	用户态和核心态	/247
6.3.5	注册表	/249
6.3.6	文件系统安全	/252
6.3.7	Windows 安全配置	/255
6.3.8	Vista/Win7 安全	/256
6.4	UNIX 系统安全	/259
6.5	设备安全	/268
	本章小结	/269
	习题 6	/269

第 7 章 软件保护与 DRM /270

7.1	软件保护概述	/270
7.1.1	软件保护概念	/270
7.1.2	软件保护技术的发展历史	/270
7.1.3	软件保护的技术目的	/271
7.2	软件保护技术	/271
7.2.1	软件的硬保护技术	/271
7.2.2	软件的软保护技术	/273
7.2.3	壳保护技术	/275
7.2.4	花指令	/277
7.2.5	SMC 技术	/277
7.2.6	补丁技术	/278
7.2.7	软件许可——激活技术	/279

7.2.8	软件保护小结	/279
7.3	软件破解原理与技术	/280
7.3.1	软件破解原理	/280
7.3.2	PE 文件格式	/281
7.3.3	软件静态分析技术	/285
7.3.4	动态分析破解技术	/288
7.3.5	脱壳技术	/290
7.3.6	其他破解技术	/292
7.3.7	软件逆向工程	/294
7.3.8	软件破解小结	/296
7.4	反跟踪技术	/297
7.5	数字版权管理	/301
	本章小结	/305
	习题 7	/306

第 8 章 黑客 /307

8.1	黑客概述	/307
8.1.1	黑客概念	/307
8.1.2	黑客攻击的一般过程	/308
8.1.3	黑客攻击分类	/310
8.1.4	黑客常用命令	/310
8.2	信息收集	/313
8.2.1	查询	/313
8.2.2	网络嗅探与监听	/314
8.2.3	扫描	/319
8.2.4	查点	/320
8.3	入侵类攻击	/321
8.3.1	口令攻击	/321
8.3.2	缓冲区溢出攻击	/324
8.3.3	格式化字符串攻击	/329
8.4	权限提升	/331
8.5	欺骗类攻击	/332
8.5.1	IP 欺骗	/332

8.5.2	TCP 会话劫持	/334
8.5.3	ARP 欺骗	/335
8.5.4	DNS 欺骗	/336
8.5.5	Web 欺骗	/338
8.6	拒绝服务类攻击	/339
8.6.1	几种典型的拒绝服务攻击	/339
8.6.2	分布式拒绝服务	/341
8.7	植入木马	/343
8.8	网络钓鱼	/344
	本章小结	/345
	习题 8	/346

第 9 章 数据库安全 /348

9.1	数据库系统简介	/348
9.1.1	数据库概念	/348
9.1.2	数据库系统体系结构	/349
9.1.3	关系数据库管理系统	/350
9.1.4	联机分析处理	/353
9.1.5	数据挖掘	/354
9.2	数据库安全概述	/356
9.2.1	数据库安全定义	/356
9.2.2	数据库的安全需求	/357
9.2.3	数据库系统安全基本原则	/358
9.2.4	数据库安全策略	/359
9.2.5	数据库系统的威胁	/359
9.3	数据库管理系统安全	/360
9.3.1	数据库的访问控制	/361
9.3.2	事务并发控制	/361
9.3.3	关系数据库的授权机制	/363
9.3.4	审计与日志	/364
9.3.5	备份与恢复	/364
9.3.6	多级安全数据库	/365
9.4	数据库的数据安全	/366

9.4.1	完整性约束	/366
9.4.2	数据库的数据加密	/368
9.4.3	敏感数据与推理	/370
9.4.4	敏感数据保护	/376
9.4.5	数据库的隐私保护	/377
9.5	数据库应用系统安全	/384
9.5.1	数据库角色与权限	/384
9.5.2	SQL 注入攻击	/387
9.5.3	数据库木马防范	/390
9.5.4	数据库安全漏洞	/391
9.5.5	数据库的安全配置管理	/393
	本章小结	/395
	习题 9	/396

第 10 章 防火墙技术 /397

10.1	防火墙概述	/397
10.1.1	防火墙概念	/397
10.1.2	防火墙的功能	/397
10.1.3	防火墙特点	/398
10.1.4	防火墙分类	/399
10.1.5	防火墙的发展简史与趋势	/399
10.2	防火墙的基本体系结构	/400
10.3	防火墙技术	/404
10.3.1	包过滤技术	/404
10.3.2	网络地址翻译技术	/407
10.3.3	网络代理技术	/409
10.4	物理隔离技术——网闸	/411
10.4.1	物理隔离部件	/412
10.4.2	物理隔离部件的功能 与特点	/413
10.4.3	物理隔离应用系统	/414
10.5	防火墙的配置与管理	/415
10.5.1	硬件防火墙的配置与管理	/415

- 10.5.2 基于主机的软件防火墙
配置 /420

本章小结 /421

习题 10 /423

第 11 章 入侵检测与防御 /425

- 11.1 入侵检测技术概述 /425
- 11.2 入侵检测原理与技术 /429
 - 11.2.1 入侵检测原理 /429
 - 11.2.2 入侵检测分析技术 /432
 - 11.2.3 入侵检测方法 /433
 - 11.2.4 入侵检测模型 /436
 - 11.2.5 入侵检测响应系统 /438
- 11.3 入侵检测的实现 /439
- 11.4 蜜罐技术 /444
- 11.5 入侵检测系统的部署和产品 /446
 - 11.5.1 IDS 部署 /446
 - 11.5.2 入侵检测系统产品 /446
 - 11.5.3 入侵检测产品的评估 /448
 - 11.5.4 入侵检测系统实例——
Snort /448
- 11.6 入侵防御系统 /450
 - 11.6.1 入侵防御系统的由来 /451
 - 11.6.2 入侵防御系统原理 /451
 - 11.6.3 基于网络的入侵防御系统 /452
 - 11.6.4 基于主机的入侵防御系统 /453
 - 11.6.5 IPS 与 IDS 比较 /454

本章小结 /456

习题 11 /457

第 12 章 数字取证技术 /458

- 12.1 计算机犯罪 /458
- 12.2 计算机电子证据 /460

12.3	计算机取证	/463
12.3.1	计算机取证定义	/463
12.3.2	计算机取证模型	/463
12.3.3	计算机取证的主要原则	/464
12.3.4	计算机取证的基本步骤	/465
12.4	计算机取证相关技术	/467
12.4.1	电子数据获取基本知识	/467
12.4.2	电子数据采集	/470
12.4.3	动态取证	/478
12.4.4	实时取证	/479
12.4.5	事后取证	/481
12.5	电子证据分析	/481
12.5.1	日志证据分析	/481
12.5.2	电子证据来源分析与鉴定	/484
12.6	计算机取证工具	/486
12.6.1	用于数据获取的取证工具	/486
12.6.2	用于数据分析的取证工具	/487
12.7	反取证技术	/488
	本章小结	/488
	习题 12	/489

参考文献	/490
------	------

第 1 章 计算机网络安全概述

1.1 信息系统与信息安全

1.1.1 信息化及信息系统

1. 信息与信息化

“信息”一词在英文、法文、德文、西班牙文中均是“information”，日文中为“情报”，我国台湾称之为“资讯”，我国古代用的是“消息”。20 世纪 40 年代，香农(C. E. Shannon)给出了信息的明确数学定义：信息是用以消除随机不确定性的东西(信息是肯定性的确认；确定性的增加)，并提出信息量的概念和信息熵的计算方法，从而奠定了信息论的基础。这一定义被人们视为经典性定义并加以引用。

控制论创始人维纳(Norbert Wiener)认为“信息是人们在适应外部世界，并使这种适应反作用于外部世界的过程中，同外部世界进行互相交换的内容和名称”。它也被作为经典性定义加以引用。我国著名的信息学专家钟义信教授认为“信息是事物存在方式或运动状态，以这种方式或状态直接或间接的表述”。美国信息管理专家霍顿(F. W. Horton)给信息下的定义是：“信息是为了满足用户决策的需要而经过加工处理的数据。”简单地说，信息是经过加工的数据，或者说信息是数据处理的结果。

根据近年来人们对信息的研究成果，科学的信息概念可以概括为：信息是对客观世界中各种事物的运动状态和变化的反映，是客观事物之间相互联系和相互作用的表征，表现的是客观事物运动状态和变化的实质内容。

信息是资源和财富。信息化的程度已经成为衡量一个国家或企业综合技术水平、综合能力的主要标志。从全球范围来看，发展信息技术和发展信息产业也是当今竞争的一个制高点。信息技术和信息产业正在改变人们传统的生产、经营和生活方式，信息已成为社会发展的重要战略资源。

林毅夫等指出：“所谓信息化，是指建立在 IT 产业发展与 IT 在社会经济各部门扩散的基础之上，运用 IT 改造传统的经济、社会结构的过程”。

信息化在改变社会、促进发展的同时，给国家的安全也带来了挑战，常规武器、核武器等离开了信息的精确制导，也就变成了瞎子，因此现代战争中出现了争夺信息控制权的信息战。下面是一些名人对信息化的评价。

美国著名未来学家阿尔温·托尔勒：“谁掌握了信息，控制了网络，谁将拥有整个世界。”

美国前总统克林顿：“今后的时代，控制世界的国家将不是靠军事，而是信息能力走在前面的国家。”

江泽民：“信息革命是人类第三次生产力的革命，四个现代化，哪一化也离不开信息化。”