

Information

Information

Information

Security

Security

Information

Security

🔒 高等学校信息安全专业“十二五”规划教材

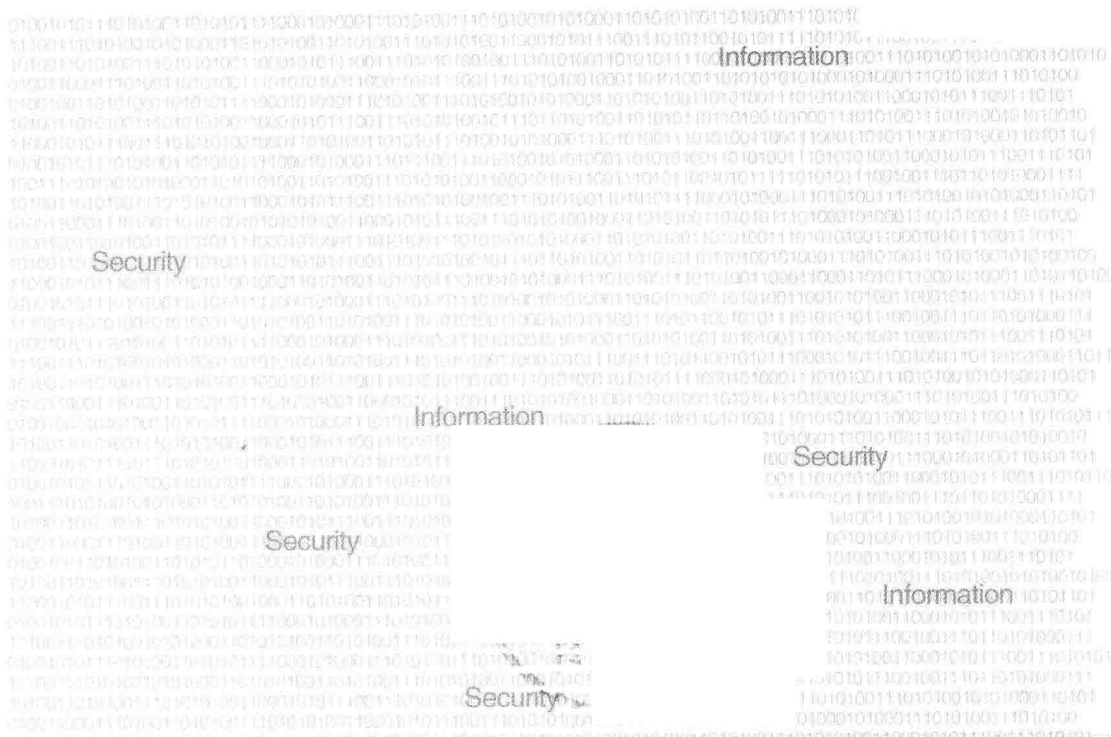
彭国军 傅建明 梁玉 编著

# 软件安全



WUHAN UNIVERSITY PRESS

武汉大学出版社



🔒 高等学校信息安全专业“十二五”规划教材

# 软件安全

彭国军 傅建明 梁玉 编著  
张焕国 审校



WUHAN UNIVERSITY PRESS  
武汉大学出版社

## 图书在版编目(CIP)数据

软件安全/彭国军,傅建明,梁玉编著. —武汉:武汉大学出版社,2015.9  
高等学校信息安全专业“十二五”规划教材  
ISBN 978-7-307-16496-3

I. 软… II. ①彭… ②傅… ③梁… III. 软件开发—安全技术—高等学校—教材 IV. TP311.52

中国版本图书馆 CIP 数据核字(2015)第 186904 号

责任编辑:林 莉 责任校对:汪欣怡 版式设计:马 佳

---

出版发行:武汉大学出版社 (430072 武昌 珞珈山)  
(电子邮件:cbs22@whu.edu.cn 网址:www.wdp.com.cn)

印刷:湖北金海印务有限公司

开本:787×1092 1/16 印张:20.75 字数:525千字 插页:!

版次:2015年9月第1版 2015年9月第1次印刷

ISBN 978-7-307-16496-3 定价:45.00元

---

版权所有,不得翻印;凡购买我社的图书,如有质量问题,请与当地图书销售部门联系调换。

## 高等学校信息安全专业“十二五”规划教材

### 编委会

---

#### 主任:

沈昌祥 (中国工程院院士, 教育部高等学校信息安全类专业教学指导委员会主任, 武汉大学兼职教授)

---

#### 副主任:

蔡吉人 (中国工程院院士, 武汉大学兼职教授)

刘经南 (中国工程院院士, 武汉大学教授)

肖国镇 (西安电子科技大学教授, 武汉大学兼职教授)

---

#### 执行主任:

张焕国 (教育部高等学校信息安全类专业教学指导委员会副主任, 武汉大学教授)

---

#### 编委 (主任、副主任名单省略):

冯登国 (教育部高等学校信息安全类专业教学指导委员会副主任, 信息安全国家重点实验室研究员, 武汉大学兼职教授)

卿斯汉 (北京大学教授, 武汉大学兼职教授)

吴世忠 (中国信息安全产品测评中心研究员, 武汉大学兼职教授)

朱德生 (中国人民解放军总参谋部通信部研究员, 武汉大学兼职教授)

谢晓尧 (贵州师范大学教授)

黄继武 (教育部高等学校信息安全类专业教学指导委员会委员, 中山大学教授)

马建峰 (教育部高等学校信息安全类专业教学指导委员会委员, 西安电子科技大学教授)

秦志光 (教育部高等学校信息安全类专业教学指导委员会委员, 电子科技大学教授)

刘建伟 (教育部高等学校信息安全类专业教学指导委员会委员, 北京航空航天大学教授)

韩臻 (教育部高等学校信息安全类专业教学指导委员会委员, 北京交通大学教授)

张宏莉 (教育部高等学校信息安全类专业教学指导委员会委员, 哈尔滨工业大学教授)

覃中平 (华中科技大学教授, 武汉大学兼职教授)

俞能海 (中国科技大学教授)

徐明 (国防科技大学教授)

贾春福 (南开大学教授)

石文昌 (中国人民大学教授)

何炎祥 (武汉大学教授)

王丽娜 (武汉大学教授)

杜瑞颖 (武汉大学教授)



# 前 言

软件是计算机系统的灵魂、信息化的核心以及互联网应用的基石。现代社会对信息系统的依赖主要体现为对软件的依赖，而且信息系统的缺陷在很大程度上也是因为软件问题产生的。

目前，软件安全正面临严峻挑战。一方面，随着软件规模的不断增大，软件的开发、集成和演化变得越来越复杂，这导致软件产品在推出时总会含有很多已知或未知的缺陷，这些缺陷对软件系统安全的可靠运行构成了严重的威胁。另一方面，软件的运行和开发环境从传统的静态封闭状态演变成互联网环境下动态开放的状态，越来越多的软件漏洞和缺陷被发现。更为重要的是，受经济利益驱使，目前计算机病毒及黑客地下产业链活动非常猖獗，软件漏洞被广泛利用，恶意代码急剧增加，且传播速度大大加快，另外 APT（Advanced Persistent Threat，高级可持续性威胁）攻击活动不断，攻击手段防不胜防，触及国家关键基础设施和各类重要信息系统，其对我国网络空间安全甚至国家安全形成了巨大威胁。

为了进一步增强学生对目前软件安全所面临的各类威胁的本质与其实现机理的理解，促使学生掌握目前系统安全防护领域的各类核心技术与理论，以提升学生的实践创新能力和学生综合利用专业基础知识来设计和研发信息安全防护产品的能力，我们编写了本教材。同时，希望借此可为学生今后的发展提供一定的专业引导，进一步激发学生的专业兴趣，增强学生的专业使命感，期盼越来越多的优秀人才投入到我国的网络空间安全事业中来，为我国的网络空间安全保障不断添砖加瓦。

本书第一部分对软件安全的基础知识进行了介绍。

其中，第 1 章从信息的概念入手，介绍了信息、信息安全的定义、属性、发展，进而描述了软件安全的概念、面临的具体威胁和来源，最后对目前典型的软件安全防护手段进行了介绍。通过本章的学习，读者将能较全面了解软件安全的基本概念、其面临的主要问题和挑战，以及目前典型的安全防护手段。

软件安全涉及较多的计算机基础知识，如磁盘结构、文件系统、CPU、内存管理、操作系统、文件格式等。第 2 章介绍了计算机的磁盘管理、Windows 的文件系统、处理器的工作模式、Windows 内存结构与管理、计算机的引导过程、EXE 文件格式等与软件安全相关基础知识。该章将为读者继续学习后续各章的专业知识打下必要的基础。

本书第二部分对软件安全的重要威胁之一“软件漏洞”的机理、利用方法与防护技术手段进行了讲解和分析。

第 3 章重点阐述了软件漏洞的概念、分类及其对系统的具体威胁，同时分析了软件漏洞产生的具体原因，攻击者利用软件漏洞的具体方式，最后还对一部分典型的软件漏洞进行了介绍。

第 4 章对两类典型的软件漏洞（缓冲区溢出漏洞及 Web 类漏洞）进行了具体的机理分析。

第5章描述了软件漏洞的具体利用方法,包括 Exploit 与 ShellCode 的编写机理,同时对软件漏洞利用的平台和框架进行了介绍,最后还对软件漏洞挖掘技术及工具进行了介绍。

第6章对微软在 Windows 系统中针对漏洞利用的典型防护手段和机制进行了介绍,包括数据执行保护 (DEP)、栈溢出检查 (GS)、地址空间分布随机化 (ASLR) 及 SafeSEH 等。通过本章的学习,可以掌握目前操作系统在漏洞防护方面的一些具体措施,同时还能够了解攻击者与操作系统在漏洞攻防方面的博弈过程。

针对目前存在的各类软件安全问题,第7章基于软件开发的整个过程介绍了安全软件设计的具体流程和方法。

恶意软件是软件安全的重大安全隐患。作为本书内容的重中之重,第三部分重点讲解和分析了恶意代码的攻防技术与手段。

其中,第8章介绍了恶意代码的定义及具体分类,第9章重点详细地介绍了几类典型的恶意代码(包括计算机病毒、网络蠕虫、木马、Rootkit,以及手机恶意软件等)的具体实现机理。

第10章主要描述了目前流行的各类反病毒技术和手段。本章对特征值检测技术、校验和检测技术、虚拟机检测技术、启发式扫描技术、主动防御技术及云查杀技术等进行了介绍,接着讲解了恶意软件的部分针对性自我保护方法。

第11章重点介绍了恶意软件的样本捕获与分析手段,包括恶意样本的捕获方法,样本分析环境的搭建,以及恶意软件的分析手段等。

本书第四部分对软件的知识产权与自我保护手段进行了讲解。

其中,第12章介绍了软件知识产权验证及保护的具体手段和机制,第13章介绍了软件的自我保护技术,包括反静态分析、反动态调试以及软件的自校验技术。

在本书编写过程中,我们从各种学术论文、书籍、期刊以及互联网中引用了大量的资料,有的在参考文献中列出,有的无法一一查证,在此特别感谢这些文献作者的贡献。

在本书的编著过程中,郑美凤、王丹、叶青晟、周源、万开、张志峰、许静、郑祎、周英骥、郭颖、鲁雄锋、王滢、李晶雯及邵玉如等同学进行了本书部分章节的资料收集、文字整理及校对工作,在此向他们表示感谢。

另外,在“软件安全”课程建设和教材编写的过程中,得到了 Intel 公司的支持,同时,在网易云课堂平台的支持下,与本教材配套的视频课程已顺利上线,在此向他们表示感谢。

由于时间和水平有限,难免存在部分错误,恳请读者批评指正,以使本书得以不断改进和完善。

作者

2015年6月



## 目 录

## 第一部分 软件安全基础知识

<b>第 1 章 软件安全概述</b> .....	3
1.1 信息与信息安全 .....	3
1.1.1 信息的定义 .....	3
1.1.2 信息的属性 .....	3
1.1.3 信息安全 .....	4
1.2 什么是软件安全 .....	5
1.3 软件安全威胁及其来源 .....	5
1.3.1 软件缺陷与漏洞 .....	5
1.3.2 恶意软件 .....	6
1.3.3 软件破解 .....	8
1.4 如何加强软件安全防护? .....	8
本章小结 .....	12
习题 .....	12
<b>第 2 章 软件安全基础</b> .....	13
2.1 计算机磁盘的管理 .....	13
2.1.1 硬盘结构简介 .....	13
2.1.2 主引导扇区 (Boot Sector) 结构简介 .....	15
2.1.3 文件系统 .....	16
2.2 80X86 处理器的工作模式 .....	20
2.2.1 实模式 .....	21
2.2.2 保护模式 .....	21
2.2.3 虚拟 8086 模式 .....	21
2.3 Windows 内存结构与管理 .....	22
2.3.1 DOS 内存布局 .....	22
2.3.2 Windows 的内存布局 .....	22
2.3.3 虚拟地址转译 .....	24
2.3.4 内存分配与管理函数 .....	25
2.4 计算机的引导过程 .....	28
2.4.1 认识计算机启动过程 .....	28



2.4.2 主引导记录的工作原理 .....	29
2.5 PE 文件格式 .....	34
2.5.1 什么是 PE 文件格式 .....	34
2.5.2 PE 文件格式与 Win32 病毒的关系 .....	34
2.5.3 PE 文件格式分析 .....	35
本章小结 .....	47
习题 .....	47

## 第二部分 软件漏洞利用与防护

第 3 章 软件缺陷与漏洞机理概述 .....	51
3.1 安全事件与软件漏洞 .....	51
3.1.1 典型安全事件 .....	51
3.1.2 软件漏洞 .....	52
3.2 漏洞分类及其标准 .....	53
3.2.1 漏洞分类 .....	53
3.2.2 CVE 标准 .....	54
3.2.3 CNVD .....	54
3.2.4 CNNVD .....	54
3.3 软件漏洞利用对系统的威胁 .....	54
3.3.1 非法获取访问权限 .....	55
3.3.2 权限提升 .....	55
3.3.3 拒绝服务 .....	55
3.3.4 恶意软件植入 .....	55
3.3.5 数据丢失或泄漏 .....	56
3.4 软件漏洞产生的原因 .....	56
3.4.1 技术因素 .....	56
3.4.2 非技术因素 .....	58
3.5 软件漏洞利用方式 .....	60
3.5.1 本地攻击模式 .....	60
3.5.2 远程主动攻击模式 .....	60
3.5.3 远程被动攻击模式 .....	61
3.6 典型的软件漏洞 .....	61
3.6.1 缓冲区溢出 .....	61
3.6.2 注入类漏洞 .....	62
3.6.3 权限类漏洞 .....	63
本章小结 .....	64
习题 .....	64



<b>第 4 章 典型软件漏洞机理分析</b> .....	65
4.1 缓冲区溢出漏洞 .....	65
4.1.1 缓冲区与内存分布 .....	66
4.1.2 栈溢出 .....	67
4.1.3 堆溢出 .....	73
4.1.4 格式化串漏洞 .....	80
4.2 Web 应用程序漏洞 .....	82
4.2.1 Web 应用安全概述 .....	82
4.2.2 SQL 注入漏洞 .....	83
4.2.3 跨站脚本 (XSS) .....	87
4.2.4 跨站请求伪造 (CSRF) .....	90
4.2.5 其他 Web 漏洞 .....	91
本章小结 .....	93
习题 .....	93
<b>第 5 章 软件漏洞的利用和发现</b> .....	95
5.1 漏洞利用与 Exploit .....	95
5.1.1 漏洞利用简介 .....	95
5.1.2 Exploit 结构 .....	96
5.1.3 漏洞利用的具体技术 .....	96
5.2 Shellcode 开发 .....	97
5.2.1 Shellcode 的编写语言 .....	98
5.2.2 地址重定位技术 .....	98
5.2.3 API 函数自搜索技术 .....	98
5.2.4 Shellcode 编码问题 .....	102
5.2.5 Shellcode 典型功能 .....	102
5.2.6 改进 Shellcode 技术——Ret2Lib 和 ROP .....	103
5.3 软件漏洞利用平台及框架 .....	106
5.3.1 Metasploit Framework .....	106
5.3.2 Immunity CANVAS .....	107
5.4 软件漏洞挖掘技术及工具 .....	107
5.4.1 基于源代码的静态分析 .....	108
5.4.2 静态分析工具 .....	109
5.4.3 动态分析 .....	110
5.4.4 Fuzzing 测试 .....	111
5.4.5 面向二进制程序的逆向分析 .....	112
5.4.6 基于补丁比对的逆向分析 .....	113
本章小结 .....	113
习题 .....	113

<b>第 6 章 Windows 系统安全机制及漏洞防护技术</b> .....	116
6.1 数据执行保护——DEP .....	116
6.1.1 DEP 保护机制 .....	116
6.1.2 对抗 DEP .....	117
6.2 栈溢出检查——GS .....	120
6.2.1 /GS 保护机制的原理的实现 .....	120
6.2.2 GS 的不足 .....	122
6.3 地址空间分布随机化——ASLR .....	124
6.3.1 ASLR 保护机制的原理和实现 .....	124
6.3.2 ASLR 的缺陷和绕过方法 .....	126
6.4 SafeSEH .....	127
6.4.1 SafeSEH 的原理和实现 .....	127
6.4.2 SafeSEH 的安全性分析 .....	128
6.5 EMET .....	129
本章小结 .....	129
习题 .....	130
<b>第 7 章 构建安全的软件</b> .....	131
7.1 系统的安全需求 .....	131
7.2 主动的安全开发过程 .....	132
7.2.1 安全教育阶段 .....	133
7.2.2 设计阶段 .....	133
7.2.3 开发阶段 .....	136
7.2.4 测试阶段 .....	136
7.2.5 发行和维护阶段 .....	137
7.3 重要的安全法则 .....	137
7.3.1 软件安全策略 .....	137
7.3.2 安全设计法则 .....	138
7.4 安全的编码技术 .....	140
7.4.1 安全编码 .....	140
7.4.2 安全性测试 .....	142
7.5 适当的访问控制 .....	145
7.5.1 访问控制 .....	145
7.5.2 访问控制策略 .....	146
7.5.3 访问控制的实现 .....	147
7.5.4 授权 .....	147
7.5.5 审计 .....	148
本章小结 .....	148
习题 .....	148



### 第三部分 恶意代码机理及防护

<b>第 8 章 恶意代码及其分类</b> .....	153
8.1 恶意代码定义 .....	153
8.2 恶意代码分类 .....	153
8.2.1 计算机病毒 .....	153
8.2.2 网络蠕虫 .....	154
8.2.3 特洛伊木马 .....	155
8.2.4 后门 .....	156
8.2.5 Rootkit .....	156
8.2.6 流氓软件 .....	157
8.2.7 僵尸程序 .....	157
8.2.8 Exploit .....	158
8.2.9 其他 .....	158
本章小结.....	159
习题.....	159
<b>第 9 章 恶意代码机理分析</b> .....	160
9.1 计算机病毒 .....	160
9.1.1 什么是计算机病毒 .....	160
9.1.2 计算机病毒的特点与分类 .....	161
9.1.3 计算机病毒的结构 .....	163
9.1.4 计算机病毒的网络传播方式 .....	166
9.2 计算机病毒机理分析 .....	167
9.2.1 Windows PE 病毒 .....	167
9.2.2 脚本病毒 .....	179
9.2.3 宏病毒 .....	184
9.2.4 ELF 类病毒 .....	191
9.3 网络蠕虫 .....	196
9.3.1 软件漏洞与网络蠕虫 .....	196
9.3.2 网络蠕虫的结构.....	199
9.3.3 网络蠕虫攻击的关键技术 .....	201
9.3.4 网络蠕虫的检测与防治 .....	203
9.4 木马 .....	205
9.4.1 什么是木马? .....	205
9.4.2 木马的通信方式与溯源 .....	206
9.4.3 木马的主要功能剖析 .....	210

9.4.4	木马实例——灰鸽子 .....	215
9.4.5	木马与后门的异同 .....	220
9.5	Rootkit .....	220
9.5.1	什么是 Rootkit? .....	220
9.5.2	Rootkit 核心技术分析 .....	221
9.5.3	Rootkit 检测原理及工具 .....	236
9.6	手机恶意软件 .....	237
9.6.1	手机恶意软件概述 .....	237
9.6.2	手机操作系统简介 .....	238
9.6.3	手机恶意软件的种类 .....	240
9.6.4	手机恶意软件主要功能技术机理 .....	243
9.6.5	手机恶意软件的防御 .....	247
	本章小结 .....	247
	习题 .....	247
<b>第 10 章</b>	<b>病毒检测技术及检测对抗技术 .....</b>	<b>249</b>
10.1	病毒检测技术 .....	249
10.1.1	特征值检测技术 .....	249
10.1.2	校验和检测技术 .....	250
10.1.3	虚拟机检测技术 .....	252
10.1.4	启发式扫描技术 .....	254
10.1.5	主动防御技术 .....	258
10.1.6	云查杀技术 .....	260
10.2	恶意软件的自我保护 .....	262
10.2.1	病毒检测技术对抗 .....	262
10.2.2	反病毒软件对抗 .....	267
10.2.3	人工分析对抗 .....	268
	本章小结 .....	272
	习题 .....	273
<b>第 11 章</b>	<b>恶意软件样本捕获与分析 .....</b>	<b>275</b>
11.1	恶意软件样本捕获方法 .....	275
11.1.1	蜜罐 .....	275
11.1.2	用户上报 .....	275
11.1.3	云查杀平台上传 .....	276
11.1.4	诱饵邮箱 .....	276
11.1.5	样本交流 .....	276
11.2	恶意软件载体 .....	276



11.3 恶意软件样本分析 .....	277
11.3.1 虚拟机环境准备 .....	278
11.3.2 系统监控 .....	278
11.3.3 文件类型侦测 .....	283
11.3.4 PE 文件格式分析 .....	283
11.3.5 静态反汇编 .....	284
11.3.6 动态调试 .....	285
11.3.7 文本及 16 进制数据分析 .....	286
11.4 恶意软件分析报告 .....	287
本章小结 .....	290
习题 .....	290
<b>第四部分 软件自我保护</b>	
<b>第 12 章 软件知识产权保护技术 .....</b>	<b>295</b>
12.1 软件知识产权保护的必要性 .....	295
12.2 用户合法性验证机制 .....	295
12.2.1 序列号验证 .....	295
12.2.2 KeyFile 验证 .....	297
12.2.3 网络验证 .....	298
12.2.4 光盘验证技术 .....	298
12.2.5 加密锁验证 .....	298
12.3 软件知识产权保护方式 .....	299
12.3.1 功能限制 .....	299
12.3.2 时间限制 .....	300
12.3.3 警告窗口 .....	301
12.4 软件知识产权保护建议 .....	302
本章小结 .....	303
习题 .....	304
<b>第 13 章 软件自我保护技术 .....</b>	<b>305</b>
13.1 静态分析对抗技术 .....	305
13.1.1 花指令 .....	305
13.1.2 自修改代码技术实现 .....	308
13.1.3 加密与多态变形技术 .....	308
13.1.4 虚拟机保护技术 .....	309
13.2 动态分析对抗技术 .....	310
13.2.1 检测自身是否处于调试状态 .....	310



13.2.2 检测调试器软件是否存在 .....	312
13.2.3 发现调试器后的处理 .....	313
13.3 软件的自校验技术 .....	314
13.3.1 磁盘文件校验 .....	314
13.3.2 内存映像校验 .....	314
本章小结 .....	315
习题 .....	315
参考文献 .....	316

第一部分



软件安全基础知识







# 第1章 软件安全概述



## 1.1 信息与信息安全

### 1.1.1 信息的定义

“信息”一词有着很悠久的历史，早在两千多年前的西汉，即有“信”字的出现。“信”常可作消息来理解。

信息是信息论中的一个重要术语，人们常常把消息中有意义的内容称为信息，或者说有价值的消息即为信息。

1948年，美国数学家、信息论的创始人香农(C. E. Shannon)在题为《通讯的数学理论》的论文中指出：“信息是用来消除随机不定性的东西。”1948年，美国著名数学家、控制论的创始人维纳(N. Wiener)在《控制论》一书中，指出：“信息就是信息，既非物质，也非能量。”

以下是一些关于信息的描述和定义：

- 信息是主体相对于客体的变化。
- 信息是确定性的增加。
- 信息是事物现象及其属性标识的集合。
- 信息是反映客观世界中各种事物特征和变化的知识，是数据加工的结果，信息是有用的数据。
  - 信息以物质介质为载体，传递和反映世界各种事物存在的方式和运动状态的表征。
  - 信息(Information)是物质运动规律总和，信息不是物质，也不是能量！
  - 信息作为一种资源，它的普遍性、共享性、增值性、可处理性和多效用性，使其对于人类具有特别重要的意义。

虽然关于信息的定义很多，但我们可以总结出信息的一个重要特征：价值，即其可用来消除不确定性。

目前，信息已经成为一种资产，与其他类别的业务资产一样，其对于组织和个人来说都是不可或缺的，因此要妥加保管。

信息可以以多种形式表现，可以打印或书写在纸上，也可以以电子数据的方式存储，通过邮寄或电子邮件方式传播，或以胶片形式显示或者通过交谈表达出来。总之，信息无处不在。

### 1.1.2 信息的属性

信息是具有价值的，而其价值则是通过其具体属性来体现的。以下是人们通常最关注的