



Denial of Service (DoS) Attack

拒绝服务攻击



李德全 著



电子工业出版社
PUBLISHING HOUSE OF ELECTRONICS INDUSTRY
<http://www.phei.com.cn>

电子信息科技专著出版专项资金资助出版

安全技术
大系

TP393.08

180

2007

Denial of Service (DoS) Attack

拒绝服务 攻击

李德全 著

国家自然科学基金资助项目 (项目编号: 60273027)

国家杰出青年基金资助项目 (项目编号: 60025205)

电子工业出版社

Publishing House of Electronics Industry

北京·BEIJING

内 容 简 介

随着网络技术和网络应用的发展，网络安全问题显得越来越重要。拒绝服务攻击由于容易实施、难以防范、难以追踪等特点而成为最难解决的网络安全问题之一，给网络社会带来了极大的危害。同时，拒绝服务攻击也将是未来信息战的重要手段之一。因此，了解和研究拒绝服务攻击的原理，探索其对策，从而在日常工作中有效地应对拒绝服务攻击是极为重要的。

本书对拒绝服务攻击的原理进行了较深入的探讨，然后分析了针对拒绝服务攻击的各种对策，包括拒绝服务攻击的防御、检测和追踪等。特别是，作为拒绝服务攻击对策的新方法——数据来源的追踪这一既可为追究法律责任提供证据，又可为其他对策如数据包的过滤、限流等提供及时信息的方法也在本书中做了详细深入的探讨。

本书既有较深的理论研究，又有丰富的实用技术，内容丰富，可供相关领域科研和工程技术人员参考，也可作为相关专业高年级本科生、研究生的网络攻防、防火墙、入侵检测等类课程的教学参考书。

未经许可，不得以任何方式复制或抄袭本书之部分或全部内容。
版权所有，侵权必究。

图书在版编目（CIP）数据

拒绝服务攻击 / 李德全著. —北京：电子工业出版社，2007.1
（安全技术大系）
ISBN 978-7-121-03644-6

I. 拒… II. 李… III. 计算机网络—安全技术 IV. TP393.08

中国版本图书馆 CIP 数据核字（2006）第 153571 号

责任编辑：孙学瑛

印 刷：北京智力达印刷有限公司

装 订：北京中新伟业印刷有限公司

出版发行：电子工业出版社

北京市海淀区万寿路 173 信箱 邮编 100036

开 本：787×980 1/16 印张：24.75 字数：531 千字

印 次：2007 年 1 月第 1 次印刷

印 数：4000 册 定价：49.00 元

凡所购买电子工业出版社图书有缺损问题，请向购买书店调换。若书店售缺，请与本社发行部联系，联系电话：（010）68279077；邮购电话：（010）88254888。

质量投诉请发邮件至 zltz@phei.com.cn，盗版侵权举报请发邮件至 dbqq@phei.com.cn。

服务热线：（010）88258888。

前 言

拒绝服务攻击由于容易实施、难以防范、难以追踪等特点而成为最难解决的网络安全问题之一，给网络社会带来了极大的危害。因为容易实施，即使不懂网络安全，甚至是刚学会使用计算机的人，都可以很容易地利用网上下载的攻击软件发起拒绝服务攻击；而因为难以防范，目前，大多数情况下受害者对拒绝服务攻击仍旧束手无策；又因为可以采用伪造源地址方式进行攻击或者使用傀儡计算机进行攻击，还没有直接有效的方法追踪到真正的攻击者，从而导致责任追究的困难。这些原因导致拒绝服务攻击的案例越来越多，造成的损失越来越大。

同时，拒绝服务攻击的上述特征也为其在军事领域中的应用创造了极为有利的条件，如今拒绝服务攻击业已成为信息战的重要手段之一。

因此研究拒绝服务攻击的原理，探索其对策，对于在日常的工作中有效地应对拒绝服务攻击，在对敌斗争中合理利用拒绝服务攻击以及防御敌对势力的攻击都是极为重要的。

作者根据多年的研究成果和经验，撰写了这本《拒绝服务攻击》，希望能给广大读者提供借鉴和参考。

由于蠕虫也是导致拒绝服务的重要原因之一，因此，出于完整性考虑，笔者在本书中预留了一章专门介绍蠕虫，鉴于中科院软件所的文伟平博士在蠕虫方面有着深入的研究，作者请文博士协助撰写了第 6 章蠕虫攻击及其对策。

需要说明的是，为了读者更好地理解相关攻击技术，我们除讲述攻击的原理外还分析讨论了一些来自 Internet 上的程序实例，这对于读者更好地检测、防御这些攻击是有益的。同时，为了读者理解和应用的方便，我们对一些程序进行了调试并做了一些小的修改。当然，技术本身并没有好与坏之分，好坏之别只在于其使用者——人。因此，本书中介绍的知识 and 技能也是双刃剑，希望读者善用之。特别是本书中介绍的一些攻击演示软件，请读者仅在自己管理的网络环境中进行实验或测试。

作者将在研究拒绝服务攻击和撰写本书过程中所用的一些参考资料一并提供给读者参考（可到 www.broadview.com.cn 网站下载），希望对读者查询相关资料有所帮助。

由于作者水平有限，疏漏之处在所难免，欢迎广大读者批评指正。

作者关于此书内容的研究得到了中科院软件所冯登国老师、苏璞睿博士和中国海洋大学曲海鹏博士等的大力帮助。本书的写作也得到了众多信息安全专家的指导和帮助，特别是中国海洋大学的曲海鹏博士给本书提供了很多有益的建议。本书在出版过程中得到了电子工业出版社各位老师的支持和帮助，特别是得到了电子工业出版社计算机图书事业部主任（总经理）郭立女士的大力支持。在此一并表示感谢。

笔 者

于中科院软件所 信息安全国家重点实验室

2006.11

目 录

第 1 章 引言	1
1.1 计算机网络的迅猛发展	1
1.2 网络安全问题日渐突出	3
1.3 网络安全重要性	5
1.4 网络为什么不安全	5
1.4.1 漏洞产生的原因	6
1.4.2 漏洞多的原因	7
1.4.3 补丁不是万能的	7
1.5 拒绝服务攻击问题的严重性	10
1.6 本书的主要内容及组织	15
参考文献	16
第 2 章 TCP/IP 协议	19
2.1 网络协议及网络的层次结构	19
2.2 ISO/OSI 参考模型	23
2.3 TCP/IP 参考模型及 TCP/IP 协议族	26
2.3.1 TCP/IP 参考模型	26
2.3.2 TCP/IP 协议族	27
2.3.3 OSI 参考模型与 TCP/IP 参考模型对比	30
2.4 IP 协议	31
2.4.1 IP 提供的服务	31
2.4.2 IP 头	32
2.5 TCP、UDP、ICMP 协议	34
2.5.1 TCP 协议	34
2.5.2 UDP 协议	37
2.5.3 ICMP 协议	38

2.6	TCP/IP 协议族的安全缺陷	41
2.6.1	IP 缺陷	42
2.6.2	ARP、RARP 缺陷	43
2.6.3	TCP 序列号预测	44
2.6.4	路由滥用	49
2.7	IP 欺骗	53
	小结	55
	参考文献	55
第 3 章	拒绝服务攻击原理	57
3.1	什么是拒绝服务攻击	57
3.2	拒绝服务攻击的动机	61
3.3	拒绝服务攻击的分类	65
3.3.1	拒绝服务攻击的属性分类法	67
3.3.2	拒绝服务攻击的舞厅分类法	72
3.4	DDoS 攻击的典型过程	77
3.4.1	获取目标信息	78
3.4.2	占领傀儡机和控制台	85
3.4.3	实施攻击	86
	小结	86
	参考文献	86
第 4 章	典型的拒绝服务攻击	89
4.1	剧毒包型 DoS 攻击	90
4.1.1	WinNuke 攻击	90
4.1.2	碎片 (Teardrop) 攻击	93
4.1.3	Land 攻击	104
4.1.4	Ping of death 攻击	108
4.1.5	循环攻击	112
4.2	风暴型 DoS 攻击	113
4.2.1	与风暴型攻击相关的 Internet 的缺陷	115
4.2.2	直接风暴型攻击	116
4.2.3	反射攻击	122

小结	135
参考文献	135
第 5 章 DoS 工具与傀儡网络	138
5.1 DoS 工具分析	138
5.1.1 Trinoo	139
5.1.2 TFN	143
5.1.3 Stacheldraht	145
5.1.4 Shaft	149
5.1.5 TFN2K	152
5.1.6 Trinity	153
5.1.7 Mstream	153
5.1.8 Jolt2	155
5.1.9 Agobot	161
5.1.10 DDoS 攻击者	161
5.2 傀儡网络	164
5.2.1 什么是傀儡网络	164
5.2.2 傀儡网络的危害	169
5.2.3 傀儡网络的工作原理	171
5.2.4 以傀儡网络为平台的一些攻击实现	174
5.3 拒绝服务攻击的发展趋势	177
5.3.1 攻击程序的安装	177
5.3.2 攻击程序的利用	178
5.3.3 攻击的影响	179
小结	180
参考文献	180
第 6 章 蠕虫攻击及其对策	184
6.1 蠕虫的历史和研究现状	184
6.1.1 蠕虫的历史	184
6.1.2 目前研究概况	189
6.2 蠕虫的功能结构	190
6.2.1 蠕虫的定义	190

6.2.2	蠕虫与病毒的区别	190
6.2.3	网络蠕虫的功能结构	192
6.3	蠕虫的常见传播策略	194
6.4	蠕虫的常见传播模型	196
6.4.1	简单传播模型	197
6.4.2	Kermack-Mckendrick 模型	198
6.4.3	SIS 模型	199
6.4.4	双因子模型	199
6.4.5	BCM 模型——网络蠕虫对抗模型	200
6.5	蠕虫的攻击手段	204
6.5.1	缓冲区溢出攻击	204
6.5.2	格式化字符串攻击	211
6.5.3	拒绝服务攻击	216
6.5.4	弱口令攻击	216
6.5.5	默认设置脆弱性攻击	216
6.5.6	社交工程攻击	217
6.6	蠕虫的检测与防范	217
6.6.1	基于单机的蠕虫检测	217
6.6.2	基于网络的蠕虫检测	221
6.6.3	其他	223
	小结	230
	参考文献	230
第 7 章	拒绝服务攻击的防御	234
7.1	拒绝服务攻击的终端防御	235
7.1.1	增强容忍性	235
7.1.2	提高主机系统或网络安全性	238
7.1.3	入口过滤	241
7.1.4	基于追踪的过滤	243
7.1.5	基于跳数的过滤	249
7.2	拒绝服务攻击的源端防御	254
7.2.1	出口过滤	255
7.2.2	D-WARD	258

7.2.3	COSSACK	261
7.3	拒绝服务攻击的中端防御	262
7.4	傀儡网络与傀儡程序的检测与控制	263
7.4.1	傀儡网络的发现	264
7.4.2	傀儡网络的控制	267
7.4.3	防止傀儡程序的植入	269
7.4.4	以工具检测与清除傀儡程序	270
7.4.5	傀儡程序的手工清除	274
	小结	277
	参考文献	277
第 8 章	拒绝服务攻击的检测	281
8.1	主机异常现象检测	283
8.2	主机网络连接特征检测	285
8.3	伪造数据包的检测	285
8.3.1	基于主机的主动检测	285
8.3.2	基于主机的被动检测	288
8.4	统计检测	290
8.5	SYN 风暴检测	290
	小结	294
	参考文献	294
第 9 章	拒绝服务攻击的追踪	295
9.1	拒绝服务攻击的追踪问题	296
9.1.1	网络追踪的定义	296
9.1.2	网络追踪 (Network TraceBack) 与攻击追咎 (Attack Attribute)	296
9.1.3	拒绝服务攻击追踪的重要性	297
9.2	包标记	297
9.3	日志记录	298
9.4	连接测试	300
9.5	ICMP 追踪 (iTrace)	301
9.6	覆盖网络 (Centertrack)	302
	小结	305

参考文献	305
第 10 章 基于包标记的追踪	308
10.1 基本包标记	308
10.2 基本包标记的分析	314
10.2.1 误报和计算复杂性	314
10.2.2 不公平概率以及最弱链	315
10.2.3 短路径伪造	316
10.2.4 按比特穿插	317
10.2.5 攻击者对基本包标记的干扰“攻击”	320
10.3 高级包标记和带认证的包标记	321
10.4 基于代数编码的包标记	323
10.5 基本包标记的进一步改进	326
小结	328
参考文献	328
第 11 章 基于路由器编码的自适应包标记	330
11.1 自适应包标记	330
11.1.1 固定概率标记的分析	331
11.1.2 自适应标记	332
11.1.3 固定概率标记与自适应标记的比较	338
11.2 路由器的编码	346
11.2.1 编码方案 I	346
11.2.2 编码方案 II	347
11.2.3 编码方案 III	347
11.3 基于路由器编码的标记	348
11.4 几种包标记的比较	355
11.4.1 重构攻击路径所需数据包的数量	355
11.4.2 误报数	357
11.4.3 路径重构时的工作量	360
11.4.4 路由器标记数据包时的工作量	360
11.4.6 可移植性	361
11.5 相关问题	362

11.5.1 拓扑信息服务器	362
11.5.2 攻击树的修剪	363
11.5.3 追踪的部署与实施	365
小结	367
参考文献	368
第 12 章 应对拒绝服务攻击的商业化产品	370
12.1 黑洞	370
12.2 天清防拒绝服务攻击系统	371
12.2.1 算法和体系结构特点	372
12.2.2 使用特点	373
12.2.3 管理功能	373
12.3 冰盾抗 DDOS 防火墙	374
12.3.1 冰盾防火墙采用的安全机制	374
12.3.2 冰盾防火墙的功能特点	375
12.4 Mazu Enforcer	376
12.5 TopLayer	377
小结	378
参考文献	378
附录 A 一些拒绝服务相关网络资源	379

第 1 章 引言

1.1 计算机网络的迅猛发展

在信息技术的推动和牵引下，人类社会已由工业时代迈进信息时代。当前，世界范围的 Internet 网络已得到空前发展并正在日新月异地改变着政治、经济、军事和文化等社会生活的各个方面。由于 Internet 的飞速发展，它早已成为一个覆盖世界的“全球网”。今天，在发达国家自不待言，即使是在中国这样的发展中国家，不仅企事业单位，居民个人上网也在飞速发展中。据中国互联网络信息中心 2005 年 1 月的《中国互联网络发展状况统计报告》[CNNIC0501]，到 2004 年底，在北京、上海这样的政治、经济、文化中心，上网用户数均已超过人口总数的四分之一，即使在西藏、青海、新疆这样的经济相对不是很发达的地区，网民数也已分别达到了本地人口的 2.6%、3.7% 和 6.2%^①。据该中心 2005 年 7 月的同类报告[CNNIC0507]，截止到 2005 年 6 月 30 日，我国的上网计算机总数已达 4560 万台，同半年前的调查结果相比，我国的上网计算机总数半年内增加了 400 万台，增长率为 9.6%，和上年同期相比增长了 25.6%；截止到 2005 年 6 月 30 日，我国的上网用户总人数为 10 300 万人，同半年前的调查相比，我国上网用户总人数半年内增加了 900 万人，增长率为 9.6%，和上年同期相比增长了 18.4%。由此可见，国内的上网计算机数和上网人数都在高速增长，网络对社会生活的影响已逐步深入。图 1.1 和图 1.2 分别为中国国内历年上网计算机数和上网人数统计情况。

^① 其 2005 年 7 月的报告中没有对各省份的类似统计数字，所以我们仅以 2005 年 1 月的报告来说明此问题。

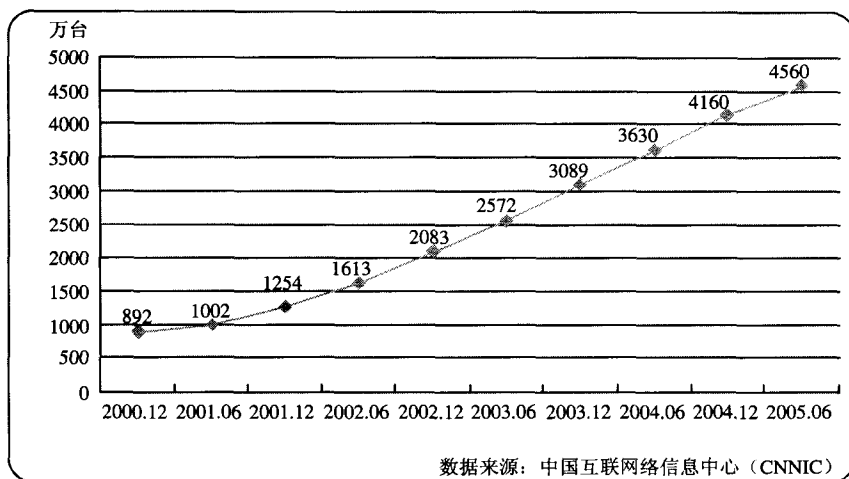


图 1.1 中国国内历年上网计算机数统计

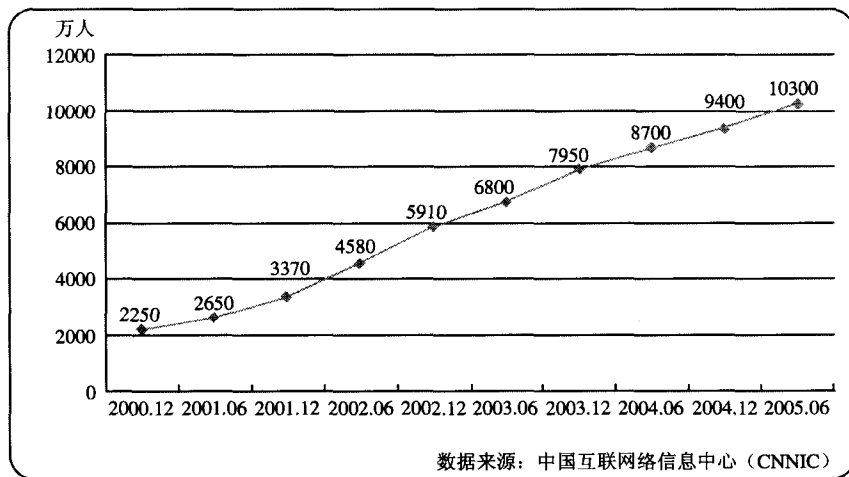


图 1.2 中国国内历年上网人数统计

现在，随着电子商务、电子政务等的发展，我们不仅可以通过网络与远方的朋友即时通信、发送电子邮件，而且，足不出户就可以通过网络购物、付费、接受远程教育、远程医疗服务等。利用由电话线与办公室网络连接的计算机在家中办公已经不再神秘。2003年4、5月间，由于北京 SARS 疫情严重，许多企事业单位都实行轮流值班，没有轮到值班的员工则在家里办公。很多 IT 相关的公司职员尤其体验到了在家办公的好处，那就是既不影响工作，又避免了上下班途中的奔波劳累之苦。世界各国电子商务、电子

政务的发展进一步促进了网络应用的发展。现在，我们对网络的依赖在逐渐增加，特别是对一些年轻的 IT 从业人员和广大“网虫”而言，一旦没有了网络（比如因为停电或者其他原因使网络暂时不可用），就会有不知所措之感。因此，网络已经深入到了我们生活的方方面面，成为生活中不可或缺的东西。

1.2 网络安全问题日渐突出

然而，任何事物都有它的两面性，网络亦然。随着人们越来越依赖于计算机网络，网络安全成为一个摆在我们面前的亟待解决的问题。例如，在 2000 年 2 月的黑客攻击事件中，世界著名的雅虎、亚马逊、微软等公司的网络遭黑客攻击而几近全面瘫痪，直接经济损失高达数十亿美元。CIH 病毒的肆虐、“红色代码”的泛滥等也给人们平静的网络生活掀起了千层波澜。

近年来，网络攻击的数量在逐年上升，从 1998 年到 2003 年，平均年增幅达 50% 左右，如图 1.3 所示^①（数据来源于[CERT_stats]）。为什么会有这么多的网络攻击事件发生呢？一方面，攻击者是有目的的，与其他类型的犯罪一样，计算机攻击的目的既有政治和经济方面的，也有出于报复、炫耀等目的的。另一方面，计算机及其网络的漏洞层出不穷，且新发现的漏洞越来越多，如图 1.4 所示。从图 1.4 中可以看出，历年中，2002 年公布的漏洞数达到顶峰，达 4129 个，2003 年、2004 年在 2002 年的基础上稍有下降，但是 2002~2004 三年间 CERT 平均每天公布的漏洞数都在 10 个以上（数据来源于[CERT_stats]），而到 2005 年，CERT 统计的漏洞数竟然达到 5990 个，平均每天超过 16 个。需要注意的是，CERT 公布的只是其接到报告的，实际发现的漏洞数应该远远超过 CERT 所公布的数字。这些漏洞给了攻击者可乘之机。有了目的，有了可资利用的条件，网络攻击的发生就不足为奇了。

据美国计算机安全研究所（CSI）和联邦调查局（FBI）2002 年关于计算机犯罪和计算机安全的调查报告[CSI02]，在接受调查的 503 家机构中，有 60% 在 2002 年内受到了攻击，其中有 223 家（占 503 家的 44%）量化了他们的经济损失，他们损失的总和达到 45.58 百万美元。据这两家机构 2003 年的同类报告[CSI/FBI03]，在接受调查的 530 家机构中有 75%（398 家）在年内受到了攻击，其中有 251 家（占 530 家的 47%）量化了他们的经济损失，其总和为 20.2 百万美元。据 2004 年的报告，有

^① CERT 提供的此统计数据只到 2003 年，在本书的写作时，未见到 2004 年和 2005 年的统计数据。

269 家机构在一年内因为计算机安全方面的问题导致的经济损失总和达 14 百万美元 [CSI/FBI04]。

由此可见，网络安全问题是多么的严峻。

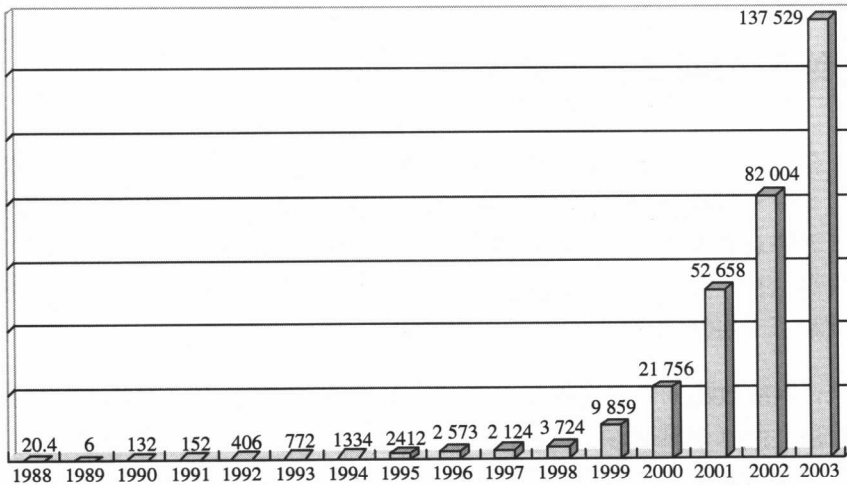


图 1.3 CERT 各年接到的安全事件报告数

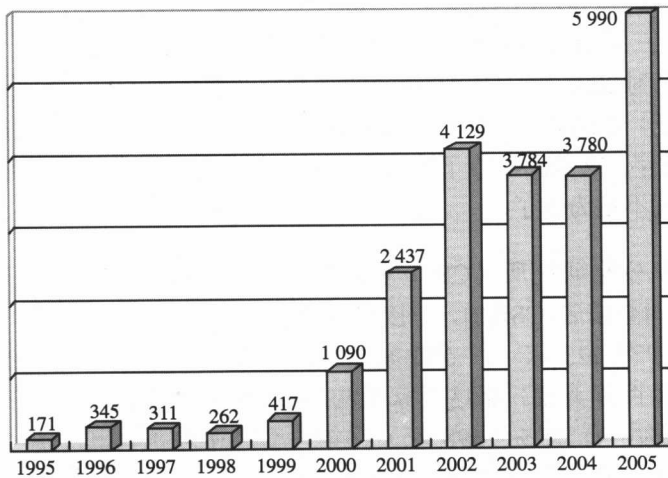


图 1.4 CERT 历年接到的脆弱点（漏洞）报告数

1.3 网络安全重要性

在当今信息社会中，社会经济的发展对信息资源、信息技术和信息产业的依赖程度越来越大，信息已成为人类宝贵的资源。近年来，Internet 正以惊人的速度在全球发展，Internet 技术已经广泛渗透到各个领域。然而，正如我们前面提到的，由 Internet 的发展而带来的网络系统的安全问题，也正变得日益突出，受到越来越多的关注。目前，网络安全已成为关系国家安全的重大战略问题。信息是战略资源，信息是决策资源，是控制战场的灵魂，信息决定火力和机动力。信息可以极大地扩充军队智力和神经（指挥）系统的协调性，军事信息化是一次全面深层次的革命。

信息战的未来战场，争夺网络优势的斗争将会十分激烈。网络是敌对双方借以获取信息优势的制高点，网络攻击与网络防护成为未来军队作战的新模式。网络的出现及其在政治、军事、经济等领域的应用，为军事对抗开辟了一个全新的领域。

网络安全将是 21 世纪军事对抗焦点。网络卫士必将成为新的兵种。美军建立了一个新兵种部队称为计算机网络卫士。网络卫士将广泛编属美国各军兵种和总司令部的直属队，担负着保障各类部队的战略级、战役级和战术级计算机系统及计算机网络应用安全的任务，网络卫士将由网络防窃部队、网络防病毒部队、网络抗毁部队和网络对抗部队组成。

因此，网络安全问题可以说是关系到国家安全、民族存亡的重大问题。因而，研究网络安全的问题是极为重要的。

1.4 网络为什么不安全

通过上述分析，我们知道，网络上时时处处都存在着不安全因素，网络安全形势极为严峻，为什么会这样呢？

现在，在 Internet 上运行着各种各样的软件和各种各样的系统。这些软件和系统中几乎每天都有可供攻击者利用的漏洞被发现。攻击者利用这些漏洞几乎可以为所欲为。那么，这些漏洞又从何而来呢？为什么会有这么多的漏洞呢？