White-Hat 安全手册

——全面解决当前面临的威胁问题

[美] Aviel D. Rubin 著
徐洸 战晓苏 译

Pearson Education
清华大学出版社

White-Hat 安全手册

——全面解决当前面临的威胁问题

[美] Aviel D. Rubin 著

徐 洸 战晓苏 译

清华大学出版社

北 京

北京市版权局著作权合同登记号　图字 01-2002-3038 号

图书在版编目(CIP)数据

White-Hat 安全手册：全面解决当前面临的威胁问题/(美)鲁宾著；徐洸，战晓苏译. —北京：清华大学出版社，2003.8
书名原文：White-Hat Security Arsenal
ISBN 7-302-06430-X

Ⅰ.W...　Ⅱ.①鲁...　②徐...　③战...　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(2003)第 018520 号

出 版 者：清华大学出版社(北京清华大学学研大厦，邮编：100084)
http://www.tup.tsinghua.edu.cn
http://www.tup.com.cn
责任编辑：冯志强
印 刷 者：世界知识印刷厂
发 行 者：新华书店总店北京发行所
开　　本：787×960 1/16　**印张**：16　**字数**：351 千字
版　　次：2003 年 8 月第 1 版　2003 年 8 月第 1 次印刷
书　　号：ISBN 7-302-06430-X/TP·4845
印　　数：0001～3000
定　　价：28.00 元

对 Aviel D. Rubin 编著的《White-Hat 安全手册》的赞扬

"作为一个研究人员，Avi 在许多领域做了极好的工作，并且他还是一个热心的作者。随着 Internet 上问题的大量涌现，复杂又令人容易混淆……本书考虑了许多这方面的问题，分析并提供了很好的解决方案。更重要的是，Avi 提供了执行方案的方法，这些方法也适用于读者将来可能遇到的相关问题……像这样的书是很有帮助的。"

——摘自 William R. Cheswick 的前言

"本书是最具可读性的图书之一，而且它详尽地描述了计算机安全技术至关重要的方面。所有的计算机用户，无论是黑客、IT 专业人员、研究人员还是普通用户，都将从本书获益。本书表达清晰而且行文亲切，这使读者看了很轻松愉快。Rubin 已经对如何识别计算机安全问题以及说明计算机安全的复杂性和微妙性做了大量工作。"

——Jack Goldman 博士，Xerox PARC 的创始人

"本书对当今每个依靠 Internet 的人来说，都是一本非常有价值的工具书。它为读者提供了一个崭新的计算机安全思路，而且，不仅对怎样保护自己做了实际的和最新的指导，还说明如果读者不注意这些问题，将会担心什么。"

——AT&T Labs-Research 的 Matt Blaze 博士

"Avi 的书非常有广度和深度地阐述了计算机安全机制。随着社会的进步，网络将快速地发展。本书帮助读者解决了网络发展所面临的束缚和威胁。"

——Peter G. Neumann 博士，国际 SRI 计算机科学实验室的首席科学家，*Computer-Related Risks* 的作者，ACM Risk 论坛的主席

"Avi Rubin 提供了丰富的资料，并且重点阐述了一些关键问题……我迫不及待地把这本书推荐给公司里以及其他公司负责网络安全的同事。这本书写得非常好，并且提供了许多随时要用到的知识。"

——Sandra Henry-Stocker，系统工程的领导者，E * Trade and Security 的专栏作家，UNIX 的权威

"《White-Hat 安全手册》集知识性和信息性为一体，并且写得非常精彩。它是我所见过

的最具可读性的计算机科学书籍之一。”

——Bruce Davie 博士，Cisco 系统公司职员，
Computer Networks: A Systems Approach 的作者之一

“Avi 的书考察了通常会遇到的安全问题，并且提供了许多计算机威胁的特性以及与 Internet 相连的计算机的弱点。但是，本书提供的绝不仅仅是基本的诊断和处理方法。对网络和安全专家来说，应该从本书学会建立安全模块，以使他们可以充满信心地设计、选择以及实现安全系统和服务。”

——Core Competence 有限公司的 David M. Piscitello

“对希望学习计算机安全的学生和专家来说这是一本极好的书。每一章都研究了一个具体的计算机安全分支。Rubin 简洁地提出了主要的挑战，并且提供了对每个问题的一般性解决方案。整本书都是以许多有娱乐性的现实例子来讨论的。读者可以很快地了解到各种安全问题以及防范措施。总的来说，对于想赶快进入当前计算机安全技术领域的人来说，阅读本书是很好的选择。”

——Dan Boneh 博士，斯坦福大学计算机科学教授

“本书并不是一本普通的网络安全书，它很好地阐述了威胁是什么，它们是如何工作的，手头有什么可以防止它们的工具。本书以讲述病毒、蠕虫以及拒绝服务的攻击开始了计算机安全的历程。最令人感兴趣的是，Rubin 仔细研究了 Morris Worm、Melissa 以及 I Love You 等病毒。他对这些广为流传的病毒的阐述是非常精彩的。这是一本特殊的网络安全书，它是广大读者真正所需要的。”

——Peter H. Salus 博士，Matrix.Net 首席知识官，
A Quarter Century of UNIX and Casting the Net 的作者

献给Ann 和 Elana

是他们给予我生活的意义

译 者 序

随着计算机和网络技术的迅猛发展，个人电脑和网络同人们的生活联系越来越紧密，并逐渐地融入人们的生活、学习和工作之中。随着科学技术的进一步发展，网络一定会成为人们生活不可缺少的一部分。计算机和网络在给人们带来巨大便利的同时，也带来了巨大的困惑，那就是计算机和网络的安全问题。近年来频繁突发黑客攻击，计算机病毒以及网络蠕虫，使安全问题越来越显现其重要性，也越来越引起人们的重视。应该如何使计算机和网络更安全呢？这个问题一直困扰着网络公司，政府部门，金融企业等的管理人员以及计算机安全人员，即使是计算机和网络的普通用户也急切需要解决这个问题。本书正是全面介绍网络安全会出现的问题及其解决方案的。

本书作者 Aviel D. Rubin 博士是一位计算机科学家，是 AT&T Labs-Research 的主要研究人员。他是计算机安全领域广为人知的专家，他还是 USENIX 协会的理事，*Web Security Sourcebook*（John Wiley & Sons, 1997）的作者之一。作为一个 AT&T Labs 的计算机安全问题专家，作者 Avi Rubin 时常与不同类型公司的 IT 人员会面。当被要求向顾客推荐相关资料时，Rubin 才认识到市场上还没有一本可以给他们简洁、直接回答所有网络安全问题的书。所以 Rubin 写了本书。作者是用一种面向问题的方法写书的，这样可以使读者遇到问题后能很方便地查阅。本书共分五部分，第一部分阐明了写本书的动机。在这里没有问题提出来，然而讲述了威胁以及人们为什么会担心计算机安全问题。第二部分讲述了信息安全存储问题。第三部分是最具技术性的，它所要处理的是在易受攻击的网络上安全地传输信息的问题。第四部分讲述的是保护网络安全以免受威胁。这里包括建立防火墙，检测入侵，还提供了对付拒绝服务攻击的方案。第五部分处理了在线商务和个人隐私。这部分内容涉及了诸如在网上使用信用卡、网页浏览等个人服务问题。

本书适合于各类读者。无论专业 IT 人员、系统管理员、学者，还是计算机网络的普通用户，都可以通过阅读本书收益匪浅。本书每一章都针对某个具体问题，读者可以根据自己所遇到的问题选择所要阅读的章节。并且每一章开头都有图标表示适合阅读的读者群，所以很方便读者查阅。虽然本书各部分相互独立，读者可以阅读自己关心的问题，但希望读者能完整地阅读一部分，这样或许使读者对此问题有更全面的了解。

本书由徐洸教授主持翻译，参加翻译和审校工作的有：战晓苏、战晓雷、田艳芳、徐晔、

苏忠、董庆霞、杨秀合、李德勇、蔡开裕、朱东升、伍湘君、王斌、陈依群、范永欣、郑军、葛颖增、刘杰、刘宏伟、仇克、田兴彦、肖其英、徐钦桂、杨树强、于兵、于贵桃、赵枫梅、廖日平、李晓勇、刘伟等。

由于译者水平有限，加上时间仓促，错误之处在所难免，恳清读者赐教。

译者

2002 年 9 月

序

Internet 是一项正在蓬勃发展的研究事业，它登上人类历史舞台已经有 30 多年了。我认为将来历史会说 Internet 的诞辰是 2000 年，或者是万维网第一次出现 Internet 协议的 1993 年。

当然，TCP/IP 比 Internet 早十年。它开始只是在学术研究领域得到应用。Internet 在与其他网络技术的竞争（诸如 SNA，DECnet 等）中取得了胜利。Internet 在各行各业中广为应用，并且终将变成人类的主要资产之一。

我们真是幸运，20 年前所做出的工程决策仍然继续在为我们服务，并且此工程保持以 6 到 7 的数量级增长。许多最初的研究人员仍然继续在督促、推动并且试图使这个非凡的创造更完美。

我有幸成为他们中的一员。我在 1985 年发送了我的（我认为的）第一个信息包。我于 1987 年 12 月加入了 Bell 实验室，并且担当“邮政局长”。还有哪个地方比这里可以学习到更多的 Internet 操作技术呢？

现在来讨论一下我的工作。我的主要工作之一就是使 e-mail 能够正确地进行传输。由于有许多 e-mail 地址的格式，所以至少可以有五种不同的传输机制。其中一位朋友是用 rdk \ %templcvm.bitnet@cunyvm.cuny.edu，另一位是用 research! norman，我是用 ches@att.arpa。我们同时也处理 ACSnet 和 CSnet。有时候 uucp 通过电话线来传递我们的邮件；有时候信息包由 ARPAnet 运送。那时有一条古怪的规则就是：信息包不允许用于私人通信，但人们如何辨别信息包是否已经用于私人通信了呢？

一年后，我的工作变为运行实验室中的防火墙。我们利用防火墙成功地击败了 Morris 蠕虫，本书中详细介绍了 Morris 蠕虫。Morris 使我们很容易想到讨论蠕虫——它的教训对现在还是有意义的。虽然细节变了，但是蠕虫病毒都具有相似的攻击性和相同的成因。

1993 年在 San Jose 召开的 USENIX 安全会议中，我担任主席，这是我第一次遇到 Avi Rubin。那是一个特殊的会议：穿 T 恤衫的人的比例不同寻常地高（我通常的贡献是作为分母）。Avi 作为分子：他穿着一件绿色 T 恤。但他具有和 Peter Honeyman 一样的深炯洞察力——敏锐的思维和丰富的活力。在 1999 年的 USENIX 安全会议上，Avi 作为会议主席，他要我作为活跃气氛的发言人。通过展示一张伪造我穿着奇异衣服的照片——把会场的活跃气氛带到了高潮。作为一名研究人员，Avi 在许多领域做了极其出色的工作，并且他还是一位热情的作者。

网络安全有许多遗留下来的问题。广大读者正面对着这样的事实，即对于大多数软件来说，它们并不比 20 世纪 80 年代的更有健壮性。有些软件得到了改善。但过去长时间内

都没有把有安全问题的 Sendmail 罗列在 CERT 的咨询表中。而且它还仍然是一种重要的 e-mail管理工具。

但是我们无法确保软件中不存在错误,即确保软件的安全性。由于有安全漏洞,Web 浏览器和新的操作系统存在着大量新的复杂问题。如果系统管理员用这些具有复杂问题的平台作为他们所信任的计算基础,显然,这就像把他们的房子建在沙地上一样不可靠。

用户也没有什么进展。大多数用户对威胁毫无认知而只追求自己的方便,他们仍然选用简单的容易记忆的口令、毫不知情地传播病毒以及为图方便使用危险的选项。这都是人性弱点在如此复杂环境中滋生的后果。我现在可以告诉大家,已故的 Fred Grampp(一位对网络安全领域有重要贡献的人),用我的解码器能够对他的密码毫无困难地解码。我想努力使自己做得比他更好。

对于读者来说,参与 Internet 上的操作,也是在做一场安全性的赌博。我们如何能对这样的"赌博"视而不见呢——它保证得到快速而丰富的回报。随着大量的新机会的涌现,Internet 上出现了许多新问题,而且越来越复杂,让人很容易混淆。对这些问题的解答带来了高额回报,但同时还可能带来海市蜃楼式的更多的威胁。

本书将帮助读者解决这些问题。

前言的开场白给我敲响了熟悉的钟声。我已经在许多场合给那些有网络安全问题的人回答了许多实际问题。忧心忡忡的经理想要对他们的网络安全做一次检查。应该如何快速安全地展开此项工作呢?黑客是如何攻击网络的呢?

很显然,Avi 已经在类似的会议以及本书上考虑了很多这方面的问题,分析它们并且提供了很好的解决方案。更重要的是,他已经提供了解决问题的方法,这种方法可以推广到解决你以后所遇到的相关问题。

我发现这本书的布局非常迎合人意。我既没有时间也没有兴趣一页一页地读那些非小说类书籍。我只对新东西、容易犯错以及容易被忽略的事情感兴趣。Avi 让我可以像挑选点心一样来选择我所要看的问题,并且跳过那些我不需要看的问题。对像网络安全问题这种大型研究来说,要做到这点是非常困难的。所以像本书这样的布局是非常有帮助的。

那么,如果读者愿意可以一页一页地阅读,或者挑选出所关心那一部分的一些章节看。Avi 在每一章前所做的图标应该对读者选出所要看的知识有所帮助。

而且,正如我已经许多次地警告那些咨询的人一样,跳过那些对自己来说十分困难的部分是正确的作法。

Bill Cheswick
Bernardsville, NJ

前　言

写此书的原因

作为 AT&T Labs 的计算机安全专家，我发现自己经常和我们的大客户的 IT 部门的工作人员会面。例如，今年我已经和 Ford 公司的 CIO、JP Morgan 的 CIO 以及美国 Axle 制造业的副主席等会过面了。每次会面，都会有一些系统管理员以及其他相关人员随行，他们总是带了一堆问题来。如何允许别人安全地远程访问网站？如何设置防火墙？员工们如何在电脑上安全储存资料呢？这一系列问题反反复复地一直问。我认真倾听他们的问题，并给他们合理的建议。

顾客总是要我推荐一本能解决所有这些问题的书。虽然有一些好书，但它们总是按一种惯例写书。通常第一章写密码学，然后是协议、SSL 等。所以，我决定开始写一本书来直接回答这些 IT 行业人员所遇到的问题。

除了某些部分，本书都是以一种面向问题的方法写的。每一章都以一个问题的陈述开始（有时是 Alice，有时是 Bob 提出问题，这些人名是借鉴密码学文献里的人物名称）。

本书分成五部分，每一部分都自成体系。所以你可以跳过那些冗长的内容。每一部分（除第一部分）都包含若干章，每一章都提出一个问题。每一章都描述一个威胁模型，解释相关技术，并且提供一些解决方案。每一章都推出一个或多个案例研究。我的主要想法是提供读者足够多的资料来理解问题的细节，并且使读者有能力找到解决方案，甚至使他们能够自己解决问题。

所针对的读者

有几种不同的人可以从本书受益。我设法确定几个计算机安全问题，这些问题是最普遍、最让人有兴趣学习的。一些人读了本书后将能勾勒出对某些特殊问题的解答。另一些人在读了以后可以使他们自己具有应付一定威胁的能力。无论你是一名经验丰富的职业 IT 人员，还是系统管理员，或是计算机科学的研究生，或者仅仅是一名普通用户，本书都有读者所需要的东西。本书中涉及的一些问题并不复杂，而且很少需要专门的技术训练。另一些问题要求有复杂的技术解答，而且这些解答似乎对那些没有计算机或者数学背景的人来说是难以理解的。为了便于读者阅读，我每一章都确定了难易程度以及所针对的读者。在每一章的开始，我就展示代表所要针对读者的图标。每一章最左边的图标表示最相关的

读者，以此类推，图标从左到右排列。

网上冲浪者/普通用户

网上冲浪者或者普通用户只是在每天生活中上上网，收发 e-mail，用用电脑。他们没有必要经过正式的计算机科学训练，但他们精通计算机的日常用法。例如他们知道如何安装软件，如何改变浏览器的设置。

职业 IT 人员

这些 IT 人员具有相当的电脑知识。他们可能是大型网络安全的负责人、程序员、系统构建者，甚至是技术经理。我们几乎可以肯定的是：这些人有一个计算机科学或者 CIS 的学位，并且他们已经用计算机工作相当长的时间了。

学者

学者通常是教授，或者是研究生。学者通常对隐藏在解决方案后面的技术细节与理论比对解决方案本身更感兴趣。他们可能会阅读其他参考资料以进一步理解问题的实质。他们不会害怕而是欢迎那些让人毛骨悚然的细节。

系统管理员

系统管理员经常要对某个网站负责。他们经常要去“救火”。如果资料丢失了，如果闯入了不速之客，那么就要开始他们紧张的工作了。这些人对确定网络系统是否安全感兴趣。虽然他们喜欢研究和理解隐藏在解决方案后面的理论本质，但他们又往往没有时间去研究。他们真正所需要的是想出如何解决瞬间向他们袭来的问题。

本书每一章都提供一个问题的解决方案，这个问题对一部分人来说是重要的。为了使读者知道这些描述中的哪一些适合自己，哪一些不适合自己，我希望在每章开始的图标能帮助读者在阅读时很好地把握本书细节以及复杂性的等级。

本书指南

本书有五部分

第一部分 第一部分阐明了我写本书的动机。在这一部分没有提出问题;然而这部分介绍了什么是威胁,以及人们为什么关注计算机安全问题。

第 1 章 本章阐述了这样的事实,就是让公司承认发生了计算机安全问题是困难的。这样使得人们正确估计计算机安全事件的破坏程度变得很困难。

第 2 章 本章涉及了是什么正受到威胁,目的是帮助读者理解威胁。

第 3 章 本章是本书最有特色的一章。计算机病毒和蠕虫是人们最常遇到的计算机安全问题,并且时常能感受到它们的存在。本章重点不是集中在问题和它的解决方案上,而是用病毒和蠕虫来帮助读者认识它们对计算机和网络造成的威胁程度。本章分析了这些攻击并且解释了它们是如何工作的。

第二部分 第二部分处理了信息的安全存储问题。

第 4 章 Alice 有非常重要的资料,她希望存到自己的电脑里。那么她应该如何保护这些数据使得即使电脑落入对手手中,那些数据仍然是安全的,并且使得她能检测出任何对资料的篡改呢? 而且最理想的情况是,Alice 想要的是容易使用而且适用于多种实际应用的解决方案。

第 5 章 Alice 使用文件系统远程储存文件。如果这些文件从对手的网络或者对手所控制的远程文件服务器通过,那么她应该如何保护数据的真实性和机密性呢?

第 6 章 Alice 考虑到她的数据非常重要。她已经饱受由于软硬件故障而丢失文件的痛苦了。Alice 电脑上的数据非常敏感。当数据在她的电脑中时,她非常擅长于保护她的电脑并且可以保证数据安全。但她应该如何备份她的数据以使备份也安全可靠呢?

第三部分 本书第三部分是最具技术性的。它所要处理的是在易受攻击的网络上安全地传输信息。

第 7 章 Alice 应该以什么方法鉴别 Bob 呢,即她可以担保将来与 Bob 通信是可以鉴别的,并且不可能有另外一方可以建立与 Alice 的通信而显现是来自 Bob 的。另外,如果 Alice 认识到有某一方(恶意的一方)可能假冒了她,那么她应该如何恢复限制恶意方所造成的破坏呢?

第 8 章 假设 Alice 和 Bob 有一个长期关系。他们既知道彼此的公共密钥,也用相互信任的机构共享对称长期密钥,或者彼此共享对称长期密钥。那么

Alice与 Bob 应该如何建立对称会话密钥以保护他们的信息呢?

第 9 章 假设 Alice 和 Bob 有对加密和验证的会话密钥。他们应该如何保护他们的通信呢? 在协议族中哪个层协议最适合保护他们通信的安全呢?

第四部分 本书的第四部分将讨论如何确保网络安全以免受威胁。这里包括建立防火墙、检测入侵以及处理拒绝服务攻击。

第 10 章 Alice 负责某个网络的安全。网络对于她来说太大太复杂以至于不能保证每台主机的安全,并且不能保护网络免受攻击。她应该如何定义一个周边,建立一个对网络的统一安全管理政策,并且可以对付那些网络外部的恶意攻击呢? 一旦她定义了一个周边,那么她应该如何允许合法用户远程访问而可以防止没有权限的用户非法登入呢?

第 11 章 Alice 负责某个网络的安全。她应该如何防止网络免受攻击呢? 她应该如何检测入侵以及采取正确的措施呢? 她应该如何处理大量的拒绝服务攻击呢?

第五部分 第五部分也就是本书的最后部分,处理了在线商务和个人隐私。这部分涉及的问题包括如何在网上正确使用信用卡以及如何确保浏览网页时的个人隐私等。

第 12 章 Alice 经营一家网络商店。她应该如何保证顾客可以在线购物,而防止被网上活跃的攻击者盗取他们的信用卡呢? 她想增加网络的安全性而不会反过来影响服务器的运行。Bob 想在线购物。他应该把他的信用卡号填到网页表单上吗? 这样做他将承担什么样的风险呢?

第 13 章 Alice 喜欢上网。她浏览感兴趣的网页,在线购物,利用 e-mail 参与讨论以及聊天,并且她还做了自己的网站。Alice 应该如何保护她个人资料中的隐私呢? 她应该如何阻止第三者收集她的相关资料以及防止她在网上被跟踪呢?

如何阅读本书

有几种阅读本书的方法。如果读者遇到了本书提到的某些问题,那么最好跳过一些章节,直接阅读那些讲述读者所关心问题的章节。如果那刚好是在一个部分的中间,因为读者可以从前面章节中找到所需要的资料,所以我推荐读者找到包含这些问题的部分,然后通篇阅读那个部分。

如果读者是对学习所有问题或者一般的安全问题感兴趣,那么就从头到尾阅读本书。本书的这些部分没有什么顺序,所以读者可以按照所喜欢的顺序阅读,但最好在一个部分内按顺序阅读各个章节。

在每一章的最后面都列出了本章所引用的所有参考文献,参考书、论文以及网站都列在

其中。我尽最大努力及时地参考所涉及的那些网站，并且在写每一节的同时我上了所有这些网站好几次。当然，网站是动态的，所以我不能担保本书涉及的资料就是最新的。但我在书里列出网站的所有链接，并且尽可能地使资料是最新的。本书的 URL 是 http://white-hat.org/。如果读者发现这个链接已遭破坏，请告诉我。本书的最后列出了书中所引用的所有参考书目。

本书所用到的所有缩写词都列在术语表中，所以如果读者要查找某个不理解的术语，术语表将对读者有所帮助。

致　　谢

写一本书是个漫长而又艰辛的过程。幸运的是，我有许多可以利用的资源并且还有许多优秀评论家的参与。首先，我要感谢我的妻子 Ann，是她在我“不得不”写本书时让我可以把所有时间都花在上面。我也要感谢 Elana，是他不知多少次地修改我的原稿。感谢我的父亲，因为他校对了本书的草稿。感谢我的母亲，因为她帮我辨别了父亲严肃正式的评论和他的玩笑。

我万分感激我的编辑 Karen Gettman，她不辞辛劳的努力使我完成了本书。并且还帮助我找到了世界级的评论家，把所有事情都安排妥当，还在精神上给我很大的鼓励。也感谢 Ed Felten，他使我形成了写本书的最初想法。感谢 Gary Zamchick，因为他出色的艺术品。

我也要感谢在 AT&T Labs 的上司，尤其是，我的经理 Bill Aiello，Hamid Admadi，还有 Ron Brachman，是他们提供给我极好的写作环境并且给我完成本书以极大的鼓励。

虽然他们都没有直接参与写本书，但我要感谢我以前的导师 Peter Honeyman、Bernard Galler 以及 Atul Prakash，是他们给我指引了计算机安全研究的方向，并且为我的职业打下了坚实的基础。Tony Bogovic 也没有直接参与写书，但我要感谢他帮助我想到单击那些链接的方法。是他使我的思想从书里解放出来，让我可以好好地享受高尔夫的乐趣。

最后，我非常感谢评论家们，是他们提供给我非常有帮助的评论。他们包括 David Backer、Dan Boneh、Robert Bruen、Lorrie Cranor、Bruce Davie、Jim Duncan、Peter Guttman、Steve Halzel、Sandra Henry-Stocker、Brad Johnson、Kevin Johnson、Dave Kormann、Gary McGraw、Craig Metz、Marcus Ranum、Eric Rescorla、Lance Spitzner、Win Treese、Wietse Venema、Avishai Wool，还有一些匿名的评论家。

Avi Rubin
rubin@research.att.com

目　录

第 1 部分　存在的威胁