第3章

Internet 欺骗与网络犯罪

本章目标

在学习了本章内容并完成所有练习之后，读者将能够掌握如下内容。

- 了解常见的 Interne 欺骗方式，例如炒股诈骗和投标屏蔽。
- 能够采取具体的措施防范 Internet 欺骗。
- 能够采取具体的步骤防范身份盗用。
- 了解网络犯罪以及相关法律。
- 了解如何积极利用计算机犯罪。
- 学习 Web 浏览器隐私配置。
- 掌握针对计算机犯罪有哪些法律武器。

3.1 本章简介

任何新领域，都会存在犯罪的影子。辽阔的大海曾经孕育了大量海盗，广袤的美国西部也滋养了大量强盗。Internet 也一样，也存在违法现象。除了黑客以及病毒攻击，还有许多形式的危险存在。欺骗在 Internet 上是很常见的，自从人类文明诞生以来，欺骗就相伴而生。在过去的几个世纪，就有江湖游医到处贩卖假药和长生不老药。随着 Internet 上电子商务的兴起，伴随而来的网络欺骗也越来越多。实际上，许多专家认为欺骗是 Internet 上最大的威胁。造成 Internet 上欺骗成风这种局面有许多原因。首先，网络欺骗没有太高的技术要求，不需要掌握黑客技术和制造病毒技术。其次，现在有许多人习惯于在 Internet 上做生意，这就给欺骗提供了大量可乘之机。

Internet 欺骗有许多途径，本章介绍几种主要的欺骗形式，有哪些惩治网络犯罪的相关法律依据，以及如何保护自己免受欺骗。本章练习会介绍如何设置浏览器隐私，以及如何使用反间谍软件。本章介绍的内容已不单纯只涉及技术方面，因为网络欺骗不仅仅只依靠技术手段，网络欺骗只是将人类历史出现的骗术实施到计算机上而已。

3.2 网络欺骗的方式

Internet 骗术花样繁多，美国安全交易委员会(Securities and Exchange Commission)网站上列出了几种主要的网络犯罪形式[①]。我们将简要讨论这些以及其他骗术，但不可能覆盖网络上的所有骗术。然而，本书不可能包含所有骗术，这样的工作一本书根本不够，至少需要好几本。本书介绍一些常见的主要的网络骗术，并从中总结经验，使读者能举一反三。这样应该能够避免大多数网络欺骗。

3.2.1 吸引投资

吸引投资并不新鲜，一些股票经纪人以此为生，到邮局查找电话簿，通过打电话劝说人们投资某支股票。一些正规的经纪公司也这么做，同时，这也是很常见的诈骗形式。在 Internet 上也允许吸引投资，正规的和设局的都有，在 Internet 上更容易广泛传播。多数读者可能已经很熟悉了，在电子邮箱中每天都有大量这种吸引投资的邮件，一些电子邮件直接将读者置身于某项投资计划当中，一些宣称有内部消息以诱惑读者。遗憾的是，多数并不是邮件中宣称的那么神乎其神，有些确实是有价值的信息，但必须了解，有些其实就是网络骗局。

引资骗术

最常见的引资骗术大概是这样的，发送一封电子邮件，声称能以极少的投资获取超额回报。最著名的案例要数尼日利亚人骗术了。在这个案例中，实施者随机向许多人发送一份电子邮件，邮件自称来自一些已故尼日利亚医生和政府官员的亲属，该已故人士可能是一些社会名流，这样看起来更诱人。邮件中发出邀请：某人具有大量财产要转移到海外，出于安全考虑，不能通过自己的账户，希望通过你的账户暂时中转一下，如果同意，你会得到一笔可观的费用。达成意向后，还会收到一封看起来相当正式的文件，足以蒙骗普通人。然后要求你交一些费用比如税费、通信费等。一旦交了钱，这些人就销声匿迹了。美国联邦经济情报局对此发出一份通报，详细描述了此类欺骗并要求加以防范。[②]

设想一下，如果你有大量钱财要转移到海外，会跟素未谋面的人交易吗？你难道不担心钱款转移到这个人的账户后此人潜逃吗？为什么钱要转移到美国，而不是巴拿马？或者，为什么不通过美国联邦快递或包裹服务来转移？重点是，有这么多转移钱财的手段，为什么要相信一个素昧平生的人。从这一点就可以断定，其中必然有诈。从这些骗术中总结出来的第一条原则是：换位思考。他是否冒了很大风险？是否只能靠你来帮助？换作是你，会这样做吗？假如不会，这可能就是一场骗局。

---

① The U. S. Securities and Exchange Commission. "Internet Fraud: How to Avoid Internet InvestmentScams." Washington, D. C.: Author, November 15, 2001. Accessed April 2011: www. sec. gov/investor/pubs/cyberfraud. htm

② The U. S. Secret Service. "Public Awareness Advisory Regarding '4-1-9' or 'Advance Fee Fraud' Schemes." Washington, D. C.: Author, 2002. Accessed April 2011: http://www. lbl. gov/IT/CIS/CITG/email/419-Fraud. html

投资建议

从某种意义上来说，这种投资建议不能算作 Internet 陷阱。许多公司专门雇人发布消息推荐某支股票，然而，这些活动不能简单地说是非法的，美国联邦安全法没有要求必须为此类建议找一个负责人，该法律基于这样的考虑，作者在提出这样的建议时，他们的观点可能完全受到了某些主观因素的影响。因此，许多在线投资建议函也不指名受雇于哪家公司，可能这些看起来客观的投资建议完全是出于某种利益驱使。所以，与其相信这些建议，还不如咨询一些收费的投资建议。这种陷阱在 Internet 也比较常见，甚至比引资骗局更普遍。

有时这些在线股票公告板可能被利用，成为阴谋的一部分，通常叫哄抬股价。经典的哄抬股价很简单，这种骗术以极低价格大量收购某支股票，然后如井喷一样拉高升值。[①] 一种常见的方法是散布谣言发布利好，鼓动大家抢购该股票，购买的人越多，股票价格升得越快。如果做得好，股票价格可以翻倍甚至 3 倍。而实施者早在之前就以低价购买了大量股票，到股票涨到一定价格时，就会全部出货以赚取现金。等到下一个财季报告发布时，股票价格又会回到正常价格。过去几十年，这种骗术很流行，应该小心这种“内幕”消息，如果某人知道 X 公司将要发布新产品，实施新计划，为什么要将这种利好消息与陌生人共享？

美国安全交易委员会发布了如下提示防止此类骗术。

1. 考虑信息来源。如果不是非常了解股票市场，那么就只接受知名的、声誉好的分析师的建议。

2. 独立判断。不要轻信任何人。

3. 研究。对股票公司历史市值、最近业绩等信息进行研究。

4. 警惕高压战略。正规的股票经纪人不会向客户施压，他们只是帮助客户选择需要的股票，如果被施压，可能就预示着有问题。

5. 保持怀疑。适度怀疑是有益的，有这样一句话：“如果一切都太对了，反而可能不太对”。

6. 确定已研究了各种投资可能。

事实上，这种欺骗得手的原因是人们的贪欲，这里不是苛责，但明白这一点很重要，如果贪婪，那么离受骗就不远了。你可能不能一夜暴富，但至少相对安全。不投资就没有风险。假如在短期内不费力赚到很多钱，就是理想的行骗对象。

练习

实际上，针对在线投资，建议与声誉好的经纪公司做生意。这条原则也就意味着不要回应任何通过电子邮件、在线广告等发起的招商引资，只参与知名经纪公司发起的投资。通常，这些经纪人来自知名投资公司，拥有长期良好的声誉，也可以提供在线服务。重要的是利用证券交易委员会对经纪人进行审查。

---

① The Fraud Bureau. “Pump and Dump Classic.” Stock Scams 101. Ontario: Fraud Bureau Corporation, 1999. Accessed April 2011: www.fraudbureau.com/investor/101/article15.html

3.2.2 拍卖欺骗

在线拍卖，如eBay，能够买到物美价廉的商品，许多人习惯用这种方式来购物。然而，任何拍卖网站都可能有骗局，能以竞拍价格拿到商品吗？商品如广告上说的那样好吗？多数在线拍卖是正规的，并且多数拍卖网站对骗局也多加防范，但问题仍在所难免。事实上，美国FTC(Federal Trade Commission，联邦交易委员会)[①]列举了以下4类在线拍卖骗局(U. S. Federal Trade Commission，2004)。

- 付款后不发货。
- 实际货物与约定不符。
- 没有按时交货。
- 没有全面显示商品相关信息。

第一类，付款后不发货，是彻头彻尾的欺骗，并很容易实施。客户付了款，却收不到货，销售人员把钱黑了。在有组织的骗局中，销售商会同时发布很多在线销售项目，收到钱就卷款潜逃。假如计划得好，整个过程都使用假身份证，使用租来的邮箱和匿名电子邮件服务。这个人只在骗局中出现，以后就人间蒸发了。

第二类，发送与约定不符的货物，可以说是灰色地带。一些情况下，确实是故意欺骗。销售虚假宣传，例如，广告称销售的是某名人签名的第一版书籍，可发送的却是第四版且没有签名。虽然在某些特殊情况下，可能是一时疏忽。销售人员宣称棒球是一位名人签过名的，但实际上签名是印刷上去的。

这个问题与美国联邦交易委员会列表上第四类问题相似，没有全面显示商品相关信息。例如，一本书可能是考证过的首印版图书，却是后来翻印的，这就会变得毫无价值。这个情况销售人员可能并没有提及，没有完全交代商品的全部信息可能是蓄意欺骗，也可能是一时的疏忽。美国联邦交易委员会还把没有按时交货定为了一种欺骗。还不清楚这到底是一种欺骗形式，还是因为客户服务不到位造成的。

美国联邦交易委员会和拍卖欺诈

美国联邦交易委员会同时还在其网站上列举了如下3种正在Internet悄然升起的投标欺骗形式。

- 标托(Shill bidding)。一些假冒的投标者竞标以哄抬价格。
- 投标屏蔽(Bid shielding)。有人假冒投标者，将价钱炒高，然后在拍卖结束的前一刻弃标。投标屏蔽会使卖方被迫接受次高标的出价(在假投标开始之前的一次投标)。
- 投标虹吸(Bid siphoning)，是指把买家从正当的在线拍卖网站引诱到看起来一模一样的下线网站，企图欺骗买家。在这个下线网站，买家没有任何诸如保险、反馈表、保证书等安全保障。

---

① The U. S. Federal Trade Commission, Accessed April 2011: www. ftc. gov/bcp/edu/pubs/consumer/alerts/alt124. shtm

标托

标托是这 3 种里面最常见的，并不十分复杂。假如实施者在一家在线拍卖网站卖东西，那么他可能同时用了好几个假身份，利用这些假身份哄抬价格。这在实际操作中很难防范，然而，经验之谈是，出价是否超出了自己的预期，任何情况下，都不要多花一分钱。

投标屏蔽

标托很难界定，但投标屏蔽对拍卖网站来说很容易发现。许多主流的拍卖网站，如 eBay，已经采取措施防止投标屏蔽。最明显的措施就是限制撤回投标人的权限，也就是说，假如某人出了高价却在最后一刻撤标，他可能永远也不能再使用该拍卖网站。

投标虹吸

投标虹吸最少见。在这个骗术里，实施者在一家拍卖网站公开拍卖一件商品，但在商品的广告中，却提供一个链接，将用户吸引到一个伪造的拍卖网站，毫未察觉的买家跟着这个链接就上了卖家的当。

3.3　身份盗用

身份盗用(Identity theft)问题越来越多，而且非常棘手。概念很简单，虽然过程可能很复杂，后果很严重。身份盗用是指某人在未授权的情况下使用他人账户，通常是利用他人账户采购。可能盗用受害者的信用卡号或驾照号。一旦实施者取得了受害者的信用卡信息，就会大肆采购物品，让受害者来买单，而受害者通常这时候还蒙在鼓里。

获得驾照号可能会使受害者替人担当不良驾驶记录，遭受不白之冤。例如，某人驾驶违规，被警察拦下，警察要求出示驾照，此人可能拿出盗来的驾照，警察检查没有问题，然而，这次违章记录就会记在受害人名下。肇事者不太可能交罚单。所以，到某个时候，受害人会收到通知由于不交罚单而驾照被吊销。除非受害人自己能证明或有证人证明自己案发时不在现场，否则只能替人受过交罚单了。

美国司法部(Department of Justice)对身份盗用的定义如下[①]：

“身份盗用和身份欺骗是指那些涉及欺骗中所有错误地获得和使用他人个人信息的犯罪，尤其是电子身份。”

Internet 的繁荣使得窃取个人身份信息更加容易。美国许多州都将法庭记录和违章记录放在网上，一些州使用个人社保号查询违章记录，这样，一旦罪犯获得了某人的社保号，就可以查询其违章记录，也可能将某人驾照复制一份。网上还能找到关于此人的法庭记录相关信息，甚至信用历史，如何利用 Internet 进行调查会在本书后面章节介绍。与其他工具一样，可以用于正当目的，也可能用于非法目的，调查到足够信息就可以伪造某人的身份。

---

① The U.S. Department of Justice Identity Theft web page, Accessed April 2011: www.justice.gov/criminal/fraud/websites/idtheft.html

练习：信用卡安全

一种新的身份盗用工具是一种手持扫描器。在美国达拉斯-沃斯堡地区发生的一起连环案件中，罪犯与餐馆服务员串通，当服务员拿着客户信用卡去结账时，会使用一种藏在口袋里的手持设备扫描信用卡信息，然后服务员将此信息给罪犯，利用这些信息就可以在线采购或制作一张假信用卡。这是一种新型的身份盗用技术，防范办法是永远不要让信用卡离开你的视线。

钓鱼

钓鱼已日益成为身份盗用的最常见方式。其过程是引导目标提供个人信息。例如，攻击者发送一封假装是银行发出的电子邮件，告诉收件人，其银行账户有问题。随后，邮件会引导用户单击一个银行网站的链接，这个链接中有出问题的银行账户。然后，电子邮件再让用户单击一个链接，这个链接是银行网站，可以登录和验证账户的。然而，这个链接是攻击者建立的假冒的银行网站。用户到了这个网站，输入了自己的信息，他就将自己的用户名和密码提供给了攻击者。

现在有许多用户已经意识到了这种问题，会避免单击电子邮件链接。但是，遗憾的是，并非每个人都这样谨慎，所以，这种攻击依然会起作用。另外，攻击者还有其他新的钓鱼方式。比方说跨站点脚本编程（cross-site scripting）。如果一个网站允许用户发帖，其他用户能看到，比如产品评论，攻击者随后就可以张贴脚本，比如 JavaScript 或其他脚本，而不是评论或其他合法内容。随后，其他用户访问网页时，加载的不是评论或解释，而是攻击者的脚本。这些脚本可以做任何事，比较常见的，是将用户重新定向到钓鱼网站。如果攻击者足够聪明，钓鱼网站看起来会与实际的网站别无二致，用户不会意识到他已经重新定向了。网站的开发人员可以过滤所有用户输入来预防这种攻击方式。

3.4 网络侵犯

侵犯最近几年受到了大量关注，主要原因是，侵犯通常是犯罪行为，包括性骚扰、谋杀等行为的前奏。因此，许多州政府都有各种反侵犯法案。然而，侵犯问题最近蔓延到了网络世界，什么是网络侵犯（cyber stalking）呢？网络侵犯是指利用 Internet 骚扰他人。美国司法部是这么定义的：[①]

“目前还没有网络侵犯的确切定义，这里对该词的定义是，利用 Internet、电子邮件或其他电子通信设备侵犯他人。侵犯通常包括持续骚扰、恐吓行为。例如某人频繁出现在他人家里或工作场所，打骚扰电话，留纸条或物品，毁坏个人物品等行为。大多数侵犯相关法律需要实施者对受害者本人造成了很大伤害这样的事实，有一些包括受害者的直系家人，还有一些要求具备持续侵犯过程这样的事实。然而，有些骚扰和恐吓行

① The U. S. Department of Justice Cyber Stalking page. Accessed April 2011: www. usdoj. gov/criminal/cybercrime/cyberstalking. htm

为属于短期非法侵犯，这种行为可能是侵犯的前奏，也应该引起重视。”

假如有人利用 Internet 骚扰、恐吓他人，那么就犯了网络侵犯罪。最常见的例子是发送恐吓电子邮件，如何定义恐吓是法官的事。这里有个经验之谈，假如电子邮件的内容超出了正常言论，有些吓人，那么就可以认为是恐吓。有一个不太明显的网络侵犯案例。假如要求某人停止向自己发送电子邮件，而此人还是不停发送，这是犯罪吗？遗憾的是，没有明确答案。可能是也可能不是，要依据电子邮件内容、造成的影响以及当事人之间的关系来由法官断定。

根据美国司法部网站资料[①]，列举 3 起网络侵犯。了解这些案例，有助于理解什么是网络侵犯。

(1) 第一起成功指控是根据加利福尼亚州的新网络侵犯法，检举方在洛杉矶社区律师的办公室收到了一份针对一名 50 岁退休保安的犯罪指控，称其利用 Internet 骚扰一名妇女，该妇女曾拒绝其追求。并指控其通过在各种 Internet 聊天室、BBS 发布受害人的电话、家庭住址以及编造的受害人曾被强奸等信息。在至少 6 个月的时间内，有时在半夜，有男子敲打受害人的房门并声称要强奸受害人。该退休保安在 1999 年 4 月被判 1 项侵犯及 3 项性骚扰罪名成立，要面对超过 6 年的牢狱之灾。

(2) 美国马萨诸塞州的地方检察官指控一名男子利用匿名电子邮件，涉及一起系列团伙骚扰受害人，恐吓要将其过去性行为告发给受害人现任丈夫。

(3) 一名圣地亚哥大学的优秀毕业生通过 Internet 恐吓 5 名在校女生长达一年时间。受害人收到了上百封恐吓电子邮件，有时一天收到 4～5 封。该毕业生被指控有罪，判刑 6 年。该毕业生对警方说，其犯罪是因为这些女生取笑他。事实上，受害者根本不认识他。

显然，利用 Internet 骚扰与当面骚扰都是严重罪行，这个问题已经延伸到了工作区事件。例如，法庭已认可，给人发送其不需要的黄色图片是一种性骚扰。假如员工抱怨总是收到不需要的电子邮件，雇主有责任改善这种境况。可以通过安装一款垃圾邮件阻止程序来实现。然而，假如雇主没有采取任何措施来解决问题，这可能被法庭认为是一种消极工作环境。如前所述，如果骚扰构成了对一个人的侵扰，那么，就可以考虑认定为网络骚扰[②]。法律字典黑皮书将骚扰定义如下：

“没有合法目的扰乱他人情绪使其不得安宁的过程。”

“使他人厌烦、惊恐以及侮辱他人的语言、姿势、动作。”

通常，针对骚扰投诉，执法人员需要一些可信的被伤害证据。简单来说，如果在匿名聊天室，有人对你污言秽语，可能并不认定是骚扰。然而，如果通过电子邮件被骚扰，就可能被认定是。

网络犯罪相关法律

在过去的几年里，美国以及其他国家和地区各立法机关已经通过了“Internet 欺骗”的定义，并严令禁止。多数情况下，当前针对欺骗和骚扰的法律也适应于 Internet；然而，一些

① Blacks Law Dictionary，1999，West Publishing Company，7th Edition.

② Blacks Law Dictionary，1999，West Publishing Company，7th Edition.

立法机关认为应当有针对网络犯罪的相关立法。

身份盗用已经成为美国各州及联邦法律讨论的焦点，大部分州政府都具备针对身份盗用的法律[①]。美国联邦法律对这种犯罪形式也有所提及。1998年，美国联邦政府通过了18 U. S. C. 1028，也称为身份盗用及假设阻止法案1998。这部法律使身份盗用成为全美公认的犯罪行为[②]。美国联邦法律适用于整个美国，一些州还有专门针对身份盗用的相关法律。

许多州明令禁止网络侵犯。通常，现存的反侵犯相关法律条文同样适用于Internet。2001年，一名加利福尼亚男子被起诉网络侵犯，就是依据现有的反侵犯法规[③]。其他国家也有关于反侵犯的法律，同样适用于Internet。加拿大在1993年通过了一部广泛适用的反侵犯法。遗憾的是，有许多类似的案件。举例如下：

- 一位70岁的老者约瑟夫·迈迪克，2010年在教堂遇到了一位16岁的女孩。迈迪克尾随女孩到她的汽车，与她搭讪，希望能共进晚餐，然后去他家。女孩拒绝了。他开始每天不断地打电话，发短信。他的行为逐步升级，直到女孩报警，将其逮捕归案。
- 2008年，20岁的肖恩·迈克尔·哈钦森在网上张贴其前女友的裸体图片进行威胁。他扬言，“如果我看到你和戴维在一起，你就别想活了。这可不是威胁，我说到做到”。

罗马尼亚已经开始严打网络犯罪，一些专家称，罗马尼亚的网络犯罪相关法律是世界上最严格的[④]。然而，有意思的是，立法者的大部分精力都花在了如何定义所有相关术语上，这对法律的严谨性来说非常重要，让不法之徒难以找到法律漏洞。但遗憾的是，罗马尼亚政府也是在罗马尼亚成为网络犯罪重灾区后才采取这样的措施，罗马尼亚曾被世界上的多家媒体报道称为“网络犯罪之城”，看来这个国家的主动防御措施做得还不够好。

代顿大学法学院有一个网站专门针对网络犯罪。上面有内容相当全面的网络犯罪、网络侵犯和其他Internet犯罪相关链接。随着时代的发展，相信会有更多的法学院致力于网络犯罪研究。

在过去几年里有一个有趣的现象，就是从事网络犯罪官司的律师逐渐出现。这强烈地预示着在现代社会网络犯罪问题正越来越严重。

3.5 防御网络犯罪

知道了各种Internet流行的欺骗形式以及相关法律，该如何自我保护呢？这里有一些Internet防御措施，可以降低被欺骗的风险。同时还有一些明确的指南，指导受害者该如何应对。

---

① The National Conference of State Legislatures. “State Computer Harassment or ‘Cyberstalking’ Laws.” Denver and Washington, DC.: Author, 2004. Accessed April 2011: www.ncsl.org/programs/lis/cip/stalk99.htm

② The Identity Theft and Deterrence Act of 1998, USC 1028

③ The Minneapolis-St. Paul Star Tribune, Accessed August 23, 2001; www.startribune.com/

④ Romanian Information Technology Initiative. Accessed April 2011: www.riti-internews.ro/cybercrime.htm

3.5.1　防止投资欺骗

为防止投资欺骗，应该做到以下 4 点。

(1) 只与知名的、声誉良好的经纪人合作。

(2) 假如一件事听起来神乎其神，最好放弃。

(3) 自问，为何此人要和你分享投资信息，为什么会把这么好的投资机会共享给你？

(4) 要记住，投资就会有风险，所以投资额度最好控制在可接受的范围内。

3.5.2　防止身份盗用

对于身份盗用，措施是明确的，主要包括以下几种。

(1) 如果不是特别必要，不要向他人提供个人信息。这条原则说明在 Internet 上不应与陌生人交流，不要泄露自己的任何信息，包括年龄、职业、真实姓名等。

(2) 销毁含有个人信息的文档。假如随便乱扔银行账单或信用卡账单，从中可以找到大量个人数据。可以从办公用品店或零售店买一个碎纸机，20 美元。将文档在丢弃之前碾碎。这条原则似乎与计算机安全无关，但非技术手段获取信息也一样可以用于身份盗用。

(3) 经常检查信用卡。许多网站如 www.qspace.com，可以查看信用卡信息。建议每年检查两次，如果看到任何未授权物品，那很有可能是成了身份盗用的受害者。

(4) 假如所在州都有在线驾驶记录，那么每年检查一次。假如看到有违章记录不是自己的，这就是说自己的身份被他人盗用了。随后的章节会详细介绍如何在网上得到这些信息，通常花费不超过 5 美元。

概括来说，防止身份盗用的第一步是尽可能不暴露个人信息。其次是注意信用卡是否有自己并没有使用的刷卡记录，这样可以注意到是否有人尝试使用你的身份。

防止身份盗用的另一方面就是保护隐私。就是说，要防止他人在未经许可的情况下获取你的个人信息。防护措施包括设置浏览器以防他人窃取个人信息。许多 Web 网站会将你的登录信息存储到一个小文件里，也就是 Cookie，这些 Cookie 文件在本机存储。Cookie 的问题是，网站可以读取本机上的任何 Cookie 文件，包括不是该网站建立的。因此，假如访问的网站存储了姓名、访问网站、时间等信息，其他网站也可以偷偷读取这些信息。清除不需要的 Cookie 的最好工具是反间谍软件，也可以使用 Internet 设置减少隐私暴露。

3.5.3　浏览器防护设置

如果使用 Microsoft Internet Explorer，可以选择 Tools(工具)→Internet Options(Internet 选项)命令(原文此处误为 Options，少了 Internet，译者注)，出现如图 3.1 所示的界面。选择第三个选项卡 Privacy(隐私)。

屏幕出现图 3.2 所示的界面。注意左边的滑块，可以选择不同的安全级别来防护 Cookie。这里选择 Medium High(中高)级别。

注意界面下方的 Advanced(高级)按钮，可用来禁止或允许个人网站创建 Cookie。改变 Cookie 设置虽然只是防护隐私的一部分，但非常重要。

可能还要选择 In Private(隐私中)浏览选项，如图 3.2 所示。

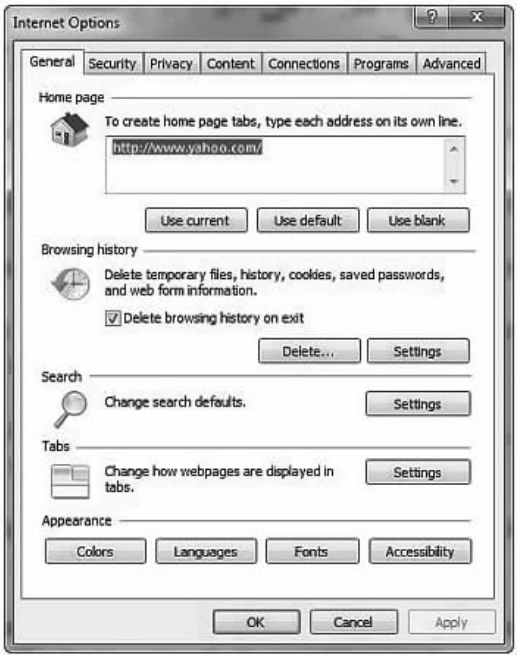

图 3.1 IE 选项

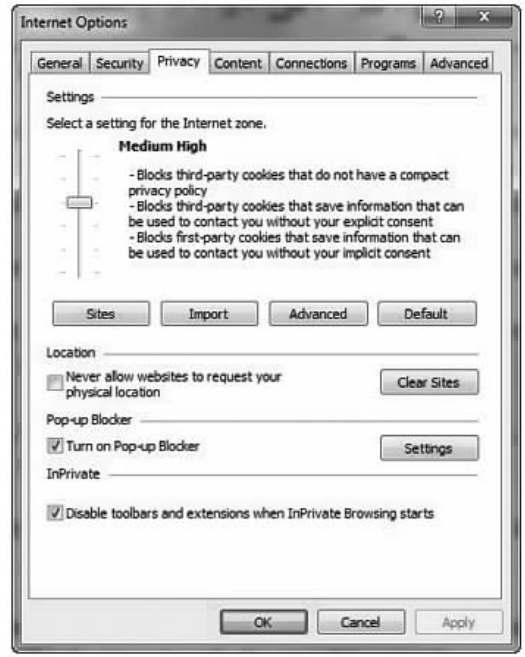

图 3.2 IE 隐私选项

如果使用 Firefox，过程类似。选择 Tools(工具)，Options(选项)，出现图 3.3 所示的对话框。

图 3.3 Firefox 选项

选择 Privacy(隐私)选项,将看到如图 3.4 所示的对话框。

图 3.4　Fire 隐私选项

从图 3.4 中可以看出,有一些可选择的隐私设置,从名称便可以看出其作用。选择 Security(安全)选项卡,可以看到如图 3.5 所示的对话框。

图 3.5　Firefox 安全设置

建议选择 High Security(高安全性),笔者只是允许第一方(first-party)Cookies。第三方 Cookies 在侵犯用户隐私方面声名狼藉。后续章节将更详细地讨论 Cookies 和间谍软件。但现在做的简单一小步,就可以在保护用户隐私上迈出一大步。

3.5.4 防止拍卖欺骗

在线拍卖有很多要注意的地方，这里有一些建议。

（1）只用声誉好的拍卖网站。最知名的是易趣（eBay），但任何广为人知的、声誉好的网站也可能有风险。只是这些网站会替消费者考虑很多防范措施。

（2）假如听起来神乎其神，最好放弃。

（3）一些网站提供卖家销售评论反馈。只与信誉好的卖家做生意。

（4）如果可能，使用一张有限额的、专门的信用卡来支付。那样的话，就算信用卡被骗了，损失也在限额之内。

在线拍卖是很好的获得物美价廉商品的途径，然而，买家必须小心行事。

3.5.5 防止网络侵犯

防止在网上被骚扰有以下一些原则。

（1）如果在聊天室、BBS等地方，不要使用真实姓名。设立一个专用的不记名电子邮件账号，如Yahoo或Hotmail，并使用假名注册。该策略可以防止网络侵犯者找到你的真实信息。

（2）假如你正遭受网络骚扰，将所有相关电子邮件的电子版和印刷版整理一下，利用一些调查手段进行调查，看是否能够找到嫌疑人。如果找到，可以拿着这些文件到法律部门起诉。

（3）任何时候都不要忽视网络侵犯，根据Halt Online Abuse网2004年的数据统计[①]，现实世界的网络侵犯案件上升了19%。

本章的目的不是耸人听闻，让用户担惊受怕地上网。我家人经常在网上娱乐、购物和获取信息。使用Internet时多留心即可。

3.6 本章小结 >>>

显然，欺骗和身份盗用已成为非常现实的越来越严重的问题。在现代社会，即时信息交互以及在线交易已经开始普及，人们一定要学会保护自己免受欺骗，利用本章介绍的措施保护隐私。在后面练习中，会有机会实践各种防护手段。另外，法律从业人员调查和解决网络犯罪问题也势在必行。

无论对平民百姓，还是执法机关，网络犯罪都是一个新问题。重要的是要理解什么是网络犯罪，什么不是。遗憾的是，网络犯罪会逐渐升级到现实世界的犯罪。

3.7 本章练习 >>>

3.7.1 多选题

1. 常见的Internet投资欺骗是：

① Working to Halt Online Abuse. Accessed April 2011: www.haltabuse.org/

A. 尼日利亚人欺骗　　B. 曼哈顿岛欺骗
C. 哄抬股价　　D. 引诱偷换

2. 不靠谱的投资建议会带来什么问题?
A. 可能得不到声称的利润　　B. 建议可能有失偏颇
C. 建议可能不是从正规渠道来的　　D. 可能会赔钱

3. 为了高价卖出而拉高股价是指:
A. 引诱偷换　　B. 尼日利亚人欺骗
C. 哄抬股价　　D. 华尔街欺骗

4. 避免网络欺骗的最好方式是什么?
A. 如果看起来神乎其神,就可能有问题　　B. 永远不要使用银行账号
C. 只与拥有可信电子邮件的人来往　　D. 不要投资外国生意

5. 下列哪一项不是安全交易委员会对防止投资欺骗所做的提示?
A. 不要在线投资　　B. 考虑投资邀请来源
C. 总是保持怀疑态度　　D. 总是进行调查研究

6. 4 类拍卖欺骗是指:
A. 不发货、不结账、发货到错误地址、不按时发货
B. 不发货、不结账、货物不符、不按时发货
C. 不结账、物超所值、不发货、不按时发货
D. 不结账、货物不符、不发货、物超所值

7. 为了哄抬物价竞标自己出售的物品是指:
A. 投标虹吸　　B. 投标屏蔽　　C. 投标欺骗　　D. 投标捣鬼

8. 以高价投假标阻止其他人投标的行为是:
A. 投标虹吸　　B. 投标屏蔽　　C. 投标欺骗　　D. 投标捣鬼

9. 身份盗用后最可能进行:
A. 非法采购　　B. 降低受害者信用　　C. 防止罪犯调查　　D. 侵犯隐私

10. 根据美国司法部的说法,身份盗用通常是因为:
A. 恶意目的　　B. 对受害者的恶作剧　　C. 经济原因　　D. 恐吓

11. 为什么网络侵犯是一种严重的犯罪?
A. 恐吓受害者　　B. 犯罪的前奏
C. 窃听通信　　D. 身份盗用的前奏

12. 什么是网络侵犯?
A. 任何利用 Internet 发布恐吓信息的行为
B. 任何利用电子通信手段侵犯某人的行为
C. 只用电子邮件发布恐吓信息的行为
D. 只用电子邮件侵犯某人的行为

13. 在界定骚扰时,执法部门通常需要什么事实?
A. 证实有死亡威胁或严重伤害　　B. 可信的死亡威胁或严重伤害
C. 证实有伤害威胁　　D. 可信的伤害威胁

14. 如果在聊天室匿名发帖,有一个匿名发帖者骂你甚至用死来恐吓你,那个人是否犯

了骚扰罪？

A. 是的，任何暴力恐吓都是

B. 可能不是。因为双方都是匿名的，所以这种恐吓不可信

C. 是的，聊天室的威胁与现实中对人的威胁没什么不同

D. 可能不是，因为聊天室的威胁与现实中对人的威胁不同

15. 在美国一个州或地区网络侵犯被认为非法需要什么条件？

A. 本州或地区针对网络侵犯的特别法律

B. 国家针对网络侵犯的特别法律

C. 什么也不需要，现有侵犯法律即可适用

D. 什么也不需要，现有国际网络侵犯法律可适用

16. 防止身份盗用的第一步是：

A. 不是特别需要不要出示任何个人信息

B. 经常检查各种记录查找疑似身份盗用

C. 不要在 Internet 上使用真实姓名

D. 经常检查计算机上的间谍软件

17. 在本地计算机上该如何防护隐私？

A. 安装杀毒软件　　B. 安装防火墙

C. 设置浏览器的安全性　　D. 设置计算机过滤

18. Cookie 是什么？

A. Web 服务器搜集的一小块用户数据

B. 一个小文件，其中包含数据，存在用户的计算机上

C. Web 浏览器搜集的一小块用户数据

D. 一个小文件，其中包含数据，存储在 Web 服务器上

19. 下列哪项对于防护在线拍卖不是很有效？

A. 只竞拍便宜物品　　B. 只使用有名的拍卖网站

C. 只跟信誉良好的卖家合作　　D. 只竞拍比较实际的物品

20. 在聊天室保证自身安全的最重要的原则是：

A. 安装杀毒软件

B. 从不使用真实的名字，不泄露任何真实的个人信息

C. 仅使用加密传输数据的聊天室

D. 仅使用知名网站或公司的聊天室

21. 在网上购物时为什么要使用一张专门的信用卡？

A. 一旦信用卡被非法盗用，能够把损失限定在一定范围内

B. 可以更好地跟踪在线购物记录

C. 一旦被欺骗，可以让信用卡公司来处理

D. 如果需要，可以轻易注销信用卡

22. 网络侵犯案件升级到现实世界犯罪的比例是多少？

A. 少于1%　　B. 25%　　C. 90%甚至更多　　D. 大约19%

23. 如果你在网络上被骚扰，如何与警察配合？

A. 什么都不用做。这是警察的工作，与我无关

B. 将骚扰我的人引到公共场所

C. 保留所有被骚扰的电子副本和实际副本

D. 在网上公布骚扰我的人的个人信息激怒他

24. 防止网络侵犯的最佳方法是：

A. 不要在网上使用真实身份　　B. 总是使用防火墙

C. 总是使用杀毒软件　　D. 不要向别人提供电子邮件地址

3.7.2　练习题

练习 3.1　在 IE 中设置 Web 浏览器隐私

这个过程在本章详细讲述过，这里好好回顾一下。

1. 在 Internet Explorer 中选择 Tools(工具)菜单。选择 Internet Options (Internet 选项)命令。

2. 选择 Privacy(隐私)选项卡。也就是第三个选项卡。

3. 单击 Advanced(高级)按钮。

4. 设置浏览器接受第一方 Cookies；提示第三方 Cookies；接受会话 Cookies。

练习 3.2　使用另一个 Web 浏览器

1. 从 www. mozilla. org 下载 Firefox 浏览器。

2. 设置隐私和安全选项。

练习 3.3　在聊天室跟踪信息

该练习的目的是演示在 Internet 上获取个人信息是多么容易。

1. 进入聊天室。假如对聊天室不是很熟悉或之前没有用过，通过下列网站可以了解这方面的内容。

http://chat. icq. com/icqchat/

www. aol. com/community/chat/allchats. html

www. javachatrooms. net/

www. chat-avenue. com/

2. 注意哪些人使用了真实姓名。

3. 注意哪些人泄露了个人信息。

4. 从那些发布在聊天室的谈话内容中尽量搜集个人信息。

该练习的目的仅仅是展示在网上了解某人信息是多么容易。任何情况下，都不要用这些信息对他人进行骚扰。

3.7.3 项目题

项目 3.1 查找关于网络侵犯的相关法律

1. 利用 Web 网站和相关资源，查找所在州、国家或省关于网络侵犯的法律。

2. 写一篇论文描述那些法律条文及其含义。可以选择总结几部法律的大意，或者深入研究某一部法律。假如选择前者，列举相关法律并描述其涵盖的内容。假如选择后者，讨论该法律作者、法律目的以及法律的相关外延。

项目 3.2 查找拍卖欺骗

访问某一拍卖网站，查找是否有卖家试图欺骗消费者。写一篇论文说明为何该卖家引起了你的怀疑。

项目 3.3 网络侵犯案例调研

1. 利用 Web 查找本章没有提到的网络侵犯案件。下列网站可能会有帮助。

www. safetyed. org/help/stalking/

www. cyber-stalking. net/

www. technomom. com/harassed/index. shtml

2. 写一篇论文讨论该案件，并讨论如何防止和改善案件中发生的情形。

3.7.4 案例研究

有一名疯狂的身份盗用者叫詹尼，受害者叫约翰。詹尼在网络聊天室认识了约翰，约翰使用真实姓名，然而，交谈了一会儿后，他就泄露了一些个人信息，比如婚姻情况、孩子、职业、宗教信仰等。最后，詹尼借口向约翰提供一些信息，比如投资提示，骗取其电子邮件。詹尼得到约翰的电子邮件后，开始频繁通过电子邮件交流，并假装使用自己的真名，这样鼓励约翰也将真实姓名告诉了詹尼，当然詹尼用的是假名玛丽。詹尼现在知道了约翰的真实姓名、居住城市、婚姻状况、职业等信息，而约翰却对詹尼一无所知。

詹尼现在有许多选择，她通过电话簿或 Web 查询，就可以找到约翰的家庭住址和电话号码。还可以通过很多渠道了解约翰的社保号，最直接的方式是在约翰上班时在他家丢弃的垃圾中找一找。然而，如果约翰工作在一家大公司，詹尼就可以找个人打电话声称是约翰的妻子或其他关系不一般的人，要求确认个人信息。假如詹尼够聪明，她就可以轻易得到约翰的社保号。接下来得到约翰的信用报告以及信用卡就是小菜一碟了。相关内容参见第 13 章。

从上面的描述中，考虑下列问题。

1. 在聊天室里，约翰可以采取哪些合理的措施来防护自己的身份安全？

2. 企业老板应该如何防止在无意中卷入身份盗用事件？

第4章

拒绝服务攻击

本章目标

在学习了本章内容并完成所有练习之后，读者将能够掌握如下内容。

- 理解拒绝服务攻击(DoS)是如何进行的。
- 了解几种典型的拒绝服务攻击，例如 SYN 泛洪、Smurf、分布式拒绝服务攻击。
- 如何应对拒绝服务攻击。
- 了解如何防御特定的拒绝服务攻击。

4.1 本章简介

到目前为止，我们已经大体了解了 Internet 上都有什么危险，并学习了基本的防护准则。在第 3 章，还学习了获取目标系统信息的各种方法。现在更深入一些，看看如何进行攻击。本章深入介绍能够对目标系统造成很大伤害的一类攻击，Dos(Denial of Service，拒绝服务攻击)。这种攻击是 Internet 上最常见的，所以理解拒绝服务攻击的机制以及如何防护是非常有必要的。另外，在本章后面的练习中，还会练习如何阻止拒绝服务攻击。在信息安全领域，有一句格言叫“知识就是力量”，这不仅是很好的建议，更是构建整个安全观的原则。

4.2 拒绝服务

综上所述，最常见也是最简单的攻击形式就是拒绝服务攻击。这种攻击不是为了入侵系统以获取敏感信息，而是要让系统崩溃，从而无法响应正当用户的请求；而且这种攻击很容易开展，无须任何技术功底；其本质思想就是认为，任何设备都有负荷限制。例如，小货车只能运输有限的货物、行驶有限的距离。计算机也一样，也有极限。不论是什么计算机系统、Web 服务器，还是网络，都只能处理有限的负荷，计算机系统的工作负荷通常以带多少用户、文件系统大小、数据传输速率、文件存储量等指标来衡量。一旦超过了负荷，再执行操作就无法响应了。例如，可以通过发起大量超出网站处理范围的请求来攻击某一网站，使系

统过载，无法响应其他请求（Webopedia，2004）。这就是拒绝服务攻击，只是通过超负荷的请求，就可以致使 Web 服务器的正当访问被拒绝。

提示：缓冲区溢出

拒绝服务攻击是最常见的攻击形式，其次就是缓冲区溢出了。但缓冲区溢出是专家争论最多的攻击形式。毋庸置疑，了解拒绝服务攻击并掌握如何防御是计算机安全领域非常重要的内容。由于现代操作系统和 Web 服务器不再容易受到影响，所以，这种攻击形式不再那么常见了。唯一执行这种攻击方式的是通过某些应用比如电子商务应用的薄弱环节。

4.3 攻击分析

分析这样的攻击很简单，尤其是在班级环境，只用第 2 章讲的 ping 命令即可。

（1）开启一个 Web 服务器服务（可以使用 Apache、IIS 或任何 Web 服务器软件）。

（2）安排一些同学打开浏览器，并在地址栏输入这台服务器的地址，应该能够正常访问。

现在，就可以进行一次原始的拒绝服务攻击了。第 2 章讲的 ping /h 命令可以显示所有 ping 命令的选项。-l 选项改变发送数据包的大小，TCP 数据包只可以是有限大小，因此，设置发送数据包大小应当尽可能大；-w 选项决定 ping 命令等待目标回应的时间，以毫秒为单位，可以使用-0 让 ping 不等待。然后使用-t 指示 ping 工具持续发送数据包，直到明确让它停止。

（3）打开 Windows XP/Vista/7 的命令提示符（UNIX/Linux 的 shell）。

（4）输入 ping ＜目标地址＞ -l 65000 -w 0 -t 并运行，会看到图 4.1 所示的结果。注意，在图中，ping 的是本机回环地址，试验中可以替换成 Web 服务器地址。

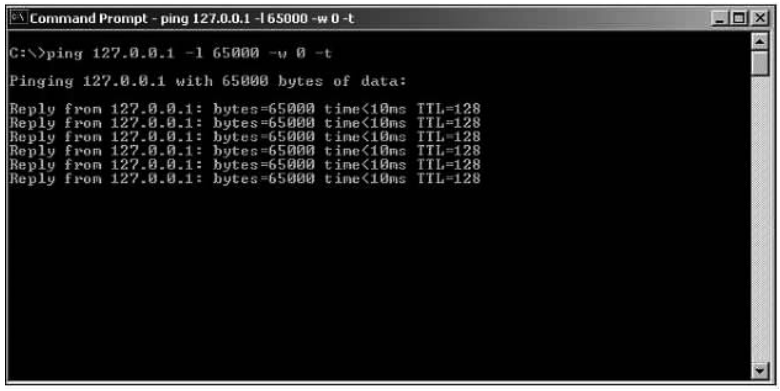

图 4.1　命令提示符里的 ping

运行结果是本机向目标机器不停地发送 ping。当然，仅仅班里的或实验室的一台主机 ping Web 服务器还不足以形成不利影响，然而，可以按照同样的方式一个接一个地让班里的主机都这么做，在添加 3～4 台机器后，再尝试访问 Web 服务器看看效果，直到达到某个

极限(ping 服务器的主机数),就会拒绝访问请求,这时就不能正常访问 Web 服务器了。

究竟用多少主机可以造成拒绝服务,取决于所用的 Web 服务器,要想用少量主机就达到拒绝服务的效果,可以用低配置的 Web 服务器。例如,在一台 CPU 为奔腾 3、操作系统为 Windows 98 的笔记本上运行 Apache Web 服务器,要让它停止对正常请求的响应,大约用 15 台就够了。当然对于选用的 Web 服务器,实际上不会使用 Windows 98 的笔记本电脑中运行。同时,真正的拒绝服务攻击方法比较复杂多样,这只是一个简单的例子,然而,万变不离其宗,核心思想是一样的:用大量的数据包泛洪目标主机,以致它不能响应正当请求。

一般来讲,拒绝服务攻击的过程要复杂很多。例如,黑客可能专门开发一个小病毒向预定目标主机发起 ping 泛洪攻击,一旦病毒传播开来,所有被感染的计算机都会向目标主机发起 ping 泛洪攻击。拒绝服务攻击很容易开展,但防起来就没那么容易了。从大量计算机同时发起拒绝服务攻击的攻击形式叫 DDoS(Distributed Denial of Service,分布式拒绝服务攻击)。

4.3.1　拒绝服务攻击常用工具

拒绝服务攻击像本书讨论的其他安全问题一样,黑客总能找到满足一堆工具,当然,对所有工具分门别类地讨论超出了本书的范畴,为了有较好的效果,这里挑出几个进行简要介绍。本节讨论两个拒绝服务攻击的典型工具,即 TFN 和 Stacheldraht。

TFN 和 TFN2K

TFN(Tribal Flood Network,部落泛洪网络)和 TFN2K 不是病毒,它们常用来进行分布式拒绝服务攻击。TFN2K 是 TFN 的新版本,支持 Windows Server(2003 和 2008)和 UNIX 平台,很容易移植到其他平台,它的一些特点使攻击很容易,检测起来却非常困难,包括发送诱骗信息以避免被跟踪。高手可以通过很多代理同时使用 TFN2K 来攻击一个或多个目标主机。另外,TFN 和 TFN2K 还可以发起 UDP SYN 泛洪攻击、ICMP 泛洪攻击和 TCP SYN 泛洪攻击(本章后续会讲到)。

TFN2K 分两部分工作。一部分以命令驱动的客户端形式运行在主控计算机上,另一部分以后台形式运行在代理计算机上。攻击原理如下。

1. 主控计算机向各个代理计算机部署攻击目标。
2. 代理计算机响应部署,并使用大量数据包向目标发起泛洪攻击。

这个工具通过多代理主机同时向目标发起攻击而使目标系统崩溃。另外,TFN2K 还有一些复杂、有效且实用的反检测措施,使检测变得很困难。

- 主控到代理之间的通信数据是加密的,并且可能夹杂了假数据。
- 主控到代理之间的通信数据和攻击数据可以随机以 TCP、UDP、ICMP 数据包发送。
- 主控可以伪造其 IP 地址(电子欺骗)。

Stacheldraht

Stacheldraht 在德语里是“带钩的电线”的意思,它把另一种常见工具 Trinoo DDoS 的特点和 TFN 分布式拒绝服务攻击工具的源码结合起来。与 TFN2K 类似,Stacheldraht 加

密主控和代理的通信数据，同时还能够自动更新代理程序。

Stracheldraht能够发起一系列攻击，如UDP泛洪、ICMP泛洪、TCP SYN泛洪和Smurf攻击，同时能够自动伪造源IP地址。

4.3.2 拒绝服务攻击的弱点

从攻击者的角度来讲，拒绝服务攻击的不足是要求必须能够持续发送泛洪包，一旦停了，目标系统一般就会恢复正常。然而，目前拒绝服务攻击/分布式拒绝服务攻击常与其他攻击手段结合使用，例如禁用劫持TCP连接的一端，或者阻止服务器之间的认证或登录。

假如黑客采用分布式攻击，那么，当管理员或所有者发现计算机已被感染，就会采取一些措施来删除病毒，从而阻止攻击。假如黑客要从本机发起攻击，必须要清楚每一个数据包都有可能被跟踪到源IP地址，这就意味着，单个拒绝服务攻击的黑客可能最终会被抓到。因此，分布式拒绝服务攻击越来越流行，其特点在本章后面介绍。

4.3.3 拒绝服务攻击

拒绝服务攻击的基本原理并不复杂，对于发动拒绝服务攻击的攻击者来说，真正的问题是如何才能避免被发现。下面说明拒绝服务攻击的具体类型，并结合典型案例来讨论，这会更加深入地了解拒绝服务攻击这一Internet威胁。

TCP SYN泛洪攻击

一种流行的拒绝服务攻击方法是SYN泛洪(SYN flood)。要理解这种攻击，就需要了解服务器连接建立的过程。在TCP协议中，客户端与服务器之间发起会话时，会使用1位标记的数据包发送给服务器，这就是SYN。SYN是synchronize(同步)的缩写。这个包要求目标服务器对通信进行同步。随后服务器分配适当的资源，然后用SYN和ACK(确认)标记组发送给客户端。客户计算机随后用ACK标记来响应。这便是三向握手。过程如下：

1. 客户端设置SYN标志发送一个包。
2. 服务器为客户端分配资源，然后设置SYN和ACK标志进行响应。
3. 客户端设置ACK标志来响应。

网上有大量知名的针对Web服务器的SYN泛洪工具，这种方法受欢迎的原因就是，任何以TCP为网络协议通信的计算机都有此弱点，而TCP协议应用又相当普遍，所有连接到Internet的机器都使用TCP通信。然而，尽管如此，还是有一些方法和技术可以防止这种攻击。最简单的防御方式是第12章讨论的防火墙。然而，在一个服务器上，可以实现几种方法和技术，以防止被攻击。基本的防御方法如下。

- Micro blocks。
- SYN Cookie。
- RST Cookie。
- 编辑堆栈。