信息泄露问题分析与探究

李俊莉 著

中原出版传媒集团

信息泄露问题分析与探究

李俊莉 著

中原出版传媒集团

图书在版编目(CIP)数据

信息泄露问题分析与探究/李俊莉著. —郑州:中原出版传媒集团,中原农民出版社,2008.9
ISBN 978-7-80739-347-4

Ⅰ.信… Ⅱ.李… Ⅲ.计算机网络-安全技术-研究
Ⅳ.TP393.08

中国版本图书馆 CIP 数据核字(2008)第 133842 号

出版:中原出版传媒集团　中原农民出版社
(地址:郑州市经五路 66 号　电话:0371—65751257
邮政编码:450002)
发行单位:河南省新华书店
承印单位:河南省诚和印制有限公司
开本:850mm×1168mm　1/32
印张:12　**字数**:301 千字
版次:2008 年 9 月第 1 版　**印次**:2008 年 9 月第 1 次印刷

书号:ISBN 978-7-80739-347-4　**定价**:26.00 元
本书如有印装质量问题,由承印厂负责调换

序　言

随着网络技术的迅猛发展和广泛应用，人们在得益于网络信息技术带来的便利和快捷的同时，也在面对着信息泄露所带来的隐私权的侵扰。现代技术在拓展人类生活空间的同时，也带来了生活空间的透明化。电磁泄露、人肉搜索、信息共享等信息泄露形式，已使人类没有了自我的一片空间，信息泄露带来的社会问题日益突出，面对这种情况，学界急需在技术、法律和道德各种层面给予更多的关注，来化解科技利用与个人信息安全保护存在的矛盾。鉴于此，作者精心撰写了《信息泄露问题分析与探究》这一专著。

《信息泄露问题分析与探究》这一著作，涉及多个学科领域，这些领域包括计算、数学、电子、数据挖掘技术和法律等。该著作的研究具有一定的深度和广度。在技术方面，作者参考研究了大量国内外书籍及互联网上的最新资料，力求紧跟国内外技术，全面、系统地反映出该研究领域的最新动态，分析预测了该问题未来的发展方向。在有关立法和法规方面，作者对我国现有的信息泄露造成的隐私权侵犯保护的法律状况进行了研究和思考。

《信息泄露问题分析与探究》在很多方面都是独特的，在其中三个方面尤为突出：首先，它研究数据处理所有关键阶段的信息泄露问题——从击键到传递过程再到接收的最终结果，从这些阶段分析了泄露的原因和原理。其次，它概括了每个网络互联阶段及整个过程中主要的固有的信息泄露问题，从攻击者行为和防御者弱点中研究涉及的安全问题。最后，它概括了各类泄露形式，揭示了各种信息泄露利用和个人隐私保护的对抗。当然，这些问题是当前信息安全领域大多数人在讨论和研究的问题。但从这一角度

出发的研究尚处于初始阶段，《信息泄露问题分析与探究》一书，正是从这一视角切入，对新形势下信息泄露犯罪进行了系统全面的探索，是一部揭示这一领域存在的问题的专门性著作。该著作具有原创性的思维和独特的研究空间。该成果的适时推出，将有利于我国信息发展战略的实施，为解决科技利用与法治时代适应性提供了理论研究基础，为研究新时代的隐私权保护和防范信息泄露等提供了借鉴，无论是从信息技术研究还是从犯罪学体系完善的理论发展角度与控制犯罪实务工作的客观需要来看，都具有非常重要的意义。

该著作内容丰富，不仅涵盖了相关领域的理论和技术，而且内容之间衔接紧凑、合理，构成了从信息泄露到犯罪取证再到法律保护较为完整的研究体系。该著作在理论和技术方面均有所突破和创新，适合于信息泄露与隐私保护的进一步研究，可作为执法中的参考和借鉴。

诚然，鉴于信息泄露问题研究的前瞻性，书中存在不足之处是难免的，但瑕不掩瑜，该专著仍不失为一部计算机信息技术研究领域的力作。

北京大学法学院　教　　授
博士生导师　张玉镶

2008 年 8 月于燕园

目　录

第1章　间谍软件——从广告软件到恶意威胁

对于流感病毒大家都听说过或感受过，它有多种变种形式，这从本质上说是一个典型的自然现象。但是可以想象，如果一个人造的恶意应用程序从默默无闻演变为一支破坏力很强的力量，将会带来多少损害。

您到商场购物当达到一定金额时，买家会给您办理金卡或银卡，以给您一定的优惠，但需要填写有关您的包括收入、学历、住址等的信息卡片。随之而来的是不断的骚扰电话和相关产品的关怀推荐，这一切您似乎都经历过，也感受到了优惠后的陷阱和苦头。而对于商场来说，您的购买信息比您购买的商品更有价值，大多数情况下，商场会把这部分折扣补到该商品的原始价格中，或者分摊到商店其他商品的价格中，所谓的价格不会对商店造成任何损失。

零售商们以备忘录般精密的形式监控并收集有关消费者的购买信息。

1.1　从商业需要到产生威胁

随着社会的发展，当各种供需达到平衡和趋于饱和之时，市场的竞争就加剧了。形形色色的公司已经花费了数十年时间来调整它们对市场的了解，找出消费者的真实需要。这些公司已经投入了数百万美元、无数人力、时间到对消费者购买习惯的心理分析的研究工作中，以便把它们的资源明智地投入到研发中去，从而使产品在投放市场之后获得较大的成功机会。随着Internet的商业运

用,各种公司尝试在使用 Internet 作为一种业务工具和明智而高效地利用电子商务作为业务的一部分之间找到平衡时,Internet 迫使它们重新组织,找出使用和利用这种全新的信息媒介的方法,就衍生出了间谍软件。间谍软件的定义是收集有关目标用户或系统的数据并将其发回给另一方的软件。而现今的间谍软件通常都是有害甚至是恶意的。

1.1.1 赢利的背后

在市场中,公司都想要确认它们拥有的产品或服务的业务消息传达到了正确的群体。某些公司花费甚至数百万元进行人口统计学研究,以确保它们的广告和商品能够被合适的人看到。您不会在专门的汽车杂志中看到最新的儿童视频游戏广告,也不会在儿童网上的卡通马拉松节目间隙看到治疗精神障碍的药物广告。南辕北辙的做法会起不到营销效果,如果每个人都选择了正确的做事方式,至少会事半功倍。

Internet 创建的首批"广告"模型是垃圾电子邮件。无需花费任何实际代价便可把一条电子邮件消息群发给世界上数以百万计的人。如果有 10 个人、100 个人或者几千个人回信,就是垃圾邮件广告运动的巨大胜利。但是,合法公司是不会愿意把它们的声誉或产品与垃圾邮件营销挂上钩的。公司为快速适应 Internet 的出现,业务人员努力寻找通过 World Wide Web 有效地销售或推销他们商品的方式。没过多久,一些人发觉可以对 Web 冲浪和 Internet购物进行监控,并从中挖掘出大量有用的用户信息。通过应用相同的技术来追踪信息化程度较低的零售店中的入口数据,再结合电子数据和数据库存储的速度与效率,公司可以再次将其营销目标定位到那些最感兴趣的人身上。

当业务人员在 Internet 上寻找有效营销和销售产品的方式时,软件开发人员也在努力。在软件销售的激烈竞争中能够取得良好开端的大型软件开发人员要具备以下三种素质:小有名气、认

同大型零售连锁店的方式和经手的营销额达到百万美元。

一些个人和小软件公司常会赠送他们的软件，这类软件叫做免费软件。然而，大多数人和公司是想从这些产品中获得一定的经济回报。他们没有选择赠送，而是使用了共享软件发布形式。

共享软件仍然是免费发布的。如果用户觉得该产品有一定的价值，要选择继续使用，就需要为该产品支付一定的费用，但是，还有一些软件并不依赖于用户的诚信，而是采用了另一种业务模型，叫做广告软件。广告软件就是用户无需为使用软件支付费用，但是该软件中包含了某些形式的广告，比如标题或弹出广告。用户免费使用软件，而软件厂商从软件带来的广告收入中赚钱。

经过不同消费人群统计选定营销目标，比仅仅群发广告并希望需要的人看到广告更有价值。广告软件开发人员意识到，如果他们能够把广告发布给正确的用户群，就可以向登广告者收取更多的费用。因此，许多软件厂商开始编写追踪用户 Web 浏览器的软件，广告软件能够收集用户的有关信息，并把这些数据发回给自己，并在广告软件中针对特定需求的用户定制要显示的广告。

1.1.2 什么是 Cookie

软件厂商编写的追踪用户 Web 浏览器的软件 Cookie 是一个文本文件，用于保存有关用户的简单信息，它不能执行。这些 Cookies 支持用户定制更加个性化的 Web 冲浪体验。广告软件厂商进一步深化了 Cookie 的概念，开始使用 Cookie 文本文件记录 URL 历史和他们能够提取的其他信息，从而记录用户感兴趣的 Web 站点类型。然后，他们就能够应用收集到的信息，将广告定位到对其更加感兴趣的用户。如图 1 - 1。

Cookie 有两种类型：会话型和永久型。会话型 Cookie 通常跟踪用户的浏览会话并存储在内存中。当关闭浏览器的时候，这些 Cookies 都将丢失，而内存或者交换文件中还有一些残留的信息。

永久型的 Cookie 都被写入硬盘并以文本文件的形式存储在前述的 Cookies 目录下。浏览会话中通常用永久型 Cookie 来保存状态信息。例如,您在浏览 www. taobaowang. com 时,发现购物车中有几天前选购的物品,www. taobaowang. com 就是用 Cookies 来识别用户的。

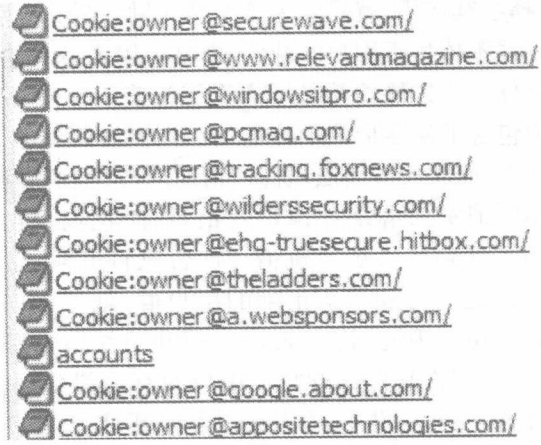

图 1 - 1　Cookies 列表片段

Cookie 不仅能识别出访问过的网址,而且可以指出在该网址进行的操作,有时还能提供用户名、密码等用户信息。Cookie 限用于一台主机并且设有有效期限,但是并没有对 Web 站点写入 Cookie 的文本作任何限制。每个 Cookie 对应一个 username@Sitename. txt 文件,包含一系列记录。每一条记录包括以下几个方面:

· 关键字:记录中存储的变量名。

· 值:关键字的值。

· 主机:写入该记录的主机的名称。

· 安全性:有 True 和 False 两个值,取值依赖于 Cookies 是否是从 SSL 下载的。

· 修改时间:最后一次修改记录的时间,同时也指出最后一次访问的站点。

· 有效期:Cookies 在有效期之后不再有效。

缺省情况下真实信息都是编了码的,因此需要使用 Cookie 查看器查看 Cookies。Cookies 文件中的信息常常被用来进行伪装性攻击。

广告软件和间谍软件的增多,以及追踪 cookie 以收集有关用户的信息与第三方共享这种做法,使得 cookie 声名狼藉。许多人认为 cookie 是一种恶意软件,事实上 cookie 本身是造不成任何危害的,也无所谓好坏,只是缘于人们利用它做了什么。

1.1.3 早期的影响

开始时,部分广告软件厂商会告知用户监控和收集有关他们的信息的目的。然而,这类告知信息通常深藏在最终用户许可证协议(End User License Agreement,EULA)中,很少有用户在安装软件之前会真的去阅读它。从技术上讲,只要接受 EULA 和安装软件,这些用户就认可了把他们的个人数据发送给广告软件厂商。一些厂商没有提供有关数据收集的任何通知,这样的收集行为是没有授权的,而是偷偷摸摸地监控用户的冲浪和计算机使用习惯。最终,监控和追踪行为已经超过了简单地追踪 Cookie 的范围,演变成为更加隐蔽的工具,比如键盘记录器和类似于特洛伊木马的程序。

1. 首次出现

首次公开使用间谍软件这个词是在 1996 年 10 月,有人在 Usenet 上发表了一篇文章,指称 Microsoft 在软件行业中具有独裁和垄断地位,而且它提供的软件可能会把某些信息发回给 Microsoft,该文章称这些软件为"间谍软件"。实际上这是在对 Microsoft 业务模型的一次玩笑式的批评。

2. 影响

大多数间谍软件在编写时都没有什么软件质量保证,或者在发布之前没有进行足够的测试,所以往往很容易给总体系统性能带来巨大的影响,它使用户的计算机系统变得缓慢甚至使系统整个崩溃。无论间谍软件有多小或多隐蔽,它必须使用内存和处理器资源才能进行追踪和监控,而且在某些地方必须使用网络带宽与"总部"进行通信。

间谍软件的其他主要影响是危及用户的隐私。大多数用户都期望能够在 Web 上自由冲浪、阅读邮件和在线购物的行为不会被公开。当用户意识到监控和追踪行为时,为换取使用便宜或免费的软件他们会选择接受,间谍软件在用户不知情或未经用户许可的情况下安装到他们的计算机上监视计算机行为就是一种隐私侵犯,这种无形的信息泄露形式使人们对互联网的使用变得谨慎。

1.1.4 早期的预防手段

要防范威胁首先要避免安装不需要的广告软件和间谍软件,要安装有名的开发商出品的软件和访问有名的 Web 站点,以及在仔细阅读 EULA 中的条款后再选择是否安装,这应该是最好的方法。

早期,针对间谍软件产生了反间谍软件,可有效删除已安装到电脑中的间谍软件。反间谍软件的早期形式实际上就是间谍软件删除工具,不具备任何实时检测或阻止功能。用户需要定期运行这些工具来清除系统中累积的广告软件和间谍软件,但是用户在删除这些软件时仍然要慎之又慎。首个官方间谍软件的删除软件是 OptOut(如图 1 -2),其作者是 Gibson Research(www. grc. com)的 Steve Gibson。Gibson 发现了他大量的个人信息和 Web 冲浪习惯被记录下来并发回给第三方的情况,感到十分气愤。他原本希望从该产品上获利,但是来自免费软件如 Lavasoft 的 Ad - Aware 等软件的竞争,使得 Gibson 这个赢利计划成为泡影。尽管这样,