<<安全之美>>

图书基本信息

书名：<<安全之美>>

13位ISBN编号：9787111334774

10位ISBN编号：7111334779

出版时间：2011-4-28

出版时间：机械工业出版社华章公司

作者：Andy Oram,John Viega

译者：徐 波,沈晓斌

前言

前言　　如果有人相信新闻标题可以揭示趋势，那么对于计算机安全领域而言现在是个有趣的时刻。
当《安全之美》出版时，我阅读了一个能够打开麦克风和摄像头并窃取数据的软件的部分代码。
这个软件在103个国家的超过1200台计算机上安装，尤其是在大使馆和其他敏感的政府部门。
另外，一家法庭支持美国调查官在没有得到授权的情况下可以查看电话和Internet记录（只要交谈的另一端是在美国境外）。
最新公布的漏洞包括Adobe Acrobat和Adobe Reader的一个缓冲区溢出漏洞（当前常称为漏洞攻击，英文为exploit），允许攻击者在用户打开PDF之后在用户的系统中通过用户的权限执行任意代码。
新闻标题实际上并不能很好地提示趋势，因为在漫长的历史中，它是由微妙的革命性变化所驱动的，而这种变化往往只有少数人注意到，例如编写本书的前沿安全专家们。
读者可以在本书中发现安全威胁的发展方向以及针对它们的响应。
我在第一段中所提到的所有令人惊恐的新闻对于安全领域而言只是普通的业务而已。
是的，它们正是我们应该担忧的安全趋势的一部分，但我们还需要注意更新的、更不易被觉察的漏洞。
《安全之美》的作者们数十年来一直奋斗在第一线，努力发现我们的工作习惯中的脆弱环节，并提议用非常规的方式来处理它们。
为什么安全是美丽的　　我要求安全专家John Viega想方设法为本书寻找一些作者，以便向普通计算机用户提供一些与安全有关的观点。
除了在媒体上所看到的骇人听闻的关于网络入侵和盗窃的新闻之外，普通人一般都觉得安全是一件乏味的事情。
对许多人而言，安全就是系统管理员喋喋不休地提醒他们创建备份文件夹，无穷无尽的在网页显示之前跳出来的要求输入密码的对话框。
办公室职员每次抄读办公桌边的笔记本上所记录的密码时都怒目圆睁小声咒骂（笔记本就放在打印出来的预算材料的上面，事实上办公室管理人员要求应该将它锁在抽屉里面）。
如果这就是安全，那还会有谁想从事这个职业呢？
谁会从O'Reilly购买一本关于安全的书呢？
谁会一次花费半分钟以上的时间去思考安全呢？
对于那些肩负创建安全系统任务的人们，他们所付出的努力看上去是毫无希望的。
站在旁边的人不会对他们的工作提供任何协助，业务经理也拒绝在安全上多花一分钱。
程序员和系统管理员由于他们必须使用的工具和语言存在没完没了的零日攻击和未打补丁的漏洞也逐渐变得懒散起来。
这就是为什么关于安全的书卖得很差（尽管在过去的一两年里销量有所上扬）。
关于如何入侵系统的书要比关于如何保护系统的书好卖得多，这个趋势着实令我震惊。
是的，本书应该改变这个现象。
它应该向读者展示安全是一项最为激动人心的职业。
它并不枯燥，也没有太多的官僚主义，更没有太多的约束。
事实上，它和其他技术一样充满着想象力。
多年以来，我编辑过的大多数编程书籍都提供了关于安全的内容。
这样的内容当然是非常实用的，因为它们允许作者讲述一些基本原则和一些良好习惯。
但是，我已经对这种做法感到厌烦，因为它为安全话题划了一条分界线。
它所灌输的都是一些老生常谈的安全观点，是一些锦上添花或者事后诸葛亮的东西。
本书将颠覆这些观念。
John为本书选择了一些作者，他们已经在安全领域证明了自己具有独特的观点，并且有一些新的思路要和大家分享。
有些作者设计了数以千计的人所依赖的系统，有些作者在大型公司担任高管职位，有些作者曾为法庭

作证并为政府部门工作。
所有的作者都在寻找普通人所不知道的问题和解决方案，但是这可能需要几年的时间才会收到成效。
　　本书的作者指出：有效的安全需要你始终保持警惕。
它会打破技术、认知和组织结构的边界。
安全界的黑帽们千方百计通过创新来取得成功。
因此，负责防御他们的人们同样需要创新。
　　本书的作者肩负着世界范围内的信息安全使命，让他们抽出时间编写本书是一件很困难的事。
事实上，许多作者在平衡本职工作和本书的写作任务时感受到了压力。
但是，他们所花的时间是值得的，因为本书将会促进他们实现更远大的目标。
如果有更多的人对安全领域产生兴趣，决定进一步对它进行探索，并向尝试通过组织上的变化以实现更好保护的人们给予他们的关注和支持，这本书就值得作者所付出的心血。
　　2009年3月19日，美国参议院商业、科学和交通委员会举行了一个听证会，它的主题是信息技术专家的缺乏以及这种现象对美国的网络安全的危害。
让学生和专业人员对安全问题产生兴趣是一项极为迫切的需求，本书就代表了迈向这个目标的一小步。
　　本书的读者　　《安全之美》适用于那些对计算机技术感兴趣并希望在最尖端领域体验生活的人们。
本书的读者包括可能追求职业生涯的学生、具有一定编程背景的人们以及对计算机有着适度或深入了解的人们。
　　本书的作者在解释技术时尽量放低门槛，使相对新手级的读者也能领略到攻击和防御活动方式的感觉。
专家级的读者能够更多地享受讨论的乐趣，因为本书能够加深他们对安全原则的理解，并提供了未来研究的指导方针。

<<安全之美>>

内容概要

大多数人不会太关注安全问题，直到他们的个人或商业系统受到攻击。
这种发人深省的现象证明了数字安全不仅值得思考，而且是个迷人的话题。
犯罪分子通过大量创新取得成功，因此防御他们的人们也必须具有同样的创新精神。
《安全之美》包含以下内容： 个人信息背后的经济：它的运作方式、犯罪分子之间的关系以及他们攻击猎物的新方法。
社交网络、云计算及其他流行的趋势如何帮助或损害在线安全。
度量指标、需求收集、设计和法律如何将安全提高到一个新水平。

作者简介

译者：徐波 沈晓斌 编者：（美国）奥拉姆（Andy Oram） （美国）John Viega

<<安全之美>>

书籍目录

章节摘录

版权页：插图：1.1.3 客户的习得性无助无从选择正如我们所看到的那样，Micfosoft在向后兼容方面作出的选择所导致的不良安全问题可能会让他们的顾客在环境、技术能力以及接受改变的意愿方面产生自暴自弃的观点（不管是否正当）。
我把当前网络上的另一个（甚至更大的）安全问题归因于开发商的习得性无助和顾客的无从选择这两个因素的结合。
大量的审查显示，大多数网络交换机的生产商有意把交换机设计为“失败时打开”而不是“失败时关闭”。
交换机用于在数据链路层上的系统之间移动数据包。
在这种情况下，“失败时关闭”意味着设备要么关闭并停止发挥作用，或者以一种“安全的”方式停止操作。
这样，数据就不会通过存在问题的系统被传递。
反之，“失败时打开”意味着系统停止执行任何智能功能，而是盲目地发送它从所有端口所接收到的数据包（注3）。
在本质上，“失败时打开”的交换机相当于把自身变成了一个哑的集线器。
如果只想消极地嗅探自己并不想要的网络交通，那么哑的集线器可能正是我们所需要的。
功能正常的交换机试图只把流量发送到合适的目的地。
许多机构觉得消极的网络嗅探并不是实实在在的威胁，因为许多交换机都是这样运行的。
但在当前，把一个嗅探器连接到一个被交换的LAN并观察自己不应该看到的数据是极为常见的做法，常常会导致该机构的网络部门的极度惊奇。
他们并没有意识到生产商不惜一切代价避免连接断开的决定（很可能是害怕顾客由于间歇性中断而产生的狂怒），因此当交换机在遇到缺陷、安全攻击或者对某些数据包的处理缺乏明确的指令等事件时，就把交换机恢复到哑的广播模式。
换句话说，生产商安静地为他们的顾客作出了最适合顾客的决定。
我相信如果顾客能够决定哪种方式更适合自己的利益，无疑会让他们处于更加有利的位置。
虽然对于装配线而言，让交换机在失败时打开无疑要比在失败时关闭更合适，但也有一些情况下交换机用于分离重要的流量并隔离内部的域和系统。
在这种情况下，对于顾客而言，最好的方式就是交换机在失败时关闭并发送一个警报。
顾在至少应该拥有选择的权力。

媒体关注与评论

通过阅读这本经过深思熟虑的作品，读者可以摆脱安全领域闪烁着欺骗光芒的心理恐惧，转而欣赏安全的微妙美感。
本书描述了安全的阴和阳，以及引人注目的破坏性和闪亮光辉的建设性之间剑拔弩张的气氛。
”　　——Gary McGraw，Cigital公司CTO，著名安全技术图书作家

编辑推荐

《安全之美》：大多数人不会太关注安全问题，直到他们的个人或商业系统受到攻击。
这种发人深省的现象证明了数字安全不仅值得思考，而且是个迷人的话题。
犯罪分子通过大量创新取得成功，因此防御他们的人们也必须具有同样的创新精神。

版权说明