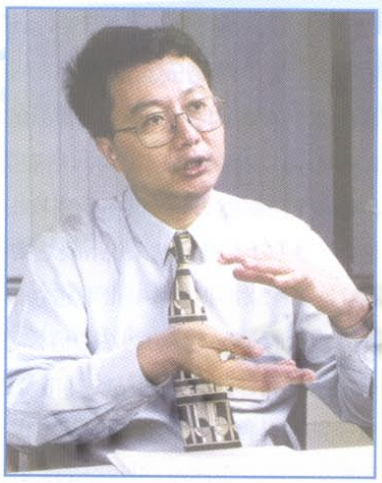
网络安全的保卫者

——访方正技术研究院副院长邹维

施 婉



邹维

1964年，出生重庆

1985年，毕业于南京大学计算机科学系

1988年，在中国科学院获硕士学位。

后来在中科院和外企工作，一直从事软件的研究和开发，曾获国家科学进步二等奖。

1995年，加入方正，从事软件开发及技术管理工作。

现任方正技术研究院副院长

沉稳内敛，学者风范，具有科学和人文精神

互联网无疑是当今社会最显著的特征，以其飞速的发展和无限的商机受到整个社会的关注。北大方正集团也不例外，继在出版业创造了辉煌业绩，又在广播电视领域大力拓展之后，方正又以其技术优势全力进军互联网。方正将自己定位为具有方正特色的电子商务的驱动者，方正技术研究院在这一整体战略中担负着互联网技术的全面研发工作。副院长邹维直接领导的互联网产品部专为电子商务的运营者提供技术和服务。其中，网络安全是一个重要的研究方向，他们推出的SHARKS网站安全解决方案在网络安全领域独树一帜。

一 网络安全问题的由来

网络安全是信息安全的一部分。从物理结构来看，网络是由节点和传输的线路所组成的一个开放体系，所以网络安全包括节点的安全和传输方面的安全，这种安全风险一方面来自系统本身，另一方面来自外界攻击。

自互联网诞生之日起，网络安全问题就一直存在。就像邹维先生所形容的，网络安全与网络的发展永远是矛与盾的关系，处在一种动态的平衡之中。目前互联网的安全防御能力非常脆弱，随着网络的飞速发展，安全问题日益突现。尤其是进入新世纪以来，黑客袭击事件不断发生，使网络安全再一次引起了世界各国的普遍关注。随着国家和企业在政治、经济等方面对网络环境和网络信息资源依赖程度的加深，涉及国家安全和社会公共安全的所有重大问题，都会在网上表现出来。网络安全攻防甚至将会成为一个国家未来战争的一种手段。

网络的安全目标

目前网络安全问题所产生的威胁，可以归纳为以下一些类型：黑客非法侵入，破坏计算机信息系统；网上制作、复制、传播和查阅有害信息；利用计算机实施金融诈骗、盗窃、贪污、挪用公款；非法盗用使用计算机资源，如盗用账号、窃取国家秘密或企业商业机密等；以及利用互联网进行恐吓、敲诈等其他犯罪活动。

为了防止以上情况的发生，网络在设计时就应该达到这样的安全目标：身份真实性，能对通讯实体身份的真实性进行鉴别；信息机密性，保证机密信息不会泄露给非授权的人或实体；信息完整性，保证数据的一致性，能够防止数据被非授权用户或实体建立、修改和破坏；服务可用性，保证合法用户对信息和资源的使用不会被不正当地拒绝；不可否认性，建立有效的责任机制，防止实体否认其行为；系统可控性，能够控制使用资源的人或实体的使用方式；系统易用性，在满足安全要求的条件下，系统应当操作简单、维护方便；可审查性，对出现的网络安全问题能够提供调查的依据和手段。

黑客——网络安全的最大威胁

近年来，从著名商业网站到政府重要部门，黑客攻击事件在世界范围内不断发生，尤其今年二月，美国Yahoo等8家著名大型网站相继被黑客攻击，导致服务中断，造成12 亿美元以上的经济损失。与此同时，国内一些著名网站也遭受到黑客袭击。此外，美国在线AOL六月被入侵，部分用户资料被窃取；Slashdot.org网站被攻击，导致服务中断，这个站点据说是聚集顶尖电脑高手最多的地方，却无法抵挡来自网络黑客的攻击。俄罗斯的网络攻击者Maxus从著名电子商务站点CDUniverse上盗窃了所有用户资料，以此向CDUniverse敲诈巨款，在要求未得到满足的情况下，他在自己的站点上公开了所有的信用卡号，受影响的人数超过30万。

这样的例子不胜枚举，显然黑客已成为网络安全的最大威胁，他们是互联网时代的一个特殊人群，在虚拟世界中随心所欲。邹维先生对黑客有独到的理解，他认为英文中黑客有两个概念，hacker和cracker。hacker是这样一类人，他们对钱财和权利蔑视，而对网络非常专注，他们在网上进行探测性的行动，帮助人们找到网络的漏洞，可以说他们是这个领域的绅士。但是cracker不一样，他们要么为了满足自己的私欲，要么受雇于一些商业机构，具有攻击性和破坏性，从简单修改网页到窃取数据，甚至破坏整个网络系统。由于其危害性较大，cracker已成为网络安全真正的，也是主要的防范对象。

正是由于黑客的存在，极大地推动了网络安全领域技术的发展，也刺激了网络安全市场的形成。

网络安全与电子商务

网络安全问题对于电子商务尤其显得重要，因为开展电子商务的关键问题就是商务活动的安全性。不久前，信息产业部电子信息中心和蓝田市场信息公司针对网民做了一项市场调查，结果显示，最让网民担心的网络安全。其中对网上交易的安全性，担心的网民数已经超过了80%。可以想象，如果没有足够的安全保障，要想在世界范围内开展大规模的电子交易活动，建立网络银行，或是企业与企业在网络上直接进行商务活动，将是非常困难的，因为谁也不会在毫无安全保障的情况下将钱随便乱扔。

电子商务与传统商务活动的安全策略有很大差别。传统商务活动大多是面对面进行的，而电子商务则大不相同，其商务活动的安全性主要表现为：有效性，保证商务活动有效进行；保密性，对信息的存储和传输进行控制，对商务活动的有关信息加密；完整性，电子商务信息要求完整，不可被修改；不可否认性，通过数字签名、数字认证等手段保证网络信息的不可否认。

方兴未艾的中国电子商务市场对网络安全的需求尤为突出。企业与消费者对电子交易安全的担忧是必然的，如何改进电子商务的现状，让用户不必为安全担心，是推动安全技术不断发展的动力。

二　网络安全现状

网站连续受到攻击的事实说明网络安全的现状令人堪忧。据调查显示，我国90%以上的网站安全意识不够，40%以上网站毫无防御能力，仅仅在受到攻击时，才开始进行安全维护。事实上，对网站来说，缺乏安全意识是非常危险的，因为在互联网世界中，很难建立信任。当网站承受不住外界攻击时，势必影响网站的信誉，而且一旦受损，将很难重新建立，这对于网站的打击是毁灭性的。

网络安全防护是网站稳定运行的基本保证。邹先生认为建立完善的网络安全体系，对现今的互联网企业来说势在必行。网站日常的维护工作已经比较繁重，很难再分出一部分资源从事专业化非常强的网络安全维护工作。另外，这也不符合社会分工越来越细的趋势。所以对于一个网站来讲，最好的方式是将安全业务外包，由网站系统分析员和专业从事网络安全服务的公司配合一起来做。

随着互联网和电子商务的发展，以及黑客攻击事件的不断发生，网络安全的市场从今年开始大规模形成，并显示了无比的前景。方正在这个方向的投入是非常有战略眼光的。据邹先生讲，方正首先将目标定位在网站安全，接下来将扩展到企业级的网络安全，最后是整个电子商务的安全。

在谈到我国政府对网络安全的重视程度时，邹先生认为政府还是非常重视这方面的工作，正在积极制定相应的法规。邹先生一直认为，在网络安全方面我国只有在加密解密的算法、安全信息平台等方面拥有自己的核心技术，才能保证国家未来的经济、政治秩序能够正常运行。他同时也希望国家在政策法规方面能够给予企业更多的支持。

三　方正SHARKS网站安全解决方案

网络安全技术涉及的内容是非常广泛的。从广义上讲，网络安全技术主要包括以下几个方面：主机安全技术、身份认证技术、访问控制技术、密码技术、防火墙技术、安全审计技术、安全管理技术、系统漏洞检测技术、以及黑客跟踪技术等。

网络安全市场的形成，吸引了大批科技公司的投入，但大多数是沿着防火墙等某一技术方向发展，产品较为单一。方正凭借雄厚的技术实力，根据互联网发展的需要，适时提出了方正SHARKS网站安全解决方案。与传统的企业网络安全解决方案不同，SHARKS尤其注重解决网站所遇到的特殊安全问题。它不仅仅是一个防火墙，而是由里至外全方位、立体的一整套网络安全解决方案和服务。SHARKS功能强大，除安全问题之外，同时解决了Internet服务商所面临的其他问题，诸如可扩展性、高可靠性、以及远程管理等等。SHARKS的安全模块包括Fire Bridge，Network Intrusion Detector，System Intrusion Detector，Active Alert，Passive Logger，Integrity Checker和VPN等，是一个安全、高可靠性、高可伸缩性且易于远程管理的集群平台。据悉，SHARKS网站安全解决方案已经申请了国家计划创新项目。

Fire Bridge

Fire Bridge是方正首创性提出的针对网站设计的防火墙。这种防火墙能够有效抵御DDoS（分布式拒绝服务攻击）的攻击。正是这种攻击手法于今年二月致使国际上著名网站Yahoo等蒙受了巨大损失。

Fire Bridge还具有其他方面的优势。首先是透明接入，Fire Bridge采用了独特的桥方式作为网站专用的防火墙产品。由于自身不存在IP地址，Fire Bridge不可能成为网络攻击的目标，在保证自身安全性的前提下，为系统树立了一道外来攻击者看不到的屏障，显著提高了整个网络的安全程度。其次，Fire Bridge支持即插即用，对于原有系统的干扰减低到最低限度，无需更改任何网络配置。它提高了防火墙产品在网站的应用效率，去除了许多作为网站安全防护的根本不需要的功能，如内部的访问控制等，把相关的功能分离出去，以更好的产品形式（Anti Port Scan等）出现，使产品的性价比大大提高，减少了用户不必要的投资。

预警及应急响应功能

在网站遭受攻击的初期，方正SHARKS中的Network Attack Detector和System Attack Detector就可以察觉95%以上的攻击，并通过Active Alert报警，同时做出应急反应。

一般网络攻击要想成功，黑客都要扫描目标服务器端口，确定服务器上所运行的服务，并试验各种攻击方式，直至攻破。可以看出，如果进行网络方案设计时就考虑到预警功能，那么在黑客攻击的早期就能及时通知管理员，并采取某种保护措施，这样大部分的网络攻击都将无法得逞。但事实上，大多数的网络方案设计往往忽视了这种预警功能，使被托管的服务器孤独地遭受各种攻击直至被攻破。SHARKS的Active Alert就提供了实时的报警功能，并能为后续的安全检查工作留下详细的日志记录，大大方便了安全漏洞的填补工作。

网络安全中如何在发现攻击后防止黑客再以相同的手法攻入是一个非常实用性的问题。SHARKS的Passive Logger为此提供了一个很好的解决方案。Passive Logger是独立在网络上的机器，不能够从网络登录，只是默默地监听所有的网络流，并记录下其中任何可疑的部分，而它本身对网络上的其他机器而言，是完全不可见的。这样，一旦发现有攻击，就可以从Passive Logger里调出最详尽的资料，迅速找出黑客攻击的蛛丝马迹，从而改进整个系统，加以防范。

方正的安全理念

SHARKS的设计体现了方正在互联网安全领域的重要理念，那就是立体安全防护理念，从对攻击的防范、对入侵的检测和应急响应等不同层次考虑，为Internet服务提供了一个立体的安全防护体系。

另外，方正也十分强调网络安全中管理和人的作用，邹先生认为网络的安全很大程度上是由系统配置不当引起的。由此方正在网络安全方面提出了另一个重要的理念，即服务式安全理念，并已建立起以SHARKS为核心的一整套安全服务体系，其服务内容包括以资深安全服务人员与各种先进的检测工具为客户进行安全评估、定期审计、安全咨询顾问，并且响应客户请求进行突发攻击事件的处理，为客户进行现场取证，数据恢复，漏洞修补等服务。

随着互联网的高速发展，保护信息安全已成为刻不容缓的问题。然而，目前信息技术中的重要软、硬件技术主要掌握在西方主要发达国家手中，对中国的网络安全带来了极大的隐患。近日，中国最权威的信息管理专家发出警告，中国信息安全正面临严峻挑战，信息战和因信息网络安全问题而导致的威胁正向中国逼近。因此，发展我国的信息安全产业已非常迫切。北大方正集团已经走到前面，担负着在互联网上保卫中国信息安全的重任。■