黑客技术

引言

很显然，黑客技术对网络具有破坏能力，“黑客”一词是由英语Hacker音译出来的，近段时间，一个很普通的黑客攻击手段把世界上一些顶级的大网站轮流考验了一遍，结果证明即使是如yahoo这样具有雄厚的技术支持的高性能商业网站，黑客都可以给他们带来经济损失。这在一定程度上损害了人们对Internet和电子商务的信心，也引起了人们对黑客的严重关注和对黑客技术的思考。

我们在这里要讨论的一个主要问题是：研究黑客技术对国家是否有利?本文以下观点仅代表个人看法，不当之处请有识之士指正。

一、黑客技术属科学技术的范畴

黑客技术是Internet上的一个客观存在，对此我们无须讳言。和国防科学技术一样，黑客技术既有攻击性，也有防护的作用。黑客技术不断地促使计算机和网络产品供应商不断地改善他们的产品，对整个Internet的发展一直起着推动作用。就像我们不能因为原子弹具有强大的破坏力而否认制造原子弹是高科技一样，我们也不能因为黑客技术具有对网络的破坏力而将其弃于科学技术的大门之外。发现并实现黑客技术通常要求这个人对计算机和网络非常精通，发现并证实一个计算机系统漏洞可能需要做大量测试、分析大量代码和长时间的程序编写，这和一个科学家在实验室中埋头苦干没有太大的区别。发现者不同于那些在网上寻找并使用别人已经写好的黑客软件的人。这个区别就好像武器发明者和使用者的区别。不像一个国家可以立法禁止民间组织和个人拥有枪枝一样，很显然，法律不能禁止个人拥有黑客技术。

二、应该辨证地看待黑客技术

它的作用是双面的。和一切科学技术一样，黑客技术的好坏取决于使用它的人。计算机系统和网络漏洞的不断发现促使产品开发商修补产品的安全缺陷，同时也使他们在设计时更加注意安全。研究过黑客技术的管理员会把自己使用的操作系统和网络配置得更安全。如果没有那些公布重大漏洞发现并提出修补建议的黑客，Internet不可能像今天这样让人们受益，也不会有今天这么强壮（相对于以前而言）。

利用黑客技术从事非法破坏活动为自己谋取私利，理所当然是遭人唾弃的行为。这种人不是把精力放在对系统缺陷的发现研究与修补上，而是出于某种目的设法入侵系统，窃取资料、盗用权限和实施破坏活动。

*（一）黑客技术和网络安全是分不开的*

可以说黑客技术的存在导致了网络安全行业的产生。

一个典型的产品安全公告产生的过程是这样的（这里的例子是微软的一个漏洞）: 一个黑客在测试一个程序时，发现存在有不正常的现象，于是他开始对这个程序进行分析。经过应用程序分析、反编译和跟踪测试等多种技术手段，黑客发现该程序的确存在漏洞，于是针对该漏洞编写了一个能获取系统最高控制权的攻击程序，证实该漏洞的确存在。随后，这位黑客向微软写信通知其漏洞细节，并附上了攻击程序，要求微软修补该漏洞。微软开始对此不予答复。无奈，黑客在其网站上对世人公布了该漏洞，并提供攻击程序下载给访问者测试。顿时很多Internet上的网络安全论坛上都谈论此事，很快传遍了Internet。这时微软马上对该bug进行分析，随后在其安全版块上公布有关的安全公告，并提供解决方案和补丁程序下载。

对于这种情况，恶意黑客会利用微软的安全公告公布的漏洞去破坏系统；而网络安全专家会根据安全公告提醒用户修补系统；网络安全产品开发商则会根据该漏洞的情况开发相应的检测程序；而网络安全服务商则会为用户检测该漏洞并提供解决方案。

*（二）反黑组织*

随着黑客对互联网造成的危害性，不少人也组织起来反黑客了，国内的黑吧安全网也出了专门的系列教程，建议网民们多关注，上网前提就是电脑需要安全不被入侵。

为了避免黑客给广大网友带来不必要损失，请大家多关注各大反黑组织网站的教程。

*（三）目前Internet网络的基础是脆弱的*

Internet的基础是TCP/IP[[1]](#footnote-1)协议、网络设备和具有联网能力的操作系统。TCP/IP协议族有一些先天的设计漏洞，很多即使到最新的版本仍然存在。更有的漏洞，是和Internet的开放特性有关的，可以说是补无可补。最近发生的对各顶级网站的攻击方式就是利用Internet的开放特性和TCP/IP协议的漏洞。

网络设备如路由器，担负着Internet上最复杂繁重的吞吐和交通指挥工作，功能强大而且复杂，以目前的技术而论，没有可能完全避免漏洞。以占市场份额70%以上的Cisco产品而论，其已知的漏洞有30多条。

各种操作系统也存在先天缺陷和由于不断增加新功能带来的漏洞。Unix操作系统就是一个很好的例子。Unix的历史可以追溯到60年代中。大多数Unix操作系统的源代码都 是公开的，30多年来，各种各样的人不断地为Unix开发操作系统和应用程序， 这种协作方式是松散的,早期这些程序多是以学生完成课题的方式或由研究室的软件开发者突击完成的，它们构成了Unix的框架，这个框架当初没有经过严密的 论证，直到今天，商业Unix操作系统如Solaris和SCOUnix都还是构建在这个基础之上的，除非重新改变设计思想，推翻三十年来的Unix系统 基础，否则以后还必须遵循这个标准。这种情况导致了Unix系统存在很多致命的漏洞。最新的版本虽然改进了以往发现的安全问题，但是随着新功能的增加，又 给系统带来了新的漏洞，很多软件开发人员只为完成系统的功能而工作，用户日新月异的需求和硬件的飞速发展，使生产商不可能也没有时间对每一个新产品做圆满 的安全测试，一些正式的软件工业标准有利于改善这种局面，即使生产商按照这些工业标准开发测试，也难以保证十全十美，因为源代码公开的特性，使黑客有足够的条件来分析软件中可能存在的漏洞。处于温室中的作物无法适应自然环境的洗礼，目前脆弱的网络必须经历磨难，付出代价，否则必将经受不住历史的考验。

*（四）全世界对黑客技术的研究显得严重不足*

如果从整个社会的文明现状来看，黑客技术并非尖端科技，充其量只能说是Internet领域的基础课题。发现黑客技术并不要求太多底层的知识，它并不神秘，但计算机产品供应商对其一直讳莫如深，黑客技术的发展从局部来说让产品供应商不安，这造成整个计算机行业对黑客技术的重视不够，从而导致当今世上黑客组织和黑客技术研究都呈无政府状态。从长远的角度看，黑客对产品的测试和修补建议将促进产品的安全性，对客户和供应商都是有利的。现在世界上也许还没有哪一个国家真正投入人力和物力研究黑客技术，所以造成目前的Internet基础仍然薄弱，对于一个黑客来说，要制造一个令媒体关注的新闻是一件很容易的事情。这也是网络安全令世人担忧的原因之一。

*（五）网络安全公司需要黑客的参与*

从事网络安全技术服务的公司，如果没有研究开发黑客技术的水平，或者没有发现客户系统潜在隐患的能力，其服务质量是提不上来的。目前国际上很多从事网络安全业务的公司纷纷雇请黑客从事网络安全检测与产品开发，甚至一些政府部门也不惜重金招纳黑客为其服务。因为网络安全的防范对象是恶意黑客，所以必须有了解攻击手段的黑客参与，才能更全面地防范黑客攻击。合格的网络安全专家必须具有黑客的能力，不了解黑客技术的网络安全专家是不可想象的。

三、一个国家的黑客技术发展是有利于国家安全的

国内的一个网络安全小组---cnns的前身，在去年对日本、台湾地区和美国的网络安全状况进行了远程分析和调查，并与中国的网络安全状况做了对比，调查显示：

日本和台湾的网络安全水平和中国相似，从人员和研究力度上看，日本网络安全和黑客技术水平比中国显得要薄弱，但在硬件设置和安全产品方面，日本对重要站点的保护措施和资金投入显得比中国做得充足，安全检测产品和防火墙使用较为普遍，很多网站都有防火墙，虽然管理不善，但这些措施对网络安全的保护起到了一定的作用，弥补了黑客技术的不足，所以总体安全水平比中国差不多。

台湾的总体网络安全状况比大陆略差，特别是政府部门的网站，安全程度不如国内的政府网站。而美国的网络安全状况比中国和日本都强了不止一筹，这和遍布美国的黑客组织和大量的网络安全产品供应商有关。另外美国出品的操作系统产品和软件在市场上占有领先的份额，这有利于黑客技术的发展。在黑客技术的研究和网络安全产品的开发上，美国都是全球做得最好的。

Internet的开放互连的特征决定黑客技术可以跨国攻击，它既可以用于攻击，也可以用于防御。用兵之道，必须攻防兼备。所以未来信息战的胜负有赖于一个国家的整体黑客技术水平，这是不需要讳言的。

黑客技术的发现，对有关的软件开发商和信息产业是"短痛"，从长远的角度看却是有利的。而对于信息国防安全的高度而言，黑客技术的发展更有利于国防建设的大局。它的客观存在性决定了如果我们不去了解和研究它，则会受制于它。在信息技术越来越发达的今天，我们需要开发自己的网络安全产品来为信息产业保驾护航，更需要本领高强的黑客参与网络安全产品的研究开发和测试，这样产品的质量才上得去。

四、现代国家的网络无法完全和Internet脱离

一个现代国家的重要部门的网络无法完全和Internet脱离，网络化的趋势不可避免，任何行业都需要网络通信。综观处于应用阶段的网络技术和硬件，发展走在最前面的依然是Internet。所以TCP/IP网络互联技术被广泛地用于各行各业。有关部门认识到Internet的安全脆弱性，采取了一定的措施，例如使重要部门的网络在物理上与Internet完全脱离。这是比较有效的。但网络安全是一个整体的概念，只要能接触重要部门网络的人没有完全与Internet脱离，就不能说该网络与Internet已经完全脱离。比如一个重要部门的系统管理员，他经常上网的个人电脑上就可能有他所在重要部门的机密资料，通过顺藤摸瓜的方法，黑客可以获取更多他们想要的信息。黑客还可能通过电话、无线电和卫星信号传输的方式对重要部门的网络进行渗透。

五、未来信息战的可能性是存在的

当今社会的信息化程度越来越高，计算机和网络与人们的生活的关系越来越紧密。一个现代化国家的社会信息网络如果遭到毁灭性打击，足以使人们的生活倒退几十年。这种战争比较文明，不会造成人员伤亡，但破坏力绝不比一场常规战争小。相对于传统的战争和能造成地球毁灭的核战争而言，信息战的可能性也许更大。在网络更加发达的未来社会，除了高能量电磁波的攻击外，信息对抗战的主力将是黑客。

诚然，网络的基础设施是电脑，而不是单片机，黑客的攻击是基于代码的数据流攻击而不是强大的电流攻击，美国政府能勉强应付棘手的D.O.S[[2]](#footnote-2)攻击，而且就算网络在攻击下瘫痪，也能在数小时内恢复。五角大楼还对过臭名昭著的Internet蠕虫，这些难关他们都一一过来了。可是，真正的黑客和网络安全专家应该能意识到，真正有组织的大规模的信息战还没有来。

个人的力量是有限的，再厉害的黑客，再高明的代码都不足以对付一个国家和社会；真正的威胁来自于政府组织的全方位攻击，这种攻击不仅仅局限于代码和数据流攻击，还包括信息渗透，机密资料连环破解，和人工的物理接触。从整体上来说，全世界的网络都存在着被人忽视的管理漏洞，机密的资料和控制指令总会有渠道泄露出去。

真正的信息战没有到来以前，谁也估计不到破坏会到什么程度。这取决于国家之间的攻守准备。要打赢这场战争，除了对网络安全技术要有足够准备外，其它方面的人力和物质准备可能不会比一场局部的常规战争少。

六、国内的现状

国内网络安全的投入和培训不足。据估计，国内电子商务站点的网络管理人员至少有90% 以上没有受过正规的网络安全培训；这几年中国的Internet处于发展建设阶段，大部分的ISP和其它从事信息产业的公司都没有精力在网络安全进行必要的人力和物力投入，很多重要站点的管理员都是Internet的新手，一些操作系统如Unix,它们在那些有经验的系统管理员的配置下尚且有缺陷，在这些新手手中更是漏洞百出。很多服务器至少有三种以上的漏洞可以使入侵者获取系统的最高控制权。

一些公司对网络安全问题非常轻视，他们认为，他们的服务器上没有重要数据，也没有资金往来，如果有人入侵他们的系统，最多是窜改一下首页而已，谈不上大的危害。但他们可能没有意识到，如果恶意黑客入侵他们的机器后，用这台服务器的身份对其它有重要资源的服务器作案，造成第三方的损失后，公司可能成为该案的"替罪羊"。

七、发展有中国特色的网络安全

发展有中国特色的网络安全/黑客技术是强网之路。无可否认，在计算机领域上我们的技术整体上比西方发达国家落后。Internet基础协议是开放的，Unix系统的代码基本上是开放的，操作系统开放源代码是必然的趋势。硬件是别人的。但软件可以是自己的。在计算机领域，中国的软件技术明显优于硬件。黑客技术不是一个非常底层的领域，其开放性尤其明显。对系统极具破坏力的攻击程序代码和脚本在Internet上不难免费得到，相对于获得商业软件产品的源代码来说，黑客程序的源代码更容易设法获取。黑客技术是起源于开放的Unix环境，在Internet上得到繁荣的发展。这个特性决定了黑客技术是无法封锁的。黑客组织具有无政府主义的特色，不乐于接受管制。去年5月北约轰炸我驻南大使馆之后，民间的中国黑客对美国和北约的网络系统发动了很成功的一系列攻击，事情发生后，克林顿总统曾经签署了一个命令，要求黑客组织不要扩散黑客技术，但却被黑客们嗤之以鼻。从信息战的角度看，对黑客技术的要求应该是："人无我有，人有我全"。

很多国家都制定了未来信息战的方略，作为一个爱好和平的国家，我们的信息战方略应该是以防御为主的。但我们不可能不研究那些攻击性极强的高深黑客技术，正如虽然我们不想使用核武器，但我们不得不去研制它一样。去年，俄罗斯黑客成功地对美国五角大楼的计算机系统实行了渗透，并窃取了一些机密资料。有迹象显示，俄国黑客还可能入侵了最高机密的计算机系统，据新闻周刊（Newsweek）的报导，俄国黑客使用的入侵手段是 "不可能检测到的"。对于美国这种对计算机依赖程度很高的国家而言，俄罗斯黑客的这种手段是很具威慑力的。这种美国人不了解的技术，永远是他们的心头大患。

付出一定代价是必要的。早付出比晚付出好对于计算机病毒，包括国人在内的计算机用户都为它付出了沉重的代价。无数重要的数据被病毒吞噬消失得无影无踪。但多年来经过几代人与计算机病毒的斗争，我国对病毒的研究和反病毒技术已经走在了世界的前列。坏事来得早比来得晚好。在和平年代，我们有充足的时间应付不利的事件，经历的风浪越多，将更使我们有足够的经验应付恶劣环境下的突发事件。

如果平时我们没有对付高明的黑客攻击的经验，很难使我们相信我们有能力去打一场未来可能发生的信息战争。

在正确地认识黑客技术作用的基础上，对保障网络安全进行立法是必要的。我们的立法应该着重于保护用户利益，而不应该鼓励缺乏网络保 安措施的系统运行于Internet上。过分严格的法律保障将使人们忽略自己保护系统的责任，用户应该对具有明显漏洞的系统负责，比如一个重要用户没有设 置密码，那么管理员和用户对由此带来的安全威胁和经济损失应该承担主要的责任。这正如把贵重钱物扔在公共场所被别人捡走，粗心大意的主人所负的责任应该比 占有失物的人大的道理一样。法律打击的对象应该是那些利用黑客研究成果从事破坏活动的人（这些人往往是没有能力发现黑客技术的）。

Internet对我们的工作和生活将会越来越重要，全世界对这个巨大的信息宝藏正进行不断的发掘和利用，人们在获得巨大利益的同时，也面临着各种各样的威胁，网络安全威胁带来的损害与人们对网络的依赖程度成正比。中国对黑客技术的认识和对网络安全的研究正处于起步阶段，在我们进行现代化建设的时代，网络安全越来越成为关系国计民生的大事，它需要全社会的重视，让我们用勇于探索，大胆创新的精神来精心研发网络安全产品和维护我们的网络安全，为中国信息产业保驾护航！

索引

1. TCP/IP（Transmission Control Protocol/Internet Protocol，传输控制协议/网际协议）体系结构是指能够在多个不同网络间实现的协议簇。TCP/IP 协议包括两部分：传输控制协议和网际协议。 [↑](#footnote-ref-1)
2. 是网络攻击最常见的一种，它故意攻击网络协议的缺陷或直接通过某种手段耗尽被攻击对象的资源，目的是让目标计算机或网络无法提供正常的服务或资源访问，使 目标系统服务停止响应甚至崩溃。 [↑](#footnote-ref-2)