信息技术专题

公安科普讲坛

公安部科技局 编

中国人民公安大学出版社

公安科普讲坛

——信息技术专题

公安部科技局　编

（公安机关　内部发行）
中国人民公安大学出版社
·北　京·

图书在版编目（CIP）数据

公安科普讲坛．信息技术专题/公安部科技局编．—北京：中国人民公安大学出版社，2008.4

ISBN 978-7-81139-065-0

Ⅰ.公… Ⅱ.公… Ⅲ.①科学技术—应用—公安—工作—普及读物②信息技术—应用—公安—工作—普及读物

Ⅳ.D035.3-49

中国版本图书馆 CIP 数据核字（2008）第 045897 号

公安科普讲坛——信息技术专题

GONG AN KE PU JIANG TAN XIN XI JI SHU ZHUAN TI

公安部科技局 编

出版发行：中国人民公安大学出版社

地　　址：北京市西城区木樨地南里

邮政编码：100038

印　　刷：北京蓝空印刷厂

版　　次：2008 年 4 月第 1 版

印　　次：2008 年 4 月第 1 次

印　　张：8.875

开　　本：850 毫米×1168 毫米　1/32

字　　数：220 千字

ISBN 978-7-81139-065-0/D·061

定　　价：16.00 元（公安机关　内部发行）

本社图书出现印装质量问题，由发行部负责调换

联系电话：（010）83903254

E-mail：cpep@public.bta.net.cn

www.phcppsu.com.cn　　www.porclub.com.cn

序

阳春三月，万物复苏，在这样一个充满期待和希望的美好季节里，《公安科普讲坛——信息技术专题》与大家见面了。

《公安部关于深入实施科技强警战略的决定》明确要求：要将科学思想、科学方法和技术手段、技术装备切实应用到各项警务工作中，普及到每一个执法岗位上，融入到公安队伍建设的各个方面，全面促进现代警务机制建设，全面提升公安机关的整体素质和战斗力。为深入贯彻落实《公安部关于深入实施科技强警战略的决定》精神，切实提高全国公安机关广大民警的科技意识和科技素质，进一步掀起公安科技应用普及的热潮，公安部科技局组织策划并具体实施了“公安科普讲坛”活动。

21 世纪，人类社会发展已步入信息化时代，信息技术的日新月异、迅猛发展，对我国的政治、经济、文化、军事、社会发展以及人们日常生活的各个方面产生了深刻影响。通过“金盾工程”一期建设，全国各级公安机关的信息化建设和应用取得了快速发展，信息化应用服务于公安基层基础建设，并成为警务改革创新的重要推动力。为更深入地发挥公安信息化建设的作用，促进公安信息化应用普及，积极推进警务改革创新，努力构建完善现代警务机制，信息技术被确定为“公安科普讲坛”的首个专题。从 2007 年 5 月起，先后邀请北京邮电大学校长、中国工程院院士方滨兴教授，北京大学计算机科学技术系主任、微处理器研究开发中心主任程旭教授，总参六十一所软件中心主任曹江高级工程师，南京市市长助理、公安局局长孙文德同志，分

别从信息技术发展与应用的不同侧面，为公安部机关部分干部和中国人民公安大学师生作了精彩的演讲，并取得了良好效果。为增强学习效果，扩大讲座影响范围，公安部科技局组织人员将讲座录像制作成 DVD，并将根据讲座录音整理的文字材料和讲座演示文稿汇编出版，下发到全国各级公安机关，特别是基层科所队，相信这一工作必将对提高全国公安机关广大民警的科技意识和科技素质起到积极推动作用。希望全国公安机关各警种、各部门，特别是各基层所队认真组织，采取集中学习与个人自学相结合、专题学习与座谈讨论相结合、撰写学习体会与交流学习心得相结合等多种形式，深入学习讲坛内容，努力营造全警学科技、用科技的良好氛围，为 2008 年基本实现公安工作信息化奠定坚实基础。

党的十七大报告提出全面建设小康社会是党和国家到 2020 年的奋斗目标，并将科学发展观确定为今后我国在社会主义经济建设、政治建设、文化建设和社会建设发展过程中必须长期坚持的指导方针。这对公安工作提出了更高要求，公安工作既面临前所未有的发展机遇，又遇到前所未有的严峻挑战。各级公安机关的广大民警要深刻认清公安工作面临的新形势、新任务，以科学发展观为指导，及时跟踪科技发展前沿，深入学习实用科技知识，全面增强科技意识、科技素质，不断提高参与科技应用普及工作的积极性、主动性和创造性，充分发挥科学技术强警增效的巨大作用，为全国公安机关切实担负起巩固共产党执政地位、维护国家长治久安、保障人民安居乐业的重大政治和社会责任提供强有力的科技支撑和保障。

公安部科技局
2008 年 3 月

目　录

信息安全的威胁与对策

北京邮电大学校长　方滨兴

我今天演讲的题目是《信息安全的威胁与对策》。我主要想围绕信息安全的几种常见威胁、它们的本质与相关现象及相应的对策作一个交流。

信息安全的威胁有哪些呢？我觉得主要表现在以下六个方面：一是针对信息系统的攻击，攻击的目的是让系统没有办法正常使用；二是信息泄露，是指信息流动中相关数据被捕获；三是信息窃取，就是信息没有流动，但是人家闯进来，把你的信息偷走；四是信息诈骗，用欺诈的方式来获取用户的信息；五是程序员作案，是指开发商提供软件的目的本身就是为了获取用户的信息；六是有害信息扩散。

一、针对信息系统的攻击

攻击信息系统的核心目的就是影响系统的正常使用。这里可能有多种情况，我只展开介绍四种主要的威胁。

（一）病毒

在公安部门，我们说起病毒和蠕虫的时候一般都不太区分，经常混在一起说。我个人认为，它们从技术角度是不应该被混在一起说的，而混在一起说仅是从管理角度。公安部原来发布过一个病毒管理条例（在20世纪90年代）。之后出现了蠕虫，我们

不可能专门针对蠕虫再发布一个管理条例；后来又出了个 Phishing（“网络钓鱼”），也不可能再发布个“网络钓鱼”管理条例。所以，我们把所有的这类恶意代码行为统统用这一个管理条例来管理。这样一来，在媒体宣传当中，也就把它统称为病毒，因为称为病毒，也就纳入管理条例了。但是，从技术角度上看，计算机病毒和蠕虫的技术特点是不一样的。计算机病毒的特点是一定要传染，要有附着物，就像一个病菌不能孤立存在，它必须要在生物体上才能生存一样。所以，如果是病毒，就必须要附着在某个程序上。而蠕虫是不需要附着在任何程序上的，它能自我蜕变，自我分裂，一变十，十变百。所以，它们的特点不一样。

换一种说法，这种不一样体现在：计算机病毒必须伴随着一个程序才能够流传。执行这个程序，才能运行这个病毒。也就是说，病毒没有强硬的能力强行运行，它是利用用户的脆弱点来攻击的。而蠕虫就不一样了，你只要有漏洞，它就传过去。你要没有漏洞，它也没有办法。

假定你已经被病毒传染了，那么你是怎么被传染上的呢？可能是因为复制软件，或者上当受骗。一旦被传染上病毒，你应该做什么呢？它的传染特征有两点：首先，它要找你邮件的地址，就是你整个网络里的各种文件，它打开翻，寻找×××@这类的邮件账号。如果找到的话，就把所有的邮件账号混在一起，成为邮件列表，然后，通过邮件列表继续往外发假邮件，附件里面就带着它的病毒。既然是从你的邮箱里发出来的，收件人往往就是你认识的人，既然是你认识的人，他当然容易打开，这样的话，就容易被传染。其次，就是找共享的文件夹。如果有共享的文件夹，它就和看上去比较热闹的程序混在一起，放到文件夹里面。这样的话，别人也能看到共享文件夹，别人一旦把它打开运行，就会被传染。

病毒怎么能得到控制权呢？病毒有几十万种，各种变种非常

多，但是它的基本思想，就是那么几种。

我这里举一个操作系统的例子：对操作系统来说，它要怎么执行运行过程？一个病毒附在程序上，如果你运行了这个程序，病毒就会运行。比如说传染给 IE，你运行 IE，它当然被运行。操作系统一定是放在引导区，放到零道零扇区。我们一开机，先是 BIOS 运行，检查完之后，就把控制权转到了引导区。也就是说，它把引导区的内容给复制到了系统内存里，然后把控制权交出去。

病毒既然知道了这一点，它就可以先把引导区给你搬家，就是把你的操作系统搬走，然后占领这个区。这样能达到什么目的呢？你一开机，首先是引导零道零扇区。那么你搬来的是什么？你搬来的是病毒。换句话说，病毒转起来了。光有系统病毒是没有用的，因为这个系统不是活的（病毒传染死人没有用，这个人被烧了，这个病毒也被烧了，所以它没有传染的机会），所以还需要让它活起来。让它活起来的办法是什么呢？就是再把引导区取过来，因为它并不知道这个系统可能是什么，是 DOS 还是 Vista，还是其他的。但不管是什么，你一定有引导区。我把你搬走了，再把你搬回来，就达到了病毒侵入的目的。而用户往往并不知道这里有病毒。

既然我们知道这样一种思路，我们就可以从思路上、从理念上和病毒作对抗。

我们现在习惯于从技巧上作对抗。所谓技巧，就是看看病毒“长”得什么样，有什么“指纹”，然后再检查有没有这种病毒。

如果我们要从理念上处理病毒，怎么办？可以设计一个防毒程序。我说的是通用防毒程序，什么叫通用防毒呢？就是两年后的病毒我也能防。这个话是不是大话，我们先看看理论上能不能做到这一点。首先把防毒系统放到引导区，然后开机。病毒也要占领引导区，因为它不知道是防病毒系统，它可能认为是某个特

别的操作系统，搬走了之后，还要插入进来。所以一开机，首先运行的是病毒程序。这一点，是病毒机理之所在。它运行之后，自己不能操作，还要把搬走的东西请过来，请过来的目的，是为了让操作系统运行起来。它没有想到的是，请过来的是通用的防毒系统。现在，控制权交给了防毒系统。防毒系统的作用是什么呢？它不能够查病毒，因为两年后的病毒什么样，它不知道，它怎么能查呢？防毒系统能做什么呢？我就看看，这个零道零扇区是我待的地方，那里放的还是不是我。我一看，如果这个区放的不是我，是谁我不关心，既然不是我，我再把我放回去。我不管你原来是谁，反正我知道那个地方是我的，有人占的话，我就把它吃掉。我把它吃掉以后，计算机里还是有病毒的，我就重启了。重启后，它又从零道零扇区转起来，这回转起来的就是我的防毒系统。虽然是我的防毒系统，但是我的防毒系统还不相信这一点，我永远怀疑我的地方被人占领，我还要再检查一遍，我那块是谁？如果就是我本人，没有别的人，那么我就把这个引导系统重新请过来。这个时候，整个系统就能正常引导起来了，而且确实没有病毒。

这是我们从理念上和病毒作斗争，而不是从技巧上，不是简单地从“指纹”上。如果采用这种方法的话，两年后操作系统病毒也没有存在的可能。为什么呢？除非它不搬家。当然后来也有个别的病毒只传染 Windows XP，因为我只传染这一个，我把 XP 的引导方法学会了，我来引导。但是，从通用的角度来看，从理念上和病毒作斗争还是很好的办法。

（二）蠕虫

蠕虫跟病毒不一样，它不需要附着在某一个层面上。蠕虫有什么机会运行呢？病毒的运行机理是要么占领了一个引导区域，要么搭载在某个运行程序上，程序运行，我就跟着你运行。蠕虫是依赖于安全漏洞而存在的。任何一个软件，都难免有安全漏

洞。安全漏洞就是那种容易被攻击者绕过正常的防护措施而进入系统获得权限的缺陷，是程序缺陷。我们说一个软件，每编一百行代码，就可能有一个小的失误。有十个小的失误，就可能形成了一个缺陷。有十个缺陷就可能导致安全问题。这么一算，差不多一万行程序就可能有一个安全问题。我们现在的程序有几百万行，那么有几百个安全漏洞，也就很正常。

国际上有一个 CERT 组织（Computer Emergence and Response Team），就是计算机应急响应组织。我们国家也有。我们国家每一个运营商都有类似的应急响应组织，还成立了一个国家级的组织。国际上第一个这种组织是在美国的 CMU 大学，是美国国防部成立的，只不过把部门放到了这个大学。这是国际上最权威的 CERT 组织，所以我们一般喜欢引用它的数据。CERT 每年都报告所出现的安全漏洞，2006 年是 8000 多个，2007 年上半年将近 4000 个。这些安全漏洞都是新出现的，而且越来越新。为什么有这么多呢？不是说漏洞越发现越多，其实是新的软件在增多。既然有新的软件，新的漏洞当然也出来了。Vista 操作系统现在逐渐要取代 XP，现在它的漏洞也越来越多，因为它是新出来的，没有经过长期的考验。这些漏洞就可能招致攻击。在过去的年代，一个安全漏洞从发布到针对这个漏洞进行攻击，周期还是比较长的，最长的将近一年，就算短的，也一个月。到了 2006 年，从安全漏洞公布到针对这个漏洞进行攻击，5 天就出来了。这说明，如果我们是每一周打一次补丁的话，我们可能还没有打补丁，就被攻击了，有漏洞被利用了。

蠕虫就是利用这些漏洞在起作用。任何一个蠕虫，它基本上都遵循这四部曲：扫描、锁定目标、攻击和自我复制。例如，2002 年的 39 号漏洞，即微软的 SQL Server 里面，存在远程过程调用（RPC）的漏洞。发现之后，就有一个叫做“冲击波”的蠕虫，专门利用这个漏洞发起攻击。蠕虫扩散时，首先找 SQL

Server，找到了再看看，这个漏洞是否补上了，一看你补上了，就再找别人；一看你没有补上，那么我就开始传染，然后再以你为跳板，往外扩散。不管是什么蠕虫，现在也有上万个蠕虫，很多蠕虫的变种，基本上都遵循这样一个规律。

当然，如果 Ipv6 出来了，这种蠕虫扩散就很难再存在了。因为蠕虫需要到处查找谁用了 SQL。它怎么查？它根据 IP 地址来查。它并不知道哪个是，所以它就对 IP 地址进行扫描。现在的地址空间，全世界也就是 40 亿，所以扫描起来才有可能。将来的地址空间是 128 位，那是什么概念？就是 40 亿 ×40 亿 ×40 亿 ×40 亿，这个太大了。所以，它想扫描到一个地址，可能要花一个月的时间，然后一看还很可能不是，因为概率不是很大，可能每 1000 台才有几台是。所以，将来这种情况会变得很少。当然，我们不排除它采取一些其他的手段。

我给大家展示几个比较经典的蠕虫。其中一个就是 Morris，这是世界上第一个利用安全漏洞来扩散的蠕虫。为什么用这个词呢？真正的蠕虫，从 20 世纪 70 年代就有人研究了。那个时候，他只研究蠕虫自身的机理。也就是说，怎么能够一个变两个，自我复制。因为你也没有那么大的空间，复制的时候，它憋死了，它也会出问题。复制完了，还有怎么把权限转过去，就是说权限的动态浮动，也就是一个比较难的问题。所以，当时是研究蠕虫自身，没有去研究怎么能够找到漏洞。那时候都是互相复制，跟病毒一样，没有漏洞，你复制下来就能起作用。

到了 20 世纪 80 年代，据说 Morris 的父亲是美国总统的信息安全顾问，他就发现了三个漏洞：一是 STMP 的邮件服务器漏洞；二是身份认证漏洞；三是 RSH 的漏洞，远程执行的漏洞。然后他就编了一个“圣诞树”。他说快到圣诞节了，给朋友送“圣诞树”。“圣诞树”很漂亮。他的朋友打开“圣诞树”时，就执行了蠕虫的程序，去找他的地址列表，然后被传染。这是通

过朋友传播病毒。同时，如果你不收他的信件，他就扫描，看你有没有这些已知漏洞。通过扫描来查，他的“效率”是几小时内传染到互联网上 6000 台机器。6000 台机器是个什么概念呢？在那个年代，全世界互联网上只有 6 万台机器，他等于传染了 10%。如果是现在的话，全世界差不多有 5 亿台机器，10% 就差不多是 5000 万台，差别非常大。

这个案例，促使美国成立了世界上第一个 CERT 组织，叫 CERT CC，就是计算机应急协调中心。后来美国成立了 80 多个 CERT，也就是说，国防部的所有军兵种，各大公司，如 IBM、Sun、过去的康柏等，大的学校，像丹佛、CMU，都成立了相应的组织。我国在这方面就欠缺一些，只是运营商成立了。其实我觉得大的部门都要成立相应的组织。因为自己的人保护自己的系统比较容易一点。请别人保护，有些东西是秘密，人家也看不了，这是个问题。

这里所介绍的是第一个蠕虫，早期还有同步风暴和木马。

我们再看最早的含有攻击性的蠕虫——“冲击波”，就是 Ms Blaster。一看 Ms Blaster，就知道跟微软有一定的竞争关系。原因从两点可以看出：首先，他专门有一句话，是写给比尔·盖茨的，他说：“比尔·盖茨，你怎么能把事情做成这个样子呢？赶紧停止赚钱，好好修理你的软件。”其次，这个病毒是 2003 年 8 月 11 日开始传染，而 8 月 16 日所有被感染的机器将自动去攻击比尔·盖茨的 www. windowsupate. com 网站。这当时是一个下载网站。为什么要攻击下载网站呢？因为微软已经看到这个病毒出来了，就马上打补丁。刚才说了，蠕虫利用的是它的一个漏洞，是 25 天前发现的漏洞。那么，能够把这个漏洞的补丁下载下来，这个病毒自然就没有了。可是它集中攻击这个下载网站，这就意味着全世界的机器几乎不太容易去打补丁了。当然了，可能别的组织、部门会帮助它打补丁。但是，实际上，它出了点差

错，因为真正的下载网站是 www. windowsupdate. microsoft. com，这个 windowsupdate. com 主要是为了抢注域名，把它抢注上了，大家要点击它的话，从它周转，我们叫做 DNS 转移定向。所以，它把重定向一断就意味着攻击不会起作用。不起作用以后，就有人想办法去修改它。美国一个 18 岁的少年叫 Jeffrey，他就改了，改成了 B 变种版本。还有罗马尼亚的 Dumitru，他编了 F 变种，这是最早的“良性蠕虫”。什么是良性的蠕虫？在学术界搞研究的时候，发现一个现象，就是蠕虫阴魂不散，如“红色代码”，那是 2001 年出现的蠕虫，结果 2003 年还有。为什么会出现这种现象呢？后来大家发现，这个蠕虫只有靠系统打补丁才能被消灭，可是很多学校实验室的机器，有一些不太重要的机器，没有人认真管理它，所以就会导致这个蠕虫长期存在。除非这个操作系统彻底被换掉了。又如这个蠕虫依赖 Windows 98，Windows 98 现在根本没有了，这个病毒才会没有。否则，它永远存在。人们说，我们可以远程杀毒，我也可以像蠕虫一样到处去查，到处去扩散，但是，我传染的目的不是为了破坏机器，而是为了看看有没有这种病毒，有，我们就把它杀掉。人们把这种运作称为良性运作。这些本来是在实验室里面研究的，但是在网络上就确实出现了真正的病毒程序，这个被称为 Nachi。

为什么它也是一个病毒呢？按理说，它到处帮你找有没有“冲击波”，如果有它就会自动帮你下载补丁，帮你杀掉病毒。如果你没中病毒，但是你有漏洞，它还抢先帮你下载补丁。但是，往往事与愿违。在 Blaster 出现病毒的时候，它影响的是终端，终端可能比较慢，会死机。但是，运营商感觉不是太强烈，可能占 20% 的带宽。可是 Nachi 一出来，它杀毒的心太急切，传染的速度非常快，A 传给 B，B 传给 C，C 传给 D，D 反过来可能重新传给 A，重新传给 B，这么反复地传播，就占了很多的带宽。它比 Blaster 还迫切，这是一点。另外，它让大家同时下载

补丁，如果大家同时下载补丁，网络带宽肯定跟不上。所以，最后它反而把运营商给憋住了。

“食人鱼”是最早出现的手机蠕虫。当然这是人为编出来的。有一个叫做“29A”的组织，它研究手机有没有蠕虫。为了防止一旦出现真正的蠕虫，导致手机用户不断花钱，因为花的钱都给运营商了，它研究不用通过网络来传输，而是通过蓝牙。也就是说，我们的手机和有蓝牙的手机在附近互相联通了之后，它主动把蠕虫传过去。当然那边会有一个提示，说有一个文件过来，你要不要？你可以不要，也就是它不想表现得太恶意。当然，它也说，它会保护得很好，不会让它流传到社会。但实际上第二年，这个蠕虫就流传到社会了。而且，人们还把它的这种提示给改掉了，就是可以在你神不知鬼不觉的情况下把它传染过去。这个被称为新式蠕虫。现在的手机系统由于逐渐采用类似于Windows操作平台，所以它有蠕虫病毒是非常自然的事，是不可抗拒的事。所以，我们对手机的病毒防范就应该像防范计算机病毒那样，才能够达到效果。除非你用最古老的、什么高级功能都没有的手机，才不会有病毒。就像现在大家早不用DOS机器了，我估计现在是没有DOS病毒了。

对于蠕虫，我们是比较看好“良性蠕虫”的。但是“良性蠕虫”扩散有问题，导致的网络阻塞比其他的蠕虫有过之而无不及。所以，我们提出一种设想，叫做“制导性受控良性蠕虫”。什么叫“制导性受控良性蠕虫”呢？首先，我们要监控网络有没有蠕虫的存在，当我们发现了蠕虫，我们自然也就知道，这个蠕虫是从哪里传过来的，然后就锁定它的源头。之后，我们就向源头定向发杀死蠕虫的“良性蠕虫”，我们把它称为一种“制导”。设想一下，这样的传输一定是最少传输了。因为只有你有，别人没有，根本不传。如果别人有，我没看见，就认为它没有。为什么呢？它没在网上传。因为如果蠕虫不路过这里，那

可能蠕虫就在你自己的机器里憋着，没有影响到大家。如果出来影响大家，我就给你杀掉。这样，就解决了前面所说的由于“良性蠕虫”导致的网络阻塞。

（三）黑客

现在对黑客的各种宣传是非常强烈的。我一问学生，大家都喜欢到这类的网站去看。但这类网站，现在似乎还没有什么手段能够限制它。当然了，即便中国有所限制，前面限制了，后面就搬到国外去了，它会继续存在。所以，黑客给网络安全带来了很大的挑战。

黑客也形成了形形色色的组织，如被称为“地下 DHT”的黑客组织。我没有找到它的成员，只找到了它的博客。像这些黑客还愿意把自己的照片放到网上。有个黑客有几个名字，英文名字叫 China Tiger，但他大部分用的是 DHT。而且，中国黑客有个特点，他喜欢把自己打扮成比较正义的样子，或者说这是他心理的支撑，因为他怕犯罪。但是，实际上他们做的事就是一种犯罪。他们有个口号：“捍卫祖国主权，维护正义和平，抵抗外来侵扰，打击反动势力……”这个一看，就是当时他们攻击我国台湾地区、攻击日本的时候写的。而且他们比较活跃，他们做的网页非常丰富，如 DHT 组织做的网页，它教你黑客技术，告诉你哪些被黑了，工具怎么使用，黑客怎么应用，用动画告诉你。而且它介绍一些黑客人物，也教你怎么防范。

还有，号称是“黑客第一大门户”的网站。这个门户网站看起来也很丰富。关键是它怎么教，它是在线教人怎么做黑客。不过看来他们还懂点法律，在这里没敢说黑政府。但是，在我的监控里看，恐怕 30% 的政府网站是他们黑的。

还有一些黑客，他们会简单声明“我是中国网络的八路军。我的成员是……”

黑客常用的手段就是口令破解，说白了就是猜口令。所谓的

猜口令，一般都是比较难以防范的。口令本身是比较简单的，而且我们知道，想穷举口令肯定是困难的，如果所有人都知道了，那就不叫口令了。所以，他们就要用“黑客字典”。什么叫“黑客字典”呢？就是收集了大量人们常用的口令的工具，比方说最近网上的“黑客字典”、“疯狂字典”、“天诛字典”都很有名。这里面收集了各种各样的口令。当然，我们的口令怎么会在他们那儿，这个就难说了。按照以前的经验来说，2% ~3% 的口令会在黑客那里。

比方说你的账号特别多，你管很多机器，那么你习惯的口令一定是账号再加上数字。否则的话，你那么多账号，会被搞糊涂的。账号数字一下子就给他猜到了。因为他猜口令肯定按一个账号猜，可能是名字的字头加数字，加电话号码，加身份证号码，你单位的字头，或者你常用这个词汇，等等。总之，这些是容易推算出来的。

同时，还有一个口令表，口令表在计算机里面存放。我们知道，有两种加密体制。一种加密是以通信为目的的加密，所以这边要加密，那边要解密。还有一种加密是以认证为目的的加密，是不可逆的，给一个数加密完了推不出来。这就好比说，我随便说一个数，除以七的余数就是我的密码，余完了之后你怎么把这个余数往回推呢？肯定推不回去。这样，里面存的就是账号和加密的结果。当我们正常人使用的时候，我输入口令，系统先把口令加密，加完密之后，到口令表比较，看加密结果和你同一个账号下存的密码是不是一样。是一样，就可以了。

如此一来，黑客就到网上找一些专门破解的程序。这些专门破解的程序是干什么的？就是做这个运行。这种程序在网上也到处都是，而且是各种各样的，你想要 Windows 的，它就有 Windows 的，你想要 PPT 的，它就有 PPT 的，还有 Excel、Word 等，应有尽有。这些网站特别愿意共享它们的“成果”。还有照片，你随