网络安全

安全技巧（十八）

小未 主编

目　录

对称、非对称和 HASH 加密的应用 1
对黑客技术的思考 8
Windows 下的隐私保卫战 18
QQ2003III安全问题大揭露 22
抵挡 DoS 远程连接让网络更安全 29
被 DDOS 攻击的解决方法 32
系统重装前保留杀毒软件升级包 33
修改注册表防范十大攻击 34
建立全局安全体系防范 DoS 攻击 51
有了 HotFix 系统安全更无忧 56
安全扫描软件浅谈 60
如何限制和关闭无用的端口 66
电子商务安全技术分析 67
构筑 MSN 的网络安全防护链 76
身份管理:保证用户安全的关键 81
Windows 日志文件的保护和分析 86
防范木马和黑客保护 QQ 安全 90
网上九大流行木马清除方法 92
巧解屏幕保护密码 103
剖析 QQ 产生的两种攻击形式 104
避免虚假 Web 站点的欺骗性攻击 105
增强收发电子邮件的安全性 108
特洛伊木马原理分析 110
详解加密技术概念及加密方法 127
木马喜欢隐藏在哪里 138

对称、非对称和 HASH 加密的应用

加密可以保证数据的保密性，也可用于验证用户，它是在实现网络安全的重要手段之一。在本课中，你将学到如何使用对称加密，非对称加密和 HASH 加密来建立一个信任关系。

加密的优势

加密提供以下四种服务，见表

服务	解释
数据保密性	这是使用加密的通常的原因。通过小心使用数学方程式，你可以保证只有你打算接收的人才能查看它。
数据完整性	对需要更安全来说数据保密是不够的。数据仍能够被非法破解并修改。一种叫 HASH 的运算方法能确定数据是否被修改过。
认证	数字签名提供认证服务。
不可否定性	数字签名允许用户证明一条信息交换确实发生过。金融组织尤其依赖于这种方式的加密，用于电子货币交易。

加密强度

加密文件一个常被讨论但又经常被误解的方面是加密强度。什么构成了加密的强度？什么是被美国出口法保护的？哪种级别的加密是被不同的安全需要所要求的？如何确定加密的有效强度？

加密强度取决于三个主要因素：

首先是算法的强度，包括几个因素，例如，除了尝

试所有可能的密钥组合之外的任何方法都不能数学的使信息被解密。从我们的角度而言，我们应该使用工业标准的算法，它们已经被加密学专家测试过无数次，任何一个新的或个体的配方将不被信任直到它被商业的认证。

第二个因素是密钥的保密性，一个合乎逻辑但有时被忽略了的方面，没有算法能够发挥作用如果密钥受到损害，因此，数据的保密程度直接与密钥的保密程度相关，注意区分密钥和算法，算法不需要保密，被加密的数据是先与密钥共同使用，然后再通过加密算法。

第三个因素是密钥程度，这是最为人所知的一个方面，根据加密和解密的应用程序，密钥的长度是由”位”为单位，在密钥的长度上加上一位则相当于把可能的密钥的总数乘以二倍，简单的说构成一个任意给定长度的密钥的位的可能组合的个数可以被表示为 2 的 n 次方，这儿的 n 是一个密钥长度，因此，一个 40 位密钥长度的配方将是 2 的 40 次方或 1099511627776 种可能的不同的钥，与之形成鲜明对比的是现代计算机的速度。

尽管可能加密的密钥的总数是非常大的，专门的计算机现在可以在不到一天时间内试验许多种密钥的组合，在一九三三年，Michaelwiener 研制出一种专门的计算机，专门破译 DES（一种使用 56－位密钥的算法）。在研制的过程中他发现设计所需要的费用是呈直线型的，考虑到他的结果和 Moore 的法则的因子（此法则指出计算力大约每 18 个月增长一倍）。其实任何密码都能破解而无论它的长度，想像一下这样的密钥利用现代的机器去破解是多么的快速。简单的说，一个人或组织在密钥破解的装备上花的钱越多，则密钥就会被越快的破

解，这种断言最近已经得到证实。ElectronicFrontierFoundation 建造的专门的计算机最近在不到三天的时间内破译了一个 64 位基础的密码。

尽管有相对的缺点,美国政府把使用超过 40 位的密钥的加密规为强加密，这种加密出口相关的法律已经获得通过。美国国内公司想要出口使用强加密的产品，首先要获得美国国务院的许可。例如，PrettyGoodPrivacy（PGP）加密工具的国际版本，虽然这些法律可能会变得日益宽松，但是一些公司和组织将毫无疑问继续遵守它。尽管公司和政府用现代化的计算机可以去击败 40 位的加密，但是耗费的成本超过了信息本身的价值。事实上，决定需要密钥的长度的一个因素是被保护信息的价值。尽管 40 位的密钥对于金融交易来说并不总是合适的，但对于个人用户的需要已经足够了。目前美国出口法对于 40 位密钥长度的限制已取消。

建立信任关系

应用加密指的是在主机之间建立一个信任关系。在最基本的级别上，一个信任关系包括一方加密的信息，并只有另一方的合作伙伴可以解密这个信息。这种任务是利用公钥加密来完成的。这种类型的加密要求你建立一个私钥和一个公钥。一旦你已经产生了一对密钥，你可以把公钥发布给任何人。

你可以通过以下两种方法来发布你的公钥：

·手动：你首先必须和接收方交换公钥，然后用接收方的公钥来加密信息。PGP 和 S/MIME 需要使用这种方法。

·自动：SSL 和 IPSec 通过一系列的握手可以安全地交换信息（包括私钥）。在本课你将学到有关这方面更

多的知识。

下面是在加密中一些术语的简单介绍：

对称加密

在对称加密(或叫单密钥加密)中，只有一个密钥用来加密和解密信息。尽管单密钥加密是一个简单的过程，但是双方都必须完全的相信对方，并都持有这个密钥的备份。但要达到这种信任的级别并不是想像中的那么简单。当双方试图建立信任关系时可能一个安全破坏已经发生了。首先密钥的传输就是一个重要问题，如果它被截取，那么这个密钥以及相关的重要信息就没有什么安全可言了。

但是，如果用户要在公共介质(如互联网)上传递信息，他需要一种方法来传递密钥，当然物理的发送和接收密钥是最安全的，但有时这是不可能的。一种解决方法就是通过电子邮件来发送，但这样的信息很容易的被截取到，从而击破了加密的目的。用户不能加密包含密钥的邮件，因为他们必须共享另一个用来加密含有密钥邮件的密钥。这种困境就产生了问题：如果对称密钥用它们自己来加密，那为什么不直接用相同的方法在第一步就使用？一个解决方案就是用非对称加密，我们将在本课的后面提到。

所有类型加密的一个主题就是破解。一种减少使用对称加密所造成的威胁的反措施就是改变密钥的规律性。然而，定期改变密钥经常是困难的，尤其是你的公司里有很多用户。另外，黑客可以使用字典程序，pass wordsniffing 来危及对称密钥的安全,或者通过搜翻办公桌，钱包以及公文包。对称加密也很容易被暴力攻击的手段击败。

非对称加密

非对称加密在加密的过程中使用一对密钥，而不像对称加密只使用一个单独的密钥。一对密钥中一个用于加密，另一个用来解密。如用 A 加密，则用 B 解密；如果用 B 加密，则要用 A 解密。

重要的概念是在这对密钥中一个密钥用来公用，另一个作为私有的密钥；用来向外公布的叫做公钥，另一半需要安全保护的是私钥。非对称加密的一个缺点就是加密的速度非常慢，因为需要强烈的数学运算程序。如果一个用户需要使用非对称加密，那么即使比较少量的信息可以也要花上几个小时的时间。

非对称加密的另一个名称叫公钥加密。麻省里工学院的数学家们在 1970 年首先开发了非对称密钥（公钥）技术。尽管私钥和公钥都有与数学相关的，但从公钥中确定私钥的值是非常困难的并且也是非常耗时的。在互联网上通信，非对称加密的密钥管理是容易的因为公钥可以任易的传播，私钥必须在用户手中小心保护。

HASH 加密把一些不同长度的信息转化成杂乱的 128 位的编码里，叫做 HASH 值。HASH 加密用于不想对信息解密或读取。使用这种方法解密在理论上是不可能的，是通过比较两上实体的值是否一样而不用告之其它信息。HASH 加密别一种用途是签名文件。它还可用于当你想让别人检查但不能复制信息的时候。

举个例子，一台自动取款机(ATM)不需要解密一个消费者的个人标识数字（PIN）。磁条卡将顾客的代码单向地加密成一段 HASH 值，一旦插卡时，ATM 机将计算用户 PIN 的 HASH 值并产生一个结果，然后再将这段结果与用户卡上的 HASH 值比较。使用这种方法，PIN

是安全的，即使对于那些维护 ATM 机的人来说。

签名

信息鉴别的方法可以使信息接收者确定：信息发送者的身份以及信息在传送过程中是否被改动过。如果信息的收发双方对该信息的内容及发送端没有争执的话，那么只采用鉴别技术也就足够了。鉴别技术可以保证在信息传送过程中对信息内容的任何改动都可以被检测出来，并且能够正确的鉴别出信息发送方的身份。但是，当信息的收发方对信息的内容及发送端产生争执时，只用鉴别技术就不够了。

收方可以伪造一份信息，从中获得非法利益，并且自称该信息是由发送方发过来的。例如，银行通过通信网络传送一张支票，收方就可以对支票数额进行改动，并且声称他已收到了这张支票。利用前面的鉴别技术丝毫也解决不了这个问题，因为鉴别使用了一个收/发双方共享的秘密密钥，这样才能是发放产生一个鉴别码而接收方又能对该鉴别码进行校验。但是收方也能对他伪造的信息产生一个合法的鉴别码，这给整个系统带来严重的安全问题。

在许多情况下，特别是商业系统中，通常都利用书面文件来规定契约性的责任，虽然鉴别技术可以完全有效的防止第三者的介入，但是却丝毫不能防止接收者的伪造。问题的另一方面是发送方可能是不诚实的，由于他发送的信息变得对他很不利，而要逃避责任，那么发送方就可能谎称他从未发过这个信息。在整个争执过程中，第三方也无法分辨那种情况是真实的。

为了解决上述问题，就必须利用另外一种安全技术----数字签名。签名必须达到如下效果：在信息通信的过

程中，接收方能够对公正的第三方（可以是双方事前统一委托其解决某一问题或某一争执的仲裁者）证明其收到的报文内容是真实的，而且确实是由那个发送方发过来的，同时签名还必须保证发送方发送后不能根据自己的利益否认他所发送过的报文，而收方也不能根据自己的利益来伪造报文或签名。

对于数字签名的产生过程来说，必须有足够的信息才能对报文和签名进行验证，没有足够的信息就会给伪造或否认报文提供可乘之机。但是收发双方用来产生与校验的签名的信息不能完全相同，因为一旦接收方能够用发送方用来产生签名的相同信息(算法和参数)来证实报文和签名，那么收方同样也能够用它来伪造报文和签名。所以签名产生者与签名证实者之间的相同信息绝对不能太多。如果发送方事后担心接收方否认接收到了他所发送的报文，那么发送方应能够请求获得报文证明，也就是说由接收方对发送方提供收到报文的证据。例如，如果甲方把报文发送给乙方，那么乙方就要向甲方发送一份签了名的报文证明收到了，由于这份报文有乙方的签名，所以乙方是不能抵赖他所收到的报文的。

随着信息经济和知识经济的迅猛发展，无纸办公彻底改变了过去手工操作的各种不便，显得更安全、更有效、更迅速、更简洁、更方便。数字签名以其独特的优势适应了这种发展,在无纸办公中占有十分重要的地位。例如,对公司内部有下级呈给上级请求批阅的公文在以往只需领导大笔一挥签名盖章，以个人的笔迹来证明其真实性。但手写的文件签名非常容易伪造。除此之外，签名者还可以否认签名，宣称它是伪造的。但在无纸办公年代，计算机网络中传送的电子公文又如何盖章呢?

又如何来证明签名的真实性呢?这就是——数字签名。

对黑客技术的思考

黑客技术，简单地说，是对计算机系统和网络的缺陷和漏洞的发现，以及针对这些缺陷实施攻击的技术。这里说的缺陷，包括软件缺陷、硬件缺陷、网络协议缺陷、管理缺陷和人为的失误。

很显然，黑客技术对网络具有破坏能力。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：研究黑客技术的利与弊?本文以下观点仅代表个人看法,不当之处请有识之士指正。

1、黑客技术属于科学技术的范畴

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。就象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屏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。这个区别就好象武器发明者和使用者的区别。不象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。

2、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他的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 不可能象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。

3、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 nternet 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。

4、目前 internet 网络的基础是脆弱的

Internet 的基础是 TCP/IP 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。

5、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。

6、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。

7、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.net 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。

8、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。

9、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 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。

10、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做案，造成第三方的损失后，公司可能成为该案的"替罪羊"。

11、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