网络安全

安全技巧（一）

小未 主编

目　　录

令电子邮件安全传递的方法－PGP 签名

在现代社会里，电子邮件和网络上的文件传输已经成为生活的一部分，因而邮件的安全问题也就日益显得突出。大家都知道在 Internet 上传输的数据是不加密的，如果你自己不保护自己的信息，第三者就会轻易获知你的所有隐秘。此外，还有信息认证的问题，如何让收信人确信邮件没有被第三者篡改，这就需要以 PGP 为代表的数字签名技术。

窗体顶部

窗体底部

PGP(PrettyGoodPrivacy)，是一个基于 RSA 公匙加密体系的邮件加密软件。它不但可以对你的邮件加密以防止非授权阅读，还能加上数字签名从而使收信人确信邮件是由你发出。让人们可以安全地通讯，而事先不需要任何保密的渠道用来传递密匙。PGP 采用了审慎的密匙管理，一种 RSA 和传统加密的杂合算法，用于数字签名的邮件文摘算法，加密前压缩等。它不仅功能强大，速度很快，并且源代码是完全免费的。

PGP 原理

RSA（Rivest－Shamir－Adleman）算法是一种基于“大数不可能质因数分解假设”的公匙体系。简单地说就是找两个很大的质数，一个公开给世界，一个不告诉任何人。一个称为“公匙”，另一个叫“私匙”。这两个密匙是互补的，就是说用公匙加密的密文可以用私匙解密，反过来也一样。假设甲要寄信给乙，他们互相知道

对方的公匙。甲就用乙的公匙加密邮件寄出，乙收到后就可以用自己的私匙解密出甲的原文。由于没别人知道乙的私匙，所以即使是甲本人也无法解密那封信，这就解决了信件保密的问题。但另一方面由于每个人都知道乙的公匙，他们都可以给乙发信，那么乙就无法确信是不是甲的来信。这时候就需要数字签名来进行认证。

在说明数字签名前先要解释一下什么是“邮件文摘”，简单地讲“邮件文摘”就是对一封邮件用某种算法算出一个能体现这封邮件“精华”的数来，一旦邮件有任何改变这个数都会变化，那么这个数加上密匙里作者的名字和日期等，就可以作为一个签名了。实际上 PGP 是用一个 128 位的二进制数作为“邮件文摘”的，用来产生它的算法叫 MD5。MD5 是一种单向散列算法，它不像 CRC 校验码，很难找到一份替代的邮件而与原件具有一样的“精华”。

回到数字签名上来，甲用自己的私匙将上述的 128 位的“精华”加密，附加在邮件上，再用乙的公匙将整个邮件加密。这样这份密文被乙收到以后，乙用自己的私匙将邮件解密，得到甲的原文和签名，乙的 PGP 也从原文计算出一个 128 位的“精华”来再用甲的公匙解密签名得到的数比较，如果符合就说明这份邮件确实是甲寄来的。这样两个要求都得到了满足。

PGP 还可以只签名而不加密，这适用于公开发表声明时，声明人为了证实自己的身份（在网络上只能如此），可以用自己的私匙签名。这样就可以让收件人能确认发信人的身份。这一点在商业领域有很大的应用前途，它可以防止发信人抵赖和信件被途中篡改。

公匙传递

公匙的安全性问题是 PGP 安全的核心，一个成熟的加密体系必然要有一个成熟的密匙管理机制配套。公匙体制的提出就是为了解决传统加密体系的密匙分配难保密的缺点。比如网络黑客们常用的手段之一就是“监听”，如果密匙是通过网络传送就太危险了。对 PGP 来说公匙本来就要公开，就没有防监听的问题。但公匙的发布中仍然存在安全性问题，例如公匙的被篡改，这可能是公匙密码体系中最大的漏洞，因为大多数新手不能很快发现这一点。你必须确信你拿到的公匙属于它看上去属于的那个人。为了把这个问题说清楚，需要先举个例子，然后再说如何正确地用 PGP 堵住这个漏洞。

以你和张三的通信为例，假设你想给张三发封信，那你必须有张三的公匙，你从 BBS 上下载了张三的公匙，并用它加密了信件用 BBS 的 Email 功能发给了张三。不幸地，你和张三都不知道，另一个叫李四的用户潜入 BBS，把他自己的密匙替换了张三的公匙。那你用来发信的公匙就不是张三的而是李四的，一切看来都很正常，因为你拿到的公匙用户名仍是“张三”。于是李四就可以用他手中的私匙来解密你给张三的信，甚至他还可以用张三真正的公匙来转发你给张三的信，这样谁都不会起疑心，他如果想改动你给张三的信也没问题。更有甚者，他还可以伪造张三的签名给你或其他人发信，因为你们手中的公匙是伪造的，你们会以为真是张三的来信。

防止这种情况出现的最好办法是避免让任何其他人有机会篡改公匙，比如直接从张三手中得到她的公匙，然而当她在千里之外或无法见到时，这是很困难的。PGP 发展了一种公匙介绍机制来解决这个问题。举例来说：如果你和张三有一个共同的朋友王五，而王五知道他手

中的张三的公匙是正确的（关于如何认证公匙，PGP 还有一种方法，后面会谈到，这里假设王五已经和张三认证过她的公匙）。这样王五可以用他自己的私匙在张三的公匙上签名（就是用上面讲的签名方法），表示他担保这个公匙属于张三。当然你需要用王五的公匙来校验他给你的张三的公匙，同样王五也可以向张三认证你的公匙，这样王五就成为你和张三之间的“介绍人”。张三或王五就可以放心地把王五签过字张三的公匙上载到 BBS 上让你去拿，没人可能去篡改它而不被你发现，即使是 BBS 的管理员。这就是从公共渠道传递公匙的安全手段。

有人会问：那你怎么安全地得到王五的公匙呢，这不是个先有鸡还是先有蛋的问题吗？确实有可能你拿到的王五的公匙也是假的，但这就要求这个捣蛋者参与整个过程，他必须对你们三人都很熟悉，还要策划很久，这一般是不可能的。当然，PGP 对这种可能也有预防的建议，那就是由一个大家普遍信任的人或机构担当这个角色。他被称为“密匙侍者”或“认证权威”，每个由他签字的公匙都被认为是真的，这样大家只要有一份他的公匙就行了。这样的“权威”适合由非个人控制组织或政府机构充当，现在已经有等级认证制度的机构存在。

对于那些非常分散的人们，PGP 更赞成使用私人方式的密匙转介方式，因为这样更能反映出人们自然的社会交往，而且人们也能自由地选择信任的人来介绍。和不认识的人们见面一样。每个公匙有至少一个“用户名”(UserID)，请尽量用自己的全名，最好再加上本人的 Email 地址，以免混淆。

注意！你所必须遵循的一条规则是：在你使用任何一个公匙之前，一定要首先认证它！无论你受到什么诱

惑，你都不要，绝对不要，直接信任一个从公共渠道（由其是那些看起来保密的地方）得来的公匙，记得要用熟人介绍的公匙，或者自己与对方亲自认证。同样你也不要随便为别人签字认证他们的公匙，就和你在现实生活中一样，家里的房门钥匙你只会交给信任的人。

下面谈一谈如何通过电话认证密匙。每个密匙有它们自己的标识（keyID），keyID 是一个八位十六进制数，两个密匙具有相同 keyID 的可能性是几十亿分之一，而且 PGP 还提供了一种更可靠的标识密匙的方法：“密匙指纹”。每个密匙对应一串数字（十六个八位十六进制数），这个数字重复的可能就更微乎其微了。而且任何人无法指定生成一个具有某个指纹的密匙，密匙是随机生成的，从指纹也无法反推出密匙来。这样你拿到某人的公匙后就可以和他在电话上核对这个指纹，从而认证他的公匙。

这样又引出一种方法，就是把具不同人签名的自己的公匙收集在一起，发送到公共场合，这样可以希望大部分人至少认识其中一个人，从而间接认证了你的公匙。同样你签了朋友的公匙后应该寄回给他，这样就可以让他可以通过你被你其他朋友认证，这和现实社会中人们的交往一样。PGP 会自动为你找出你拿到的公匙中有哪些是你的朋友介绍来的，那些是你朋友的朋友介绍来的，哪些则是朋友的朋友的朋友介绍的……它会帮你把它们分为不同的信任级别，让你参考决定对它们的信任程度。你可以指定某人有几层转介公匙的能力，这种能力是随着认证的传递而递减的。

转介认证机制具有传递性，这是个有趣的问题。PGP 的作者 PhilZimmermann。有句话：“信赖不具有传递

性；我有个我相信决不撒谎的朋友。可是他是个认定总统不撒谎的傻瓜，很显然我并不认为总统决不撒谎。”

私匙管理

和传统单密匙体系一样,私匙的保密也是决定性的。相对公匙而言，私匙不存在被篡改的问题，但存在泄露的问题。RSA 的私匙是很长的一个数字，用户不可能将它记住,PGP 的办法是让用户为随机生成的 RSA 私匙指定一个口令。只有通过给出口令才能将私匙释放出来使用,用口令加密私匙的方法保密程度和 PGP 本身是一样的。所以私匙的安全性问题实际上首先是对用户口令的保密。当然私匙文件本身失密也很危险，因为破译者所需要的只是用穷举法试探出你的口令了，虽说很困难但毕竟是损失了一层安全性。在这里只用简单地记住一点，要像任何隐私一样保藏你的私匙，不要让任何人有机会接触到它。

PGP 在安全性问题上的精心考虑体现在 PGP 的各个环节。比如每次加密的实际密匙是个随机数，大家都知道计算机是无法产生真正的随机数的。PGP 程序对随机数的产生是很审慎的,关键的随机数像 RSA 密匙的产生是从用户瞧键盘的时间间隔上取得随机数种子的。对于磁盘上的 randseed.bin 文件是采用和邮件同样强度的加密的。这有效地防止了他人从你的 randseed.bin 文件中分析出你的加密实际密匙的规律来。

安全初级教程：“新手”杀毒之完全手册

病毒是六亲不认的,不论是谁都有可能‘与毒共舞”,

而如果是“新手”（电脑初级用户）不巧碰上了病毒，我想那情形必定会像我刚跟病毒打交道那样：手忙脚乱，不知所措，不知实时监控、防火墙为何物，有何区别，那一项项的杀毒设置更是不知该不该选,怎样选？等等。哈，哈，别谎，看过本文后你心里就自然有底了。下面让我们一起来练一练杀毒的“基本功”吧。

一、安装杀毒软件

1、在无毒的环境下安装。如果你的电脑已感染了病毒那么再安装任何软件时都可能立刻被感染病毒，因此最好在你的电脑还没有被感染病毒前就要安装杀毒软件，这样做也同时可利用它的实时监控或防火墙的功能以有效地防止病毒的“入侵”。

2、电脑已被病毒感染则最好用软盘进行杀毒。如果你的电脑已感染了病毒但还没安装杀毒软件，这时最好用杀毒软盘进行杀毒，因为杀毒软盘的文件不用安装在你的电脑里，因此也就不怕它染上毒了。

安装杀毒软件的光盘版和安装其它的光盘一样，一般都很简单只需按照屏幕提示操作就可以了。

二、制作及使用杀毒软盘

杀毒软盘除了有以上用途外还能杀灭一些在 Windows 环境下难以清除的病毒，尤其是引导型病毒，因此，当你在 Windows 环境下杀过毒后，别忘了再在 DOS 模式下杀一遍。有些杀毒软盘在你购买杀毒软件时就附带有，有些则没有，要你在安装杀毒软件的后期自行制作，对于一些在网上下载的杀毒软件来说更是如此。制作的方法一般都很简单只需按照屏幕提示操作就可以了。使用时有些要你用启动盘启动计算机引导其进入 DOS 环境再往软驱上插入杀毒软盘再进行杀毒，有些则只需你

在启动计算机前插入杀毒软盘，计算机启动后它就会自动进行杀毒程序。

但有时我们会遇到某些在网上下载的杀毒软件在你自行制作了杀毒软盘后却不能像上面说的那样直接自动进入到 DOS 模式下杀毒,这时就要你自己找到该杀毒盘的杀毒程序文件在 DOS 模式下作为命令来启动它了,那怎么找呢？方法如下：

㈠、将一张已制作好的用于 DOS 环境下杀毒的软盘放进软驱。

㈡、在 Windows 环境下进行杀毒测试。

⑴、先在 Windows 中打开该软盘，然后再从“开始－程序－MS-DOS 方式”打开 DOS 窗口。

⑵、将鼠标移至任务栏并按下右键，在弹出的快捷菜单中选择“横向平铺窗口”或“纵向平铺窗口”并单击，以便能同时在 A 盘窗口和 DOS 窗口两个窗口中工作。

⑶、在打开的软盘文件中看看有哪些最尾的字样为“EXE”的文件(即扩展名为 EXE 的程序文件)，并将它作为命令输进 MS－DOS 窗口，再看看它能不能被启动并查杀病毒，如果不能就再找下一个这类的文件测试，直到找到为止，找到并经测试后确认它能被运行就可以确定它是杀毒引擎的文件了，然后按“ESC”键停止该程序的运行，再将该杀毒引擎的文件名用笔抄下来，作为在纯 DOS 下杀毒的命令，最后关闭 MS－DOS 窗口。注意：有些杀毒软盘不支持在 Windows 环境的 DOS 模式下杀毒，如瑞星 2001 标准版，这时，在找到该杀毒引擎的文件后它会给出提示，这样也同样可以确定它是杀毒引擎的文件。

㈢、进入纯 DOS 环境后进行杀毒。

在纯 DOS 模式下进行杀毒和在 Windows 环境的 DOS 模式下进行杀毒测试时启动杀毒引擎所需输入的命令是一样的。

三、做好防杀病毒的各项设置

一般来说，安装杀毒软件后首次启动的杀毒设置是不能满足我们的需要的，这时我们就要对其进行相应的设置了。

1、查杀的位置的设置。

一般分为：A、C、D、E 盘和本地所有硬盘及由用户自定义位置（如 C 盘中的某个文件夹）这几种方式供用户选择。具体的查杀位置用户应根据自己的实际情况来选择，一般来说初级用户应取出软盘和光盘后再选择对本地所有硬盘进行全面的查杀最好。

2、查杀病毒前的具体设置。

即在查毒或查杀计算机的病毒前，电脑用户根据自己的实际需要所要做的各方面具体的设置。设置一般有可选项和复选项两类。可选项即在二个或二个以上的被选项中只能选择一项，而复选项就不同了，你可以一次性选择多项或全都选或全都不选，但如果你选了许多你并不需要的选项的话则该杀毒软件可能会因要执行了太多的命令而减慢杀毒的速度而拖长了杀毒的时间，降低了工作效率。因此，在做这些设置时要尽量认真点，要选的一定不能漏选，不要选的就尽量不要选。另外，不同的杀毒软件的设置选项名称和类型都可能有些差异，但总的来说还是十分接近的。下面是在杀毒软件中进行查杀病毒前要做的设置的详细介绍。

⑴、查杀范围的可选项有：

●所有文件：选中此项后，该杀毒软件会查或查杀由电脑用户选择的杀毒位置（如 C 盘或本地所有硬盘）的所有文件。这样由于要查杀的对象较多而会慢些，但这样却又最保险，能防止漏查或漏杀病毒，对于新手们来说，一般都要选择此选项。

●程序文件：选中该选项后只能查杀应用程序类的文件。

⑵、查杀范围的复选项有：

●查压缩文件：如果病毒是被由因特网下载的压缩文件所感染的话，则一定要选择此选项，因为只有这样才能将它们所带有的病毒查出来并清除掉，因此，如果你的电脑有上网的话最好要选中该选项。

●内存、主引导区和分区引导区等选项：如果你的电脑中毒较深，就有可能内存和主引导区和分区引导区都被病毒感染了，这时就一定要选择此选项，为保险起见，请尽量选择此选项。

⑶、查毒内容复选项有：查未知宏病毒、包含子文件夹等。在一般情况下最好将这些都选中。

⑷、发现病毒时的处理方式设置（可选项）：一般有：询问后处理、直接清除、删除文件、忽略，继续扫描、更改文件名。“询问后处理”即在查到有病毒时，电脑会出现一个对话框，问你如何处理这病毒，你可以根据对话框中提出的询问选择“清除”或“删除”或“忽略，继续扫描”或“更改文件名”。一般来说，选择“直接清除”最合适，因为杀毒软件一般都能将查出的病毒杀掉而没什么不良的后果，而且也省事，而当该软件不能清除该病毒时又会出现一个类似于上面所说的对话框，由你选择怎样处理，在这种情况下，如果是重要的文件的

话就要慎重对待，如果是一些网页、帮助类等不重要的文件的话就最好干脆将其删除掉，斩草除根!而“忽略，继续扫描”这一选项新手们则最好别选，即使在迫不得已的情况下要选，也要将该文件先备份或记下它所在的目录，以便能准确无误地将它们找到，再作进一步的处理。

⑸、扫描完成后的动作。即请你选择在查杀完所有的目标文件后要求电脑做出什么档的动作。它的可选项一般有：返回主程序、退出程序、重启计算机、关闭计算机。复选项有：提示扫描完成等。我个人认为，在可选项中选择“返回主程序”并选中“提示扫描完成”的复选项为佳。

3、对防火墙进行适当地设置。

防火墙的作用是对病毒的过滤有着良好的实时性，也就是说病毒一旦入侵系统或从系统向其他资源感染时，它就会自动将其检测到并加以清除，这就最大可能地避免了病毒对资源的破坏。其次,“病毒防火墙”能有效地阻止病毒从网络向本地计算机系统的入侵。再者，“病毒防火墙”的“双向过滤”功能保证了本地系统不会向远程（网络）资源传播病毒。这一优点在使用电子邮件时体现得最为明显，因为它能在用户发出邮件前自动将其中可能含有的病毒全都过滤掉，确保不会对他人造成无意的损害。如从网上下载有关文件或接收电子邮件，运行有关邮件附件的文档或程序时，它会时刻监视着这些文件是否带毒，一旦出现病毒，在该杀毒软件能识别的情况下可立即将其截拦并做出由用户设置好的处理方式（如询问你如何处理或直接将该病毒清除掉等），从而避免你的电脑被该病毒感染。

它除了有与查杀病毒类似的设置外通常还会有“系统启动时自动装入防火墙”(复选项)这类的设置。选择该选项的好处是可以避免你在拨号上网或使用软盘(特别是别人的软盘)时忘了打开防火墙或实时监控程序而使病毒乘虚而入情况发生。同时有些杀毒软件在选中它后，当你的计算机启动或在进入 Windows 时该杀毒软件就会自动对你的电脑进行扫描。但选了该选项后又会占用较多的系统资源(有的占 5%以上)，从而减慢电脑开机后进入系统的速度并影响了执行其它应用程序的速度和质量。所以，如果你常上网的话最好选择此项，如果自个儿用该电脑而且极少上网则就可以不选了,因人制宜。

除此之外，我们还要注意及时升级杀毒软件。因为新的病毒不断涌现，如果你电脑里所装的杀毒软件的更新速度跟不上，就容易感染上新病毒。一般来说，现在稍为有些名气的杀毒软件都空一至二个星期更新一次病毒库，并提供在线升级。在线升级的升级开始会探测你电脑的现有版本，如果你的电脑的现有版本是最新的它会停止升级告诉你你的电脑的版本是最新的不必下载升级，省去许多时间和银子，而且，由于在线升级不用下载本地主机上已有的文件而只下载新的文件从而使升级时下载文件的时间缩短了许多。因此我们应尽量使用在线升级。

防火墙到底应该有多“厚”

Internet 的开放便利性，与网络安全的隐忧，一直是矛盾共存。随着企业对 Internet 依存的加深，对网络安

全的防范与布署，就成了必备的知识。大家都知道，特洛伊城之所以久攻不破，是它有一道坚固的城墙；在 Internet 上我们也需要一道坚实的防火墙，以确保防火墙不会因被击溃而导致企业内部电脑的入侵危机。

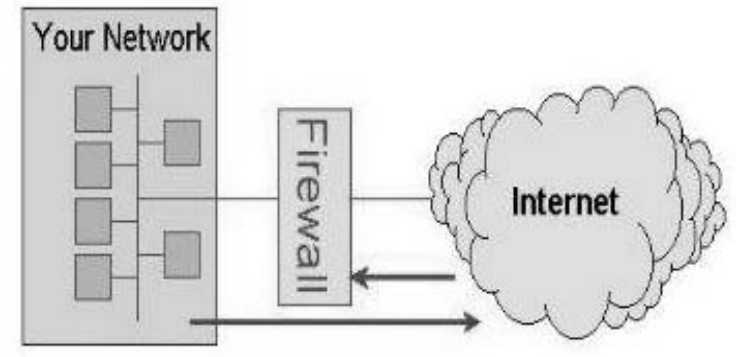
公元前 12 世纪，希腊与特洛伊的一场战争，造就了荷马(Homer)史诗中的两位英雄人物 Achilles 与 Odysseus；而这场战争最终决定性的胜利竟然是一只木马，这样富戏剧性的结局更让人不可思议，除了具军事教训意味外，着实也多了许多趣味性。如今这场战争却活生生地搬上了 Internet 舞台，虽然少了美女 Helen 助阵，不过精采的程度却不下于 3000 多年前的盛况，只不过整个场景都虚拟于网络之中。。

打造一道网络城墙

据荷马史诗记载，希腊联军共围剿特洛伊城达十年之久，当时没有现代的空中部队，因此整个防卫所依靠的都是城墙！据说当时特洛依城城墙厚度达五公尺，在这么坚固城墙防卫下，希腊一直都无法将特洛依城攻下。

相对于特洛依城墙的厚度，到底一道网络的城墙要多“厚”才安全呢？在 Internet 中的城墙，我们称之 Firewall 或是防火墙，主要的作用是进行网络交通过滤与管制。

这道网络虚拟的城墙强度虽然不能以实体厚度来衡量，但打造这道城墙同样要考虑到“是否地基够稳？”、“是否有钢筋结构？”、“城门卫兵是否尽职？”，此外这一整套控管机构“是否有品质保证？”，如此才能评判防火墙是否足以抵御外侮。



打造一道网络城墙

稳固的地基--操作系统

高楼平地起，因此打好地基是建造一道坚固城墙的基础！如何打造防火墙的稳固地基？在电脑系统里，防火墙不能独立存在，必须建立在操作系统(OS)上，因此操作系统就是防火墙的地基。操作系统的稳固与否，在于安全性上是否有保障，从以下几个方面来设计操作系统，就能有稳固牢靠的地基。

1、以安全的角度出发，来设计操作系统

一般操作系统的设计是用来满足所有的应用环境，因此出发点是以“弹性”考虑，在此前提下，操作系统呈现的是“多而杂”，样样都可以做，不过却不见得都一定用得上；而以“安全”角度来设计的操作系统，设计的用途是专供防火墙用的，是个“小而美”的操作系统，因此可与防火墙紧密搭配，当然可以有效提升防火墙的强度。

2、删除不需要的功能与指令

系统存在的程序与指令愈多，漏洞也就相对地增加，黑客常常会利用操作系统上运作程序的漏洞，作为入侵

的途径，并利用系统上可用的指令来破坏系统的运作。因此将不必要的程序与指令删除，黑客的攻击目标自然减少了。

3、删除所有操作系统上既存的程序的漏洞

有些程序是必须存在操作系统上以利系统运作，而这些程序本身仍然可能遭受到黑客攻击，因此作为一个防火墙上的操作系统，就不能沿用一般操作系统上的运作程序，必须重新审视程序内容是否隐藏漏洞，一一删除漏洞后再重新设计，然后才供系统运作使用。

防火墙的“钢筋”结构

为了加强建筑物的抗震强度，人们采用钢筋结构来强化耐震度。而在 Internet 世界中，黑客的入侵手法日益先进，入侵事件更是与日俱增，就好比强震一波波朝防火墙袭击而来，因此有必要为防火墙加筑钢筋结构才能有效抵挡黑客的“强震”撼动！

1、各程序具有独立的执行空间

各程序执行时不能彼此干扰，同时也不能共用相同目录，否则一旦某一个程序遭受入侵，其他程序也可能同时遭殃。因此各程序执行时所需的文件，如函数库或指令，都必须摆放在各自的目录中，不能有共用的情形。

2、各程序以最少许可权执行

每一个程序的执行者权限只够执行程序本身，同时不能任意切换目录，以防止权限设定不当的破坏。

3、所有权限类别设为只读

为了确保防火墙系统的正常运作，避免黑客破坏正常运行的程序或类别，甚至防止黑客程序伪装成正常程序，将防火墙系统上的权限类别设为只读，黑客就不能进一步进行破坏。