网络安全

安全技巧（八）

小未 主编

目　录

PGP 加密的优越性

我们知道 PGP（PrettyGoodPrivacy）是目前最流行的一种加密软件，它是一个基于 RSA 公钥加密体系的邮件加密软件。我们可以用它对邮件保密以防止非授权者阅读，它还能对用户的邮件加上数字签名，从而使收信人可以确信发信人的身份。它让用户可以安全地和从未见过的人们通信，事先并不需要任何保密措施的来传递密钥，因为它采用了非对称的“公钥”和“私钥”加密体系。

但 PGP 不是一种完全的非对称加密体系，它是个混合加密算法，它是由一个对称加密算法（IDEA）、一个非对称加密算法（RSA）、一个单向散列算法（MD5）以及一个随机数产生器（从用户击键频率产生伪随机数序列的种子）组成的，每种算法都是 PGP 不可分割的组成部分，PGP 至所以得到流行，得到大家的认可，最主要的一半是它集中的几种加密算法的优点，使它们彼此得到互补。

我们知道采用“公钥”和“私钥”加密体系最大的安全性问题就是公开的“公钥”可能被人篡改，影响文件的解密，虽然 PGP 也采用这一加密体系，并且所有“公钥”和“私钥”都可以由用户自己产生，不需要专门的认证机构，但它却有一个比较完善的密钥管理体制，所以它的另一半优点就体现在 PGP 独特的密钥管理体制上。

下面我们就从 PGP 加密机制和密钥管理的角度来

分析 PGP 加密的优越性。

一、PGP 的加密机制

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。邮件的安全问题也就突出了，大家都知道在互联网上传输的数据是不加密的。如果用户不保护自己的信息，第三者就会轻易获得用户的隐私。还有一个问题就是信息认证，如何让收信人确信邮件没有被第三者篡改，就需要使用数字签名技术。

RSA 公钥体系的特点使它非常适合用来满足上述两个要求：保密性（privacy）和公证性（authentication）。PGP 的创始人是美国的 PhilZimmermann，他的创造性在于他把 RSA 公钥体系的方便和传统加密体系的高度结合起来，并且在数字签名和密钥认证管理机制上有巧妙的设计。

RSA(Rivest-Shamir-Adleman)算法是基于大数不可能被质因数分解假设的公钥体系。简单地说就是找两个很大的质数。一个对外公开，一个不告诉任何人。公开的一个称为“公钥”，另一个叫“私钥”（Prblickey&SecretkeyorPrivatekey）。这两个密钥是互补的，也就是说用公钥加密的密文只可以用私钥解密，反过来也一样。

假设甲要寄信给乙，他们互相知道对方的公钥。甲就用乙的公钥加密邮件寄出，乙收到后就可以用自己的私钥解密出甲的原文。由于别人不知道乙的私钥，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。另一方面，由于每个人都知道乙的公钥，他们都可以给乙发信，那么乙怎么确信来信是不是甲的，这就是数字签名的必要性，用数字签名来确认发信的身份。

PGP 的数字签名是利用一个叫“邮件文摘”的功能，

“邮件文摘”（messagedigest），简单地讲就是对一封邮件用某种算法算出一个最能体现这封邮件特征的数来，一旦邮件有任何改变这个数都会发生变化，那么这个数加上用户的名字（实际上在用户的密钥里）和日期等等，就可以作为一个签名了，确切地说 PGP 是用一个 128 位的二进制数进行为"邮件文摘"的，用来产生它的算法就是 MD5(MessageDigest5。MD5 的提出者是 RonRirest，PGP 中使用的代码是由 ColinPlumb 编写的 MD5，MD5 是一种单向散列算法，它不像校验码，是一份替代的邮件并且与原件具有同样的 MD5 特征值。

PGP 给邮件加密和签名的过程是这样的：首先甲用自己的私钥将上述的 128 位值加密，附加在邮件后，再用乙的公钥将整个邮件加密（要注意这里的次序，如果先加密再签名的话，别人可以将签名去掉后签上自己的签名，从而篡改了签名）。这样这份密文被乙收到以后，乙用自己的私钥将邮件解密，得到甲的原文和签名，乙的 PGP 也从原文计算出一个 128 位的特征值来和用甲的公钥解密签名所得到的数进行比较，如果符合就说明这份邮件确实是甲寄来的。这样两个安全性要求都得到了满足。

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（在网络上只能如此了），可以用自己的私签名，这样就可以让收件人能确认发信人的身份，也可以防止发信人抵赖自己的声明。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。

为什么说 PGP 用的是 RSA 和传统加密的杂合算法呢？因为 RSA 算法计算量很大而且在速度上也不适合

加密大量数据，所以 PGP 实际上用来加密的不是 RSA 本身，而是采用了一种叫 IDEA 的传统加密算法，又称为“对称加密法”。

传统加密方法就是用一个密钥加密明文，然后用同样的密钥解密。这种方法的代表是 DES(USFederalData EncryptionStandard)，也就是乘法加密，这的主要缺点就是密码长度较短，且的传递渠道解决不了安全性问题，不适合网络环境邮件加密需要。

IDEA 是一个有专利的算法，专利持有者是 ETH 和一个瑞士公司：Ascom-TechAG。IDEA 的加（解）密速度比 RSA 快得多，所以实际上 PGP 是以一个随机生成的密钥（每次加密不一样），用 IDEA 算法对明文加密，然后用 RSA 算法对该密钥加密。这样收件人同样是用 RSA 解出这个随机密钥，再用 IDEA 解密邮件本身。这样的链式加密就做到了既有 RSA 体系的保密性，又有 IDEA 算法的快捷性。PGP 的创意有一半就在这一点上了，为什么 RSA 体系 70 年代就提出来，一直没有推广应用呢？速度太慢！那 PGP 创意的另一半在哪儿呢？就是下面我要谈的密钥管理。

二、PGP 的密钥管理

一个成熟的加密体系必然要有一个成熟的密钥管理机制配套。公钥体制的提出就是为了解决传统加密体系的密钥分配过程保密的缺点。比如网络黑客们常用的手段之一就是"监听"，如果密钥是通过网络传送就太危险了。对 PGP 来说公钥本来就要公开，就没有防监听的问题。但公钥的发布中仍然存在安全性问题，例如公钥被篡改（publickeytampering），这可能是公钥密码体系中最大漏洞。用户必须确信用户的公钥属于需要收信的那

个人。

为了把这个问题说清楚，先举个例子进行说明，然后再说如何正确使用 PGP 堵住这个漏洞。

以用户 A 和用户 B 通信为例，现假设用户 A 想给用户 B 发信，首先用户 A 就必需获取用户 B 的公钥，用户 A 从 BBS 上下载或其它途径得到了 B 的公钥，并用它加密了信件发给了 B。不幸的是，用户 A 和 B 都不知道，另一个用户 C 潜入 BBS 或网络中，侦听或截取到用户 B 的公钥，然后在自己的 PGP 系统中用用户 B 的名字生成密钥对中的公钥替换了用户 B 的公钥，并放在 BBS 上或直接以用户 B 的身份把更换后的用户 B 的“公钥”发给用户 A。那用户 A 用来发信的公钥是已经是更改过的，实际上是用户 C 伪装用户 B 生成的另一个公钥。这样谁都不会起疑心，但这样一来用户 B 收到用户 A 的来信后就不能用自己的私钥解密了，更可恶的是，用户 C 还可伪造用户 B 的签名给用户 A 或其他人发信，因为用户 A 手中的公钥是伪造，用户 A 会以为真是用户 B 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钥，但能做到这一点的是非常困难的，一种方法是直接从用户 B 手中得到他的公钥，然而当他在远在他乡或在时间上根本不可达到时，这是不可办到的。

但 PGP 发展了一种公钥介绍机制来解决这个问题，其思路是这样的：如果用户 A 和用户 B 有一个共同的朋友 D，而 D 知道他手中的 B 的公钥是正确的。这样 D 就成为用户 A 和 B 之间的公证人，用户 B 为了防止别人篡改自己的公钥，就把经过 D 签名的自己的公钥上载到 BBS 上让用户去拿，用户 A 想要取得用户 B 的公钥

就必需先获取 D 的公钥来解密 BBS 或网上经过 D 签名的 B 的公钥，这样就等于加了双重保险，一般没有可能去篡改它而不被用户发现，即使是 BBS 的管理员。这就是从公共渠道传递公钥的安全手段。

说到这里也许有人会问想到，只通过一个签名公证力度是不是小了点，聪明的 PGP 当然会想到这一点，就是把不同签名自己的公钥收集在一起,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，从而间接认证了用户的公钥。同样用户签了朋友的公钥后应该寄回给他，这样就可以让他通过该用户被该用户的其他朋友所认证。有点意思吧，和现实社会中人们的交往一样。PGP 会自动根据用户拿到的公钥中有哪些是朋友介绍来的，把它们分为不同的信任级别，供用户参考决定对它们的信任程度。也可指定某人有几层转介公钥的能力，这种能力是随着认证的传递而递减的。

也许还有人会问：如何安全地得到 D 或其他签名朋友的公钥呢。确实有可能用户 A 拿到的 D 或其他签名的朋友的公钥也假的，但这就求这个用户 C 必须对你们三人甚至很多人都很熟悉，这样的可能性不大，而且必需经过长时间的策划。当然，PGP 对这种可能也预防的建议，那就是由一个大家普遍信任的机构担当这个角色，他被称为认证权威机构，每个由他签过字的公钥都被认为真的，这样大家只要有他的公钥就行了，认证这个人的公钥是方便的，因他广泛提供这个服务，假冒他的公钥是极困难的，因为他的公钥流传广泛。这样的"权威机构"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，如广东省电子商务电子认证中心（www.cnca.net)就是一个权威的认证机构。

对于那些非常分散的用户，PGP 更赞成使用私人方式的密钥转介方式，因这样有的非官方途径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朋友来公证，总之和不认识的人们之间的交往一样，每个公钥至少有一个"用户名"（UserID），请尽量用自己的全名，最好再加上本人的 E-mail 地址，以免混淆，这就是 PGP 推荐使用的电话密钥认证。

PGP 的每个密钥有它们自己的标识（keyID），keyID 是一个 8 位十六进制数，两个密钥具有同 keyID 的可能性只有十亿分之一，而且 PGP 还提供了一种更可靠的标识密钥的方法："密钥指纹"(keysfingrprint)，每个密钥对应一串数字（16 个 2 位十六进制数），这个指纹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钥，密钥是随机生成的，从指纹也无法反推出密钥来。用户拿到某人密钥后就可以他在电话上核对这个指纹，从而认证他的公钥。

防止内部 IP 地址泄漏的 2 种方法

当访问 IIS 网站上的静态 HTML 文件时，比如 index.htm，IIS 响应中会包含一个 Content-Location 文件头。如果 IIS 配置不当，Content-Location 文件头中将包含服务器的 IP 地址内容，这样就导致了隐藏在 NAT 防火墙或者代理服务器后面的内部网 IP 地址信息的泄漏，给攻击者有漏可乘。

下面我就介绍 2 种解决办法，实现将 IP 地址信息替换为域名信息的目的，帮助系统管理员消除内部网的 IP

地址泄漏隐患。

什么是 IIS 对页面文件的响应信息

当我们使用浏览器访问 IIS 网站 Web 服务器上的页面内容时，IIS 将返回给用户一个完整的响应信息。简单情况下，我们可以认为这个响应信息包含 2 部分内容：

1、系统信息：

诸如访问状态、服务器信息、文件类型、正文长度等内容。

2、正文信息：

通常情况下就是我们在浏览器中看到的页面内容，也就是在浏览器中可以查看到的页面源代码内容。

当我们使用高级语言中的相关 Internet 控件访问一个页面内容时，比如使用 VB 的 InternetControl 控件来编写自己的浏览器或者下载程序，最终就会得到包含上述 2 部分内容的完整响应信息。

首先我们来看看一个例子，它显示了默认安装情况下 IIS 对 HTML 文件的响应信息：

```
HTTP/1.1200OK
Server:Microsoft-IIS/5.0
Content-Location:http://192.168.1.1/index.htm
Date:Wed,31Oct200104:19:40GMT
Content-Type:text/html
Accept-Ranges:bytes
Last-Modified:Fri,12Oct200107:48:06GMT
ETag:"03f7e3af252c11:9a2"
Content-Length:7141
```

上面响应信息的第 3 行内容包含了内部网的 IP 地址信息，这是我们不希望的。我们希望 IIS 响应如下的内

容：

HTTP/1.1200OK

Server:Microsoft-IIS/5.0

Content-Location:http://www.mywebsite.com/index.htm

Date:Wed,31Oct200104:19:40GMT

Content-Type:text/html

Accept-Ranges:bytes

Last-Modified:Fri,12Oct200107:48:06GMT

ETag:"03f7e3af252c11:9a2"

Content-Length:7141

也就是说，将第 3 **行内容中的** IP **地址信息替换为域名信息。下面来看看解决办法。**

解决方法一：执行脚本程序 Adsutil.vbs

通过修改 IIS **数据库中的一个数值，就可以达到将** Content-Location **文件头中的** IP **地址信息转换为域名信息的目的。**

第一种方法是通过执行一个 VBS **脚本程序完成** IIS **数据库的相关修改工作，这个脚本程序叫做** Adsutil.vbs，**它随** IIS **安装后生成。**

注意：由于实际的应用环境不同，微软公司没有担保这个软件的使用安全性。所以，我建议在执行这个脚本程序前，做好服务器上的重要数据备份。

对于 IIS4.0 **服务器，执行步骤如下：**

1、**点击“开始/运行”，输入“**cmd**”，点击“确定”，进入命令行状态窗口。**

2、**切换到** IIS4.0 **系统程序安装目录，一般是** c:\winnt\system32\inetsrv\adminsamples。

3、执行以下命令，修改 IIS 数据库相关数值，设置 Content-Location 文件头使用域名信息：

adsutilsetw3svc/UseHostNameTrue

4、执行以下命令，关闭 Internet 服务程序：netstop iisadmin/y

5、执行以下命令，重新启动相关 Internet 应用程序：netstartw3svc

注意：在执行完第 4 步后，要观察一下都有哪些 Internet 应用程序被停止，然后在第 5 步中依次重新启动它们。

对于 IIS5.0 服务器，执行步骤如下：

1、点击“开始/运行”，输入“cmd”，点击“确定”，进入命令行状态窗口。

2、切换到 IIS5.0 系统程序安装目录，一般是 c:\inetpub\adminscripts。

3、执行以下命令，修改 IIS 数据库相关数值，设置 Content-Location 文件头使用域名信息：adsutilsetw3svc/UseHostNameTrue

4、执行以下命令，关闭 Internet 服务程序：netstop iisadmin/y

5、执行以下命令，重新启动相关 Internet 应用程序：netstartw3svc

同样请注意：在执行完第 4 步后，要观察一下都有哪些 Internet 应用程序被停止，然后在第 5 步中依次重新启动它们。

解决方法二：将.htm 文件改名为.ASP 文件，并定制文件头信息

我要介绍的第二种方法采取了一种间接处理的方

式：

1、首先将.HTM 文件改名为.ASP 文件。

2、因为 IIS 对 ASP 文件的响应中，并不包含 Content-Location'>文件头内容，所以接着要在 IIS 管理器中为之创建一个定制文件头，以返回特殊的 Content-Location 文件头内容。

下面我们来看看具体的操作步骤：

1、将静态页面文件（比如.htm，.html）改名为.asp 文件。注意，经过这样的文件改名后，当访问原来的.htm 文件时，将启动 ASP 引擎，从性能上来看，是稍稍有些降低的。

2、启动 Internet 服务管理器

3、双击“ Internet 信息服务 ”，扩展下属内容

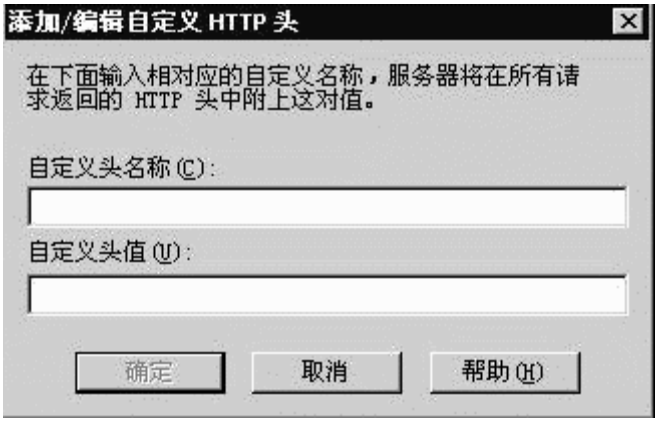
4、点击要处理服务器名字左边的＋号，扩展下属内容

5、右键点击“ 默认 Web 站点 ”，选择“ 属性 ”

6、点击“ 头 ”选项卡

7、**在“自定义头”部分，点击“添加”**

8、**在“自定义头名称”处输入“**Content-Location**”，在“自定义头值”处输入你期望的域名信息，比如“**ttp://www.mywebsite.com**”：**



9、**依次点击“确定”，完成全部修改工作**

Windows2000 安全设置检查清单

前段时间，中美网络大战，我看了一些被黑的服务器，发现绝大部分被黑的服务器都是 Nt/win2000 的机器，真是惨不忍睹。Windows2000 真的那么不安全么？其实，Windows2000 含有很多的安全功能和选项，如果你合理的配置它们，那么 windows2000 将会是一个很安全的操作系统。我抽空翻了一些网站，翻译加凑数的整理了一篇 checklist 出来，希望对 win2000 管理员有些帮助。

本文并没有什么高深的东西，所谓的清单，也并不完善，很多东西要等以后慢慢加了，希望能给管理员作一参考。

具体清单如下：

初级安全篇

1.物理安全

服务器应该安放在安装了监视器的隔离房间内，并且监视器要保留 15 天以上的摄像记录。另外，机箱,键盘，电脑桌抽屉要上锁，以确保旁人即使进入房间也无法使用电脑，钥匙要放在另外的安全的地方。

2.停掉 Guest 帐号

在计算机管理的用户里面把 guest 帐号停用掉，任何时候都不允许 guest 帐号登陆系统。为了保险起见，最好给 guest 加一个复杂的密码，你可以打开记事本，在里面输入一串包含特殊字符,数字，字母的长字符串，然后把它作为 guest 帐号的密码拷进去。

3．限制不必要的用户数量

去掉所有的 duplicateuser 帐户,测试用帐户,共享帐号，普通部门帐号等等。用户组策略设置相应权限，并且经常检查系统的帐户，删除已经不在使用的帐户。这些帐户很多时候都是黑客们入侵系统的突破口，系统的帐户越多，黑客们得到合法用户的权限可能性一般也就越大。国内的 nt/2000 主机，如果系统帐户超过 10 个，一般都能找出一两个弱口令帐户。我曾经发现一台主机 197 个帐户中竟然有 180 个帐号都是弱口令帐户。

4．创建 2 个管理员用帐号

虽然这点看上去和上面这点有些矛盾，但事实上是服从上面的规则的。创建一个一般权限帐号用来收信以及处理一些日常事物，另一个拥有 Administrators 权限的帐户只在需要的时候使用。可以让管理员使用“Run AS”命令来执行一些需要特权才能作的一些工作，以方便管理。

5．把系统 administrator 帐号改名

大家都知道，windows2000 的 administrator 帐号是不能被停用的，这意味着别人可以一遍又一边的尝试这个帐户的密码。把 Administrator 帐户改名可以有效的防止这一点。当然，请不要使用 Admin 之类的名字，改了等于没改，尽量把它伪装成普通用户，比如改成：guest one。

6．创建一个陷阱帐号

什么是陷阱帐号?Look!>创建一个名为”Administrator”的本地帐户，把它的权限设置成最低，什么事也干不了的那种，并且加上一个超过 10 位的超级复杂密码。这样可以让那些 Scriptss 忙上一段时间了，并且可以借

此发现它们的入侵企图。或者在它的 loginscripts 上面做点手脚。嘿嘿，够损！

7.把共享文件的权限从”everyone”组改成“授权用户”

“everyone”在 win2000 中意味着任何有权进入你的网络的用户都能够获得这些共享资料。任何时候都不要把共享文件的用户设置成”everyone”组。包括打印共享，默认的属性就是”everyone”组的，一定不要忘了改。

8.使用安全密码

一个好的密码对于一个网络是非常重要的，但是它是最容易被忽略的。前面的所说的也许已经可以说明这一点了。一些公司的管理员创建帐号的时候往往用公司名，计算机名，或者一些别的一猜就到的东西做用户名，然后又把这些帐户的密码设置得 N 简单，比如“welcome” “iloveyou”“letmein”或者和用户名相同等等。这样的帐户应该要求用户首此登陆的时候更改成复杂的密码，还要注意经常更改密码。前些天在 IRC 和人讨论这一问题的时候，我们给好密码下了个定义：安全期内无法破解出来的密码就是好密码，也就是说，如果人家得到了你的密码文档，必须花 43 天或者更长的时间才能破解出来，而你的密码策略是 42 天必须改密码。

9.设置屏幕保护密码

很简单也很有必要，设置屏幕保护密码也是防止内部人员破坏服务器的一个屏障。注意不要使用 OpenGL 和一些复杂的屏幕保护程序，浪费系统资源，让他黑屏就可以了。还有一点，所有系统用户所使用的机器也最好加上屏幕保护密码。