第19章 IP 安 全

作者：Tim Parker

本章内容包括：

- 使用加密
- 数字签名认证
- 破译加密的数据
- 保护网络
- 应付最坏的情况

在上一章中，读者已经清楚了防火墙、代理服务器和报文过滤器是如何工作的。防火墙是为网络提供安全的重要组成部分，防止非法入侵和访问重要的数据。然而，防止网络的入侵者仅仅是安全问题的一部分。有许多其他问题需要考虑，包括确保用户发送到 Internet上的数据不被不该知道的人读取，确保用户邮件发送人 (或发来邮件的人)身份确实没被冒充，并且在有人确实想通过防火墙时，在网络内部提供特别的安全级别。

很难用绝对的标准来判断所需安全的多少。虽然大多数操作系统提供了基本的文件和目录保护，但是用户可能需要加密或其他方法来保护自己的系统。虽然美国国防部确实想为自己的微型机和大型机 (大多数运行UNIX或过时的操作系统)分配不同的安全级别，但是总体上没有对安全级别进行评价的标准。国防部的防御级别及其描述按从小到大依次为：

- D(最小的保护) 不提供安全和数据保护。
- C1(普通安全) 用户通过用登录名进行标识并且控制对文件和目录的访问。
- C2(控制访问) C1加上审查功能(记录系统行为)并且给予管理员登录特权。
- B1(标记安全) C2加上不能超越的访问控制。
- B2(结构保护) B1加上所有设备安全，支持信任主机，应用程序访问控制。
- B3(安全域) B2加上把系统对象放到不同组里的功能，并且在组内有访问控制。
- A1(可验证的设计) B3加上硬件和软件系统设计可以被验证。

A1安全级别通常认为是不可获得的并且当前没有一个操作系统支持这一级别。多数 UNIX和Windows NT系统能获得C2安全级。一些系统可以达到 B1级，但是B1级以上的安全施加给系统的限制是不可管理的。

所以用户对位于局域网上的操作系统如 Windows、Macintosh、UNIX或Linux能做些什么呢？用户需要采取许多步骤来使自己的系统安全。安全使自己的应用程序免受攻击。如果用户通过TCP/IP连接到Internet，就需要十分小心与协议及其应用程序相关的安全问题。

这一章首先讨论加密问题，加密是为数不多的方法中的一种，使用户数据即使在被劫获的前提下也不被读取。之后，会考查网络安全和 TCP/IP应用程序安全。

19.1 使用加密

几乎没有哪家公司或企业不对数据安全越来越关心，特别是现在每天都有关于黑客进入

企业网内部、商业间谍及解雇员工搞破坏的报告。对更高数据安全的需要越来越显得重要，特别是随着远程访问工作的迅速发展，员工可以从家中、旅店里或在大街上使用移动服务来访问公司网络。用户必须考虑往返于 Internet和电话线上的数据保护，使即使劫获了数据的人也读不懂。惟一有效且相对容易的方法是通过加密来保护数据。

加密已经成为一项重要的并且有利可图的事情。从事加密产品生产的公司遍布世界各地，几家核心的公司已经从事这项技术的推动工作几十年了。仅仅在几年以前，得到真正优秀的加密产品还比较难，因为聪明的代理尽量使加密算法不要太强大 (因此可以防止他们监听自身)。直到几年前，出口任何比 40位更好的加密产品在美国还是不合法的，因为加密系统可以当作武器。随着通过 Internet可以容易地访问免费或共享的加密产品，同时迫于应用程序生产商和操作系统生产商的压力， 128位的加密产品也能出口到世界各地 (除了限制为数不多的几个国家之外)一些国家，甚至可以得到更强大的加密方法。

在没有作更细致的考查之前，加密使用密钥来打乱数据使得没有密钥来解码数据的人读不懂。密钥越长，加密数据所需时间就越长。简单的口令加密能很好地工作，因为必须清楚地知道口令才能解密数据。当用户使用口令把一个信息打乱时，只有相同的口令才能解密消息。

如果读者对基于口令的加密工具感兴趣，可以访问站点 http://www.fim.uni-linz.ac.at/codeddrag/codedrag.htm。CodedDrag的一个评估拷贝是免费的，通过给站点服务器基金会发少量的捐款就可以注册这一拷贝，无限制地使用。 CodedDrag由奥地利的Linz大学所开发，提供了数据加密标准 (DES)非常快的实现(实际上， CodedDrag提供了DES, Triplo-DES以及Blowfish加密方法；其中后两个比 DES更难被解密)。CodedDrag能作为Windows 95/98或Windows NT的组成部分嵌入系统，在弹出菜单中加入加密、解密选项即可。在一次性提供给系统口令之后，加密和解密文件就能以不被察觉的速度完成。

19.1.1 公共-私钥加密

公共-私钥加密对Internet用户来说是使用很广泛的加密方法，因为它允许在不必知道其他密钥的情况下来解密报文。公共 -私钥系统的工作方式很简单：用户有两个密钥或口令串，其中一个任何人都可以得到；而另一个串，是用户的私钥，只有用户自己知道。某个人如果想发送加密的消息，他就需要知道公钥。之后，加密软件根据公钥打乱数据。在接收到数据之后，只有私钥能对报文进行解密，使只有知道私钥的人才能读懂数据。公钥不能解密数据。当用户需要给别人发消息时，他应使用对方的公钥。为了传播这种加密方法，许多用户把自己的公钥附加在电子邮件里。

1. RSA数据加密

最早的一个提供公共 -私钥加密工具的商业产品是 RSA数据安全(http://www.rsa.com)，这个公司由麻省理工学院的科学家在 1977年成立。RSA仍在广泛使用，并且价格比较便宜，非常安全，使用方便。 RSA为不同的操作系统提供了几种不同形式，但是最简单的形式是给浏览工具(如Windows Explorer)加上一些菜单项。选择一个文件并使用加密菜单选项，在用户输入口令之后加密文档将能自动完成。为了解密，菜单项会弹出一个窗口询问口令，如果口令正确，就可以得到解密的文件。口令可以存储以简化这一过程。

2. Phil Zimmermann的PGP

一个最有名的加密工具是 Phil Zimmermann的PGP。美国政府指控Zimmermann有罪，因

为他使PGP在Internet上可以免费获得。指控最后被撤消，但却说明了 PGP的广泛使用，特别是在美国之外的国家。 PGP可以从许多Web站点上获得，并且可以经常看到 PGP密钥作为电子邮件的附件。

19.1.2 对称私钥加密

加密的最基本形式是对称私钥。这非常类似于许多年前的解码器环。简单的对称密钥使用一些字母代替别的字母。比如，所有的 a被x代替，所有的b被d代替，等等。对称密钥的最简单形式是选择字母表中新的起始点，按顺序依次取代 (a变为d，b变成e，c变为f等等)。

更灵活的对称密钥随机地产生替代，有时需要一个口令来指出编码是如何实现的。对称密钥容易开发且工作效率高。不幸的是，简单的对称密钥非常容易被破解。原因很简单：给出一定数量的文本，就可以通过字母频率得到所使用的字母映射关系。字母 e是语言中最常见的字母；如果加密的文本中的 x最多，就可以设想x和e具有映射关系。一旦找出一些映射，其他映射可以通过观察字段来加以识别，这就像完成一个填字游戏。相同的密钥既用于加密也用于解密。为了使对称密钥更安全，开发了许多编码替代选择方案。

19.1.3 DES、IDEA及其他

IBM在1976年为美国政府开发了数据加密标准 (DES)。DES是使用64位密钥的56位算法。加密和解密报文使用相同的密钥。 DES不是真正的对称私钥加密。理论上，解密 DES总是可能的。需要作72×10^{15}次测试，但是有个小组确实成功解密 (赢得10 000美元)，证实了DES不是完全安全。关于DES面临挑战的更多信息可以在站点 http://www.frii.com/~rcv/deschall.htm上找到。Triple DES加密是对基本算法的改进，它使用更多的位，有效地增加了被解密的难度。

国际数据加密算法 (IDEA)可能是今天最安全的算法。 IDEA由瑞士联邦技术研究所开发，IDEA是使用128位密钥的64位算法。但使用反馈操作使算法强化。 IDEA的一个增强版本是Triple IDEA。完全的IDEA算法要耗费一些时间，所以研究人员开发出几个简单的版本。一个最有名的系统是Tiny IDEA。获得关于Tiny IDEA的更多信息并且下载一个免费的拷贝，可以访问：http://www.dcs.rhbnc.ac.uk/~fauzan/tinyidea.html

CAST(开发者Carlisle Adams和Stafford Tavares的名字首字母)，使用64位密钥和64位数据块进行加密。在CAST背后有许多程序，称为S-boxes，使用8位和32位输入。在这里细节不重要，因为解释清楚要用整个一本书。 CAST还没有被破解过，但和IDEA一样，CAST加密/解密速度慢。在站点：http://www.cs.wm.edu/~hallyn/des/sbox.html可以得到关于CAST的更多信息。

一个称为Skipjack的加密系统由国家(美国)安全局专门为Clipper芯片开发，这个芯片美国政府想用在所有的在线设备中 (达到监控目的)。Clipper芯片没有成功实现，而Skipjack系统却开发成功了。 Skipjack的细节是保密的，但知道 Skipjack使用80位的密钥进行 32次处理。Skipjack使用两个密钥：一个私钥，一个由政府保留的主 (master)密钥。理论上讲，破译Skipjack加密的报文，要用现在最好的机器工作 4000亿年。AT&T为几家生产商，包括其自己提供Clipper芯片(同时提供Skipjack)。

RC2和RC4是由RSA数据安全开发的保密算法。对他们而言不幸的是，算法源码在Internet通过邮件转发，使其不再是保密的。 RC4被认为是相当安全的， Netscape公司在Navigator的出口版中使用RC4。但几乎同时，由两个不同的组织只用了大约 8天完成了对密文

的破译工作。

所提及的算法中，哪一个是最快而又最安全的加密算法？最安全的 Triple DES、IDEA、Triple IDEA、Skipjack的安全性差不多，这几个算法相当安全，非授权的解密几乎不可能。然而，加密解密所需的开销也值得注意。如果假设 DES用1秒来加密或解密一个文档，那么Triple DES会用3秒钟，IDEA用2.5秒，Triple IDEA用4秒钟。看起来时间很短，但是如果是大文档且有许多文件要加密，越安全的算法所造成的延迟就越不容忽视。理论上， Skipjack与DES一样快，但是谁又相信掌握了密钥的(美国)政府呢？

今天使用的基本公共-私钥加密系统是RSA，RSA由发明者名字首字母构成(Rivest、Shamir和Adleman)，另一个强劲的竞争者是Phil zimmermann的PGP。RSA和PGP都能使用很长的密钥，经常100位或更长。密钥越长，加密和解密所需的时间就越长，在没有密钥的前提下，解密报文就越困难。使用1024位的密钥也不少见。RSA站点(http://www.rsa.com/rsalabs/newfaq)讨论了加密强度与密钥长度的关系。512位的密钥要使用相当多的计算机来破译，但确实可以做到这一点。更长的密钥(768位或1024位)需要更强大的计算机，而绝大多数黑客不具有这个条件。理论上讲，任何密钥系统都可以被破译，或者通过硬性分析方法，或者基于一些加密的文字进行猜测，但是RSA和PGP只要使用足够长的密钥就可以应付这些破译企图。

Diffie-Hellman系统是密钥交换算法(Key Exchange Algorithm，KEA)，用于控制和产生公共密钥分发过程中需要的密钥。Diffie-Hellman不对消息进行加密和解密处理：它的惟一作用是产生安全的密钥。过程简单，但需要通信端(发送方和接收方)一同工作，基于素数来产生密钥。

19.2 数字签名认证

除了加密数据之外，还有一个重要的安全问题需要讨论——能够确认消息发送人(接收人)的身份。毕竟，加密的错误信息和加密的有价值信息一样安全。为了认证发送方和接收方身份可以使用数字签名系统。数字签名使用公共-私钥加密。公共-私钥加密允许任何人依赖于公钥(公共密钥)确认发送方的身份，因为消息由发送方使用私钥进行加密。

美国政府开发，采用了数字签名标准(DSS)系统。正如其名字，DSS系统提供了数字签名认证。但是，DSS有一个主要缺陷，如果相同的随机加密号被选择两次，同时，黑客有两个使用那个随机数的报文，DSS就容易暴露自己的密钥。甚至消息的内容有时容易被破译。

安全hash算法(SHA)和安全hash标准(SHS)也是由美国政府开发，但是比DSS更安全。SHS使用160位密钥的散列算法，但有点慢。考虑到RSA和PGP的工作速度，所以人们不愿意采用SHS。

另一个数字签名方法是消息摘要算法，这个算法中至少有 3个比较常用(MD2、MD4和MD5)，MD系列算法使用输入产生一个数字“指纹”。“指纹”是128位的编码，称为消息摘要。没有两个相同的消息会产生相同的消息摘要(理论上)。MD5是最安全的，由RSA利用特殊的散列算法开发。微软在Windows NT用户文件中使用MD4加密口令项。MD4已被破译过多次。在一些Web站点上可以得到一些程序来加密Windows NT口令文件(如http:// www.masteringcomputers.com/util/nt/pwdump.htm和相同页面上的ntcrack.htm)。

证书服务器管理公司或组织的公共密钥，并且通常情况下可以通过 Internet访问该服务器。有一些商业的证书服务器为 Windows和UNIX平台设计。最好的一个是 Netscape公司开发的。Netscape制作了一个FAQ用于描述用户使用证书服务器的原因是及其产品的特点。访问 FAQ，http://www.netscape.com/comprod/server_central/support/faq/certificate_faq.html#1。

最后讨论一下kerberos。如果用户浏览过Web或已安装了服务器，那么就运行过 kerberos好几次了。通过在用户级控制对网络的访问， kerberos提供了一种安全方式。 kerberos服务器位于网络中的某个地方 (通常在一台安全机器上)。kerberos服务器有时被称为密钥分发中心(KDC)。一旦用户请求一些网络服务， kerberos服务器就会认证用户的身份，并确定服务在某台适当的机器上。 kerberos系统的安全基于私钥加密系统，这个私钥加密系统以 DES为基础。网络上的每一个客户机和服务器有一个私钥，这个私钥在每一个kerberos控制的行为中被检查。kerberos需要一台专门的服务器，所以 kerberos服务器经常出现在大型网络并且需要严格安全控制的场合。

19.3 破译加密的数据

破译密码系统的科学(有人称为艺术)称为密码分析。这个过程是在不知道密钥的情况下试图读懂加密的消息，密钥用于在第一阶段加密消息。有许多破解密码的方法，最常见的是知道一些消息内容或密钥的一部分。如果知道消息是关于 ABC公司股票的事，那么就可以很好地检测加密消息中特定词的含义。这样可以更快地得到加密所使用的密钥。这种破译加密类型称为平文(plaintext)破译，因为破译者知道了一部分消息并从消息的其余一部分中得到密钥。

有时密钥会被偶然地或有目的地泄漏。知道密钥的部分内容，或知道密钥的可能组成，也会缩短破译时间。举个例子，如果知道某人有喜欢用自己孩子的名字作为密钥的习惯，并且知道了他孩子的名字，就非常可能破译消息。得到密钥通常不是很难，特别是消息在Internet上传送时。有许多劫获IP报文的方法并且可以最终劫获用户关于密钥的想法。如果破译者能得到部分密钥或消息两端的公共密钥，那么破译整个报文就容易得多。

如果没有这些有益的信息，密码学分析会采取硬性方法。有许多不同的方法用于破译消息，这要依赖于黑客所使用的技术：猜测消息或密钥，以及充分地使用大脑智力和计算机。当只有加密的消息时可以使用密码文 (Ciphertext)方法。之后计算机试图用各种密钥来解密报文，有时需要一些解密专家的帮助，这些人能猜出报文中的一些词。由于大多数消息遵循标准的格式(有多少种不同的方式来构造一封商业信件？)，解密人员可以使用一部分加密的报文来选择一个密钥最终达到破译整个报文的目的。

如果加密算法是已知的，就可以使用变化的平文方法。解密者使用相同的加密算法 (但是不同的密钥)把一条消息编码成目标形式。使用不同的消息和密码重复这一过程，就可以得到用于加密消息的密钥的信息。这种技术相当有效。

数学上有一些复杂的方法用于破译消息，这些方法依赖于公共 -私钥的复杂性。在密钥和加密消息之间有一种关系，并且这种关系可以通过足够的数字组合推导出来。数学家已经写了整整一本书用于论述采用理论方法破译加密消息的方法，其中许多方法已被为国家安全局工作的科学家和工程师所采用。

19.4 保护网络

大多数局域网不认为具有安全问题，但是局域网往往会成为进入系统的最容易方法。如果网络上的任何一台机器是弱访问点，那么网络上的所有机器将通过那台机器提供的服务被访问。

PC和Macintosh几乎没有安全性可言，特别是和呼入调制解调器相连时，所以它们经常被

用来以相同的方式访问网络服务。关于局域网的一个基本规则是：如果有非安全机器，那么相同网络上不可能有安全机器存在。因此，针对于任何一台机器的解决方法要在网络上的所有机器上实现才行。

19.4.1 登录名和口令

通过网络，调制解调器联接或坐在终端前面等待来进入系统的最常见方法是利用安全性差的口令。安全性差(意味着容易猜测)的口令非常普遍。当系统用户使用安全性差的口令时，即使最好的安全系统也不能保证不被入侵。

假如读者正管理具有多用户的系统，就应该实现一种策略，要求用户在固定的间隔时间内设置其口令(时间间隔取为6到8个星期较好)，并且口令要使用非英文单词。最好的口令应是在字典里找不到的字母与数字组合。

但是，有时仅有防止安全性差的口令策略还不够。用户可能想通过使用公共域或能对口令进行安全性检查的商业软件来加强软件的安全性。对大多数操作系统而言，可以得到由第三方厂商提供的用于强化口令安全性的商业和共享软件工具。

如果用户运行的是UNIX或Linux操作系统，那么就需要特别注意 /etc/passwd和/etc/group文件。这些文件应该设置非使用帐号不能在文件中出现，所有帐号应设置口令保护。Windows NT用户通过用户管理域正确地实现用户帐号，用户管理域允许用户设置工作组和域帐号。但Windows 95和98这两个操作系统上没有真正的帐号安全性。任何用户使用机器时都可以建立一个新的帐号。如果 Windows 95或98机器不是Windows NT系统所控制域的一部分、Windows 95或98客户程序就会成为网络的薄弱点。

19.4.2 文件的目录允许权限

文件的允许访问级别是安全问题的来源，应该仔细加以考虑。如果想保护文件免受非授权侵入者或其他用户窃取，就应小心地设置文件的允许访问权限，以便获得最高的安全性。

设置文件或目录访问权限的方式依赖于操作系统。在 UNIX或Linux操作系统上，用户可以使用 Chmod(改变模式)命令，然而在视窗 95、98和NT系统上用户需要使用访问控制表(Access Control List，ACL)。

调制解调器是进入每个系统最常用的接口 (除了用户完全单机工作或在一个封闭的网络上之外)。调制解调器用于远程用户访问，同时也用于网络和 Internet之间的访问。保护系统调制解调器的安全是免受入侵的简单方式，能有效地阻止文件被读取。

防止非授权用户通过调制解调器进行访问的最有效技术是采用回调调制解调器。回调调制解调器允许用户按一般方法联接系统；之后，在与用户建立呼叫之前这种调制解调器会参考一个有效用户列表及其电话号码。回调调制解调器非常昂贵，所以对许多系统而言，这不是实用的方法。

回调调制解调器也有一些问题，特别是当用户经常改变位置时。现代电话交换机的呼叫转发特性也会导致回调调制解调器的脆弱性。

如果调制解调器在用户会话过程完成之后没有正常挂起，也会引起问题。更常见的问题是调制解调器线路问题或配置设置问题。

线路问题好像无关紧要，但是许多使用手工接线的电缆线系统不能正常控制所有的针，

可导致系统使调制解调器会话非正常关闭或退出不能完成。任何呼叫调制解调器的用户能从上一个用户结束的地方继续。为了防止这种问题，要确保调制解调器电缆和机器的是完全连接的。用制造优良的商业电缆代替令人担心的手工接线电缆。当几个会话结束时也可以观察调制解调器以确保线路正常挂起。

19.4.3 信任关系

在信任关系中，一台机器决定允许另一台机器的用户访问资源而无需再次登录。这是基于如下的假设，一台机器上的合法用户能被另一台机器所信任。信任关系是几年前提出的，用于简化用户对网络资源的访问。假设用户登录到另一台机器上，需要那台机器上的文件或应用程序。每次都要输入登录名和口令很不方便，因此信任关系允许用户不需每次登录就可以访问资源。信任关系不同于网络信息服务 (NIS)或者黄页(YP)，NIS和YP使用集中式用户和口令文件。

大多数操作系统允许设置信任关系， Windows NT、UNIX和Linux中有这样的特殊例程。信任关系的问题显而易见：如果某个人闯入系统，就可以访问与这个系统有信任关系的每台机器。

信任关系可以是双向的 (两台机器彼此信任)也可能是单向的 (一台机器信任另一台机器，但是反之不然)。整个网络可以具有信任关系。举个例子，假设在公司网内有三个子网，其中一个子网含有需要安全保护的重要信息，而另外两个子网包含一般用户。为了防止访问资源时登录每个网络，可以在三个子网之间设置信任关系，但是管理员可能不想建立安全网络对不安全网络的信任关系(但允许安全网络访问非安全网络上的任何资源)。两个非安全网络之间是双向信任关系，安全网络和非安全网络之间是单向信任关系， Windows NT和UNIX可以非常容易地设置信任关系。

从安全的角度看，必须要确保设置的信任关系能限制从信任的主机或网络来的入侵所造成的损害。包含重要信息的机器不应该信任可以被广泛访问到的那些机器。

19.4.4 UNIX和Linux系统上的UUCP

UNIX UUCP程序设计时就很好地考虑了安全。然而， UUCP是许多年前设计的，这些年，对安全的要求已经发生了重大变化。已经发生了许多和 UUCP有关的安全问题，其中许多问题通过改变系统或为系统打补丁得到解决。一些管理员仍然要注意 UUCP以确保其能正常、安全地工作。

如果用户不打算使用 UUCP，可以把UUCP用户从/etc/password文件中完全删除或者使用不被猜到的强口令 (在/etc/passwd文件中的口令域前加一个“ * ”号，能有效地阻止登录)。删除/etc/passwd中的UUCP不会影响Linux系统上的任何其他设置。

管理员要对 UUCP设置尽可能严格的访问权限 (UUCP目录通常位于 /usr/lib/uucp、/usr/spool/uucp、和/usr/spool/uucppublic)。多数系统对这些目录的访问权往往不一样，所以使用chown、chmod，以及chgrp来限制其只能在UUCP登录时才能被访问。所有文件的组和用户名应设置为UUCP。经常性地检查文件的访问权限。

UUCP使用几个文件来控制允许登录的用户。这些文件 (/usr/lib/uucp/Systems和/usr/lib/uucp/Permissions)的所有权和可访问权限，应该只限制为 UUCP登录。这样可以防止非法入

侵者使用另一个登录名来修改这些文件。

目录/usr/spool/uucppublic是非法入侵者一般的攻击目标，因为这个目录要求访问它的所有系统具有读和写访问权。为了保护这个目录，可以创建两个子目录：一个用于接收文件另一个用于发送文件。如果管理员想更安全，可以为每一个在合法用户列表中的系统更进一步创建子目录。

19.5 应付最坏情况

假设有人确实闯进了网络并对网上机器造成了破坏，在这种情况下该如何处置？显然，备份系统是有帮助的，因为这样使管理员能恢复被损害或被删除的文件。但在这之后，应该采取怎样的行为？

首先，找出入侵者进入系统的方式，之后对访问方法采取安全措施，防止再次被入侵。如果不能确信访问方法是否安全，关掉所有的调制解调器和终端并且仔细地检查所有的配置和设置文件，寻找漏洞。一定存在漏洞，否则入侵者不能进入系统。也要检查口令和用户列表文件，寻找安全弱点或陈旧的信息。

如果被重复攻击，可以考虑使用审查系统记录入侵者进入的方法及其所作所为，一看到有入侵者登录，就要把他们驱除走。

如果入侵行为持续发生，可以寻求地方当局帮忙。侵入计算机系统 (不论是大型公司还是家庭)在大多数国家是非法的，当局一般知道如何跟踪用户到其呼叫点。他们侵入到别人的系统，不应该消遥法外。

19.6 小结

本章讨论了加密和认证，同时也讨论了一些基本的安全注意事项。 TCP安全问题有许多方面，本章只是讨论了表面的一些东西。如果读者想了解关于计算机和网络安全方面更多的知识，可以参考有关这一主题的书籍，其中一本比较优秀的是 Sams公司出版的《Maximum Security》一书。