网络安全

安全技巧（十九）

小未 主编

目　录

确保你邮件安全的技巧

“假痴不癫”意为凡有作为的人，一般都腹有良谋，筹划于暗中，不露声色而后发制人。在 E-mail 的安全防范中，我们同样可以使用“假痴不癫”之计谋，从系统、杀毒、防黑等多方面为 E-mail 打造出一条安全防线……

E－mail 的安全隐患浅析

E-mail 作为目前网络中人际交往中使用最广泛的通信工具，它的安全问题在数年前就引起了各方面的关注。简单地说，E-mail 在安全方面的问题主要有以下直接或间接的几方面：

●密码被窃取：木马、暴力猜解、软件漏洞、嗅探等诸多方式均有可能让邮箱的密码在不知不觉中就拱手送人。

●邮件内容被截获

●附件中带有大量病毒：它常常利用人们接收邮件心切，容易受到邮件主题吸引等心理，潜入和破坏电脑和网络。目前邮件病毒的危害已远远超过了传统病毒。

●邮箱炸弹的攻击

●本身设计上的缺陷

下面将针对电子邮件可能对我们构成的种种威胁，从保证邮箱与邮件的安全，以及对系统安全性的目的出发，来谈一些切实可行的防范对策。

邮件客户端软件使用限制

由于邮件客户端软件（如 Foxmail）是邮件收发的操作环境，所以对邮件客户端软件进行使用限制，我们

可以将其视为第一道防线。以 Foxmail 为例，根据操作系统的不同，通常有如下几种限制方法：

1.在 Windows98 等安全性设计不完善的操作系统中，可使用 PCSecurity 等第三方安全工具来完成对 Foxmail 的使用限制。在安装完该软件后，只需右键点击 Foxmail 图标，在弹出的快捷菜单中依次选择“ PCSecurity ”、“ Lock ”即可达到“ 锁定 ”式的限制使用效果。当需要使用 Foxmail 的时候，必须输入相应的解锁密码方可使用 Foxmail。

2.在使用 WindowsXP 等安全性较好的系统时，除了可以使用 PCSecurity 这类的第三方加密工具外，还可以使用系统本身的加密功能。前提是 Foxmail 软件应该安装在 NTFS 分区中，然后就可以右键点击该图标，在弹出的菜单中选择“ 属性 ”，点击切换到“ 安全 ”选项卡设置界面后，根据需要，设置有权使用此程序的用户。

邮箱密码的安全措施

邮箱密码是目前最容易遭到破解的注册密码之一，其危害性之大、波及范围之广均不容忽视。因此我们应该采用以下措施来尽量降低风险：

1.强烈建议使用“ 足够长度的不规律密码组合+定时更换的密码 ”。

2.设置密码提示问题及回答要复杂。在注册邮箱的时候大都会需要设置一个密码提示问题，用于恢复密码时使用。但是这有时将会给黑客带来“ 猜测 ”的机会！比方说一些用户的提示问题是 123，回答的答案是 321。那么稍有经验的黑客都会首先测试这样的问题与答案，从而不费吹灰之力将邮箱破解掉。所以对于这个提示问题和密码，还是应该起一个既有意义容易记忆且又不易

被黑客猜中的问题密码为宜。

邮件的加密

邮件的加密是一种比较有效的、针对邮件内容的安全防范措施，而 HotCrypt 正是这样一款用于邮件加密的软件，非常适合新手使用。HotCrypt 采取了先进的加密算法，可以有效地保障数据的安全，它支持任何邮件程序或其他文件编辑窗口，通过热键即可快速加密，方便易用。接下来，我们就详细介绍一下如何在 Foxmail 下进行邮件加密的操作：

步骤一：在运行 HotCrypt 并在 Foxmail 邮件撰写窗口中编辑内容后，按组合键“ Ctrl+E ”即可调出 HotCrypt 的加密窗口对邮件加密。

步骤二：在“ 输入密码 ”下方的文本框中输入密码后，单击“ 确定 ”按钮返回到邮件编辑窗口中，你会发现邮件正文内容已经变成了加密后的密文。

小提示：HotCrypt 只能对最上层的当前窗口中内容进行加密。当朋友收到这封邮件后，他也需要在运行 HotCrypt 后，按组合键“ Ctrl＋D ”调出密码输入窗口后输入正确的密码方可正常阅读到邮件的内容。

邮件病毒的防范

当电子邮件日益成为日常交往的重要手段的同时，病毒的阴影也开始环绕在电子邮件的周围。今天，有超过七成以上的计算机病毒是通过电子邮件传播的。那么我们如何才能较全面地阻截邮件病毒呢？通常可以使用如下措施：

1．禁止其他程序暗中发送邮件

为了防止邮件病毒自动查询用户的通讯录，再以用户的名义发给用户的亲朋好友。以 OutlookExpress6.0 为

例，我们可以进行如下设置：

依次点击“工具→选项→安全”，点击选中设置界面中的“当别的应用程序试图以我的名义发送电子邮件时警告我”选项前的复选框，这样，当任何悄无声息的“地下邮件发送活动”都将被发现并立即报告用户。

2．启动 OutlookExpress6．0 的自防毒选项

由于邮件病毒大多是通过加载邮件附件的方式进行传播，所以可以使用禁止 OE 打开附件的方法防止此类病毒的侵害。方法如下：运行 OE6.0，依次点击“工具”、“选项”、“安全”，点击选中设置界面中的“不允许保存或打开可能有病毒的附件”标签前的复选框，这样就可以启用 OE 的自我保护机制功能了。

3．修改关联

有些蠕虫通过.vbs 等格式的邮件附件传播，要减少这类病毒带来的风险，一种简单的办法是修改文件的关联属性，使得打开脚本文件时（例如用户双击一个附件）它不会自动运行。打开 WindowsXP 的“控制面板”，双击“文件夹选项”，选择“文件类型”选项卡，选中.vbs 文件类型。

接着把它的默认操作改成记事本（而不是默认的用 VBScript 运行），点击“高级”按钮，在“编辑文件类型”对话框中选中“编辑”，在弹出的“编辑这种类型的操作”对话框中指定打开的程序为记事本。

小提示：对于．vbe、．wsf、．wsh、．js 和．jse 这些文件类型也可以做同样的修改，修改文件关联属性的办法不可能隔绝所有的风险。

修改文件的关联属性之后，当你点击一个脚本文件，它不会再像原来那样自动运行，而是会用记事本打开并

处于编辑状态。如果要运行脚本，你必须在脚本的快捷方式中显式地指定要用 VBScript.exe 来打开脚本文件。

4．使用杀毒软件

现在绝大多数的杀毒软件都提供了对邮件内容进行病毒检测的功能，比方说瑞星杀毒软件就可以很好地做到这一点，它可以让我们在发送与接收邮件时，自动对邮件进行一遍病毒检测，以防系统“中毒”。

邮箱炸弹的防范

邮件炸弹的防范比较繁琐,而且很难保证万无一失，但我们可以使用如下方法来尽可能地避免邮件炸弹的袭击和做好善后处理：

●不随意公开自己的信箱地址

●隐藏自己的电子邮件地址

如将 shy@public.sq.js.cn 在输入时改成 shy·public.sq.js.cn，这样一来大家都知道这个实际上就是邮箱，但是一些邮箱自动搜索软件就无法识别这样的“邮箱”了。

●谨慎使用自动回信功能

“自动回信”功能设计初衷很好，但也有可能被利用制造邮件炸弹！试想一下，如果接收和发送双方都设置了“自动回信”设置，而双方都没有及时看信的话，就会在反复“自动回信”中造就了一颗邮箱炸弹。

打好补丁

在软件设计中，经常会出现一些意想不到的错误和漏洞，给程序带来安全和稳定性方面的隐患。因此，经常保持对软件的更新，是保证系统安全的一种最简单也是最直接的办法。

邮件的备份

谈到邮件的安全就不能不谈谈备份这个话题，但由

于邮件备份的方法因软件的不同，往往可以使用很多的方法，所以本文不便细述。但基本上都应做到为接收的邮件设置一个专门的目录、导出“通讯簿”等方面的备份操作。

以太网中进行监听的原理

网络监听工具是提供给管理员的一类管理工具。使用这种工具，可以监视网络的状态、数据流动情况以及网络上传输的信息。

但是网络监听工具也是黑客们常用的工具。当信息以明文的形式在网络上传输时，便可以使用网络监听的方式来进行攻击。将网络接口设置在监听模式，便可以源源不断地将网上传输的信息截获。

网络监听可以在网上的任何一个位置实施，如局域网中的一台主机、网关上或远程网的调制解调器之间等。黑客们用得最多的是截获用户的口令。

什么是网络监听

网络监听是黑客们常用的一种方法。当成功地登录进一台网络上的主机，并取得了这台主机的超级用户的权限之后，往往要扩大战果，尝试登录或者夺取网络中其他主机的控制友。而网络监听则是一种最简单而且最有效的方法，它常常能轻易地获得用其他方法很难获得的信息。

在网络上，监听效果最好的地方是在网关、路由器、防火墙一类的设备处，通常由网络管理员来操作。使用最方便的是在一个以太网中的任何一台上网的主机上，

这是大多数黑客的做法。

以太网中可以监听的原因

在电话线路和无线电、微波中监听传输的信息比较好理解，但是人们常常不太理解为什么局域网中可以进行监听。甚至有人问：能不能监听不在同一网段的信息。下面就讲述在以太网中进行监听的一些原理。在令牌环中，道理是相似的。

对于一个施行网络攻击的人来说，能攻破网关、路由器、防火墙的情况极为少见，在这里完全可以由安全管理员安装一些设备，对网络进行监控，或者使用一些专门的设备，运行专门的监听软件，并防止任何非法访关。然而，潜入一台不引人注意的计算机中，悄悄地运行一个监听程序，一个黑客是完全可以做到的。监听是非常消耗 CPU 资源的，在一个担负繁忙任务的计算机中进行监听，可以立即被管理员发现，因为他发现计算机的响应速度令人惊奇慢。

对于一台连网的计算机，最方便的是在以太网中进行监听，只须安装一个监听软件，然后就可以坐在机器旁浏览监听到的信息了。

以太网协议的工作方式为将要发送的数据包发往连在一起的所有主机。在包头中包含着应该接收数据包的主机的正确地址。因此，只有与数据包中目标地址一致的那台主机才能接收信包。但是，当主机工在监听模式下，无论数据包中的目标物理地址是什么，主机都将接收。

在 Internet 上，有许多这样的局域网。几台甚至十几台主机通过一条电缆一个集线器连在一起。在协议的高层或用户看来，当同一网络中的两台主机通信时，源

主机将写有目的主机 IP 地址的数据包发向网关。但是，这种数据包并不能在协议栈的高层直接发送出去。要发送的数据包必须从 TCP/IP 协议的 IP 层交给网络接口，即数据链路层。

网络接口不能识别 IP 地址。在网络接口，由 IP 层来的带有 IP 地址的数据包又增加了一部分信息：以太帧的帧头。在帖头中，有两个域分别为只有网络接口才能识别的源主机和目的主机的物理地址，这是一个 48 位的地址。这个 48 位的地址是与 IP 地址对应的。也就是说，一个 IP 地址，必然对应一个物理地址。对于作为网关的主机，由于它连接了多个网络，因此它同时具有多个 IP 地址，在每个网络中，它都有一个。发向局域网之外的帧中携带的是网关的物理地址。

在以太网中，填写了物理地址的帧从网络接口中，也就是从网卡中发送出去，传送到物理的线路上。如果局域网是由一条粗缆或细缆连接机而成，则数字信号在电缆上传输，信号能够到达线路上的每一台主机。当使用集线器时，发送出去的信号到达集线器，由集线器再发向连接在信线器上的每一条线路。于是，在物理线路上传输的数字信号也能到达连接在集线器上的每一主机。

数字信号到达一台主机的网络接口时，在正常情况下，网络接口读入数据帧，进行检查，如果数据帧中携带的确良物理地址是自己的，或者物理地址是广播地址，则将数据帧交给上层协议软件，也就是 IP 层软件，否则就将这个帧丢弃。对于每一个到达网络接口的数据帧，都要进行这个过程。然而，当主机工作在监听模式下，则所有的数据帧都将被交给上层协议软件处理。

局域网的这种工作方式，一个形象的例子是，大房间就像是一个共享的信道，里面的每个人好像是一台主机。人们所说的话是信息包，在大房间中到处传播。当我们对其中某个人说话时，所有的人都能听到。但只有名字相同的那个人，才会对这些话语做出反映，进行处理。其余的人听到了这些谈话，只能从发呆中猜测，是否在监听他人的谈话。

当连接在同一条电缆或集线器上的主机被逻辑地分为几个子网时，如果一台主机处于监听模式下，它还能接收到发向与自己不在同一子网(使用了不同的掩码、IP 地址和网关)的主机的那些信包。也就是说，在同一条物理信道上传输的所有信息都可以被接收到。

许多人会问：能不能监听不在同一个网段计算机传输的信息。答案是否定的，一台计算机只能监听经过自己网络接口的那些信包。否则，我们将能监听到整个 Internet,情形会多么可怕。

要使主机工作在监听模式下，需要向网络接口(Interface)发送 I/O 控制命令，将其设置为监听模式。在 UNIX 系统中，发送这些命令需要超级用户的权限。这一点限制了在 UNIX 系统中，普通用户是不能进行网络监听的。只有获得超级用户权限，才能进行网络监听。但是，在上网的 Windows95 中，则没有这个限制。只要运行这一类的监听软件即可。同时，在微机上运行的这类软件具的操作方便，对监听到信息的综合能力强的特点。

目前的绝大多数计算机网络使用共享的通信信道。从上面的讨论中，我们知道，通信信道的共享意味着，计算机有可能接收发向另一台计算机的信息。

另外，要说明的是，Internet 中使用的大部分协议都

是很早设计的，许多协议的实现都是基于一种非常友好的，通信的双方充分信任的基础之上。因此，直到现在，网络安全还是非常脆弱的。在通常的网络环境下，用户的所有信息，包手户头和口令信息都是以明文的方式在网上传输。因此，对于一个网络黑客和网络攻击者进行网络监听,获得用户的各种信息并不是一件很困难的事。只要具有初步的网络和 TCP/IP 协议知识,便能轻易地从监听到的信息中提取出感兴趣的部分。

网络监听常常要保存大量的信息，对收集的信息进行大量的整理工作，因此，正在进行监听的机器对用户的请求响应很慢。

首先，网络监听软件运行时，需要消耗大量的处理器时间，如果在此时，就详细地分析包中的内容，许多包就会来不信接收而漏掉。因此，网络监听软件通常都是将监听到的包存放在文件中，待以后再分析。

其次，网络中的数据包非常复杂，两台主机之间即使连续发送和接受数据包，在监听到的结果中，中间必然会夹杂了许多别的主机交互的数据包。监听软件将同一 TCP 会话的包整理到一起，已经是很不错了。如果还希望将用户的详细信息整理出眯，需要根据协议对包进行大量的分析。面对网络上如此众多的协议，这个监听软件将会十分庞大。

其实，找这些信息并不是一件难事。只要根据一定的规律，很容易将有用的信息一一提取出来。

信息安全管理的国际标准

对一个企业或机构来说，信息和其它商业资产一样有价值。信息安全就是保护信息免受来自各方面的威胁，是一个企业或机构持续经营策略和管理的重要环节。信息安全管理体制的建立和健全，目的就是降低信息风险对经营的危害，并将其投资和商业利益最大化。从对信息安全的认识来说，一方面，新闻媒体上不断披露的安全漏洞、频繁的病毒和黑客的攻击、日益增多的网络犯罪让人们不断地提高安全意；另一方面，人们也已经越来越深刻地认识到，信息安全不只是个技术问题，而更多地是商业、管理和法律的问题。实现信息安全不仅仅需要采用技术措施，还需要更多地借助于技术以外的其它手段，如规范安全标准和进行信息安全管理，这一观点会被越来越多的人们所接受。单纯的技术不能提供信息全面的安全保护，仅靠安全产品并不能完全解决信息的安全问题已逐渐成为共识。

在全社会普遍关注信息安全的情况下，各个企业或机构又都面临遵循保密标准与安全法规的要求，越来越多的经理人和董事会或领导层也逐渐认识到自己在信息安全管理中所必须担负的责任和义务。同时，有关信息安全标准、法律和法规的数量正在迅速增加，许多机构都面临遵守各种安全标准和法规的要求。随着越来越多的标准、法律和法规的出台，统一安全标准的需求自然成为一个很现实的问题。

信息安全管理国际标准的发展过程

1992 年，世界经济合作与发展组织（oecd）发表了《信息系统安全指南》,旨在帮助成员和非成员的政府和企业组织增强信息系统的风险意识，提供一般性的安全知识框架。美国、oecd 的其他 23 个成员，以及十几个非 oecd 成员都批准了这一指南。

该指南旨在提高信息系统风险意识和安全措施，提供一个一般性的框架以辅助针对信息系统安全的有效的度量方法、实践和程序的制定和实施，鼓励关心信息系统安全的公共和私有部门间的合作。促进人们对信息系统的信心，促进人们应用和使用信息系统，方便国家间和国际间信息系统的开发、使用和安全防护。这个框架包括法律、行动准则、技术评估、管理和用户实践，及公众教育/宣传活动。该指南的最终目的是作为政府、公众和私有部门的信息安全管理的基准，相关机构能通过此基准来衡量本身在信息安全管理方面的进展。

国际会计师联合会于 1998 年也发表了一个有关《信息安全管理》的文件，认为信息系统安全的目标有三个：可用性，即确保信息系统在需要的时候可用；保密性，即对数据信息的访问控制设计完备的策略；完整性，即保证数据信息不受未经授权的修改。

1993 年 1 月，英国标准协会（britishstandardsinstitution,简称 bsi）成立了信息安全的行业工作小组。1993 年 9 月，信息安全管理体系实施要则出版。1995 年 2 月，英国标准协会制定的信息安全管理体系标准 bs7799-1 出版。1998 年 2 月，bs7799-2 出版。bs7799 对信息安全的控制范围、安全准则、安全管理等要素做出了规范性的表述。2002 年 9 月：bs7799-2:2002 出版。

iso(国际标准化组织)和 iec(国际电工委员会)是世界

范围的标准化组织。各国的相关标准化组织都是其成员，并通过各种技术委员会参与相关标准的制定。其他国际组织，政府机构及非政府机构也协同工作。国际标准的草案，需能得到所有会员 75%以上的赞成票，该标准才可被公布为国际标准。在信息技术领域，iso 和 iec 成立了一个联合技术委员会 iso/iecjtc1。该委员会以英国标准协会制定的信息安全标准 bs7799 为蓝本，并对 bs7799-1 做了 23 处修改后，制定了信息安全的国际标准 iso/iec 17799 草案。该草案在联合技术委员会 iso/iecjtc1 的安排下，通过一个特殊的“快速通道”（fast-trackprocedure），并行地得到了 iso 和 iec 成员国的批准。2000 年 12 月，国际标准 iso/iec17799 出版。iso/iec17799 第二部分 2000 年 9 月公布。同年，iso/iec17799 工具箱出版。

iso/iec17799 的体系介绍

iso/iec17799 是由国际标准化组织（iso）颁布的一套全面和复杂的信息安全管理标准，旨在帮助各种类型和规模的组织实施并运行有效的信息安全管理体系，从而增强企业识别、防止、减少和控制组织信息安全风险的能力。

iso/iec17799 标准是由两部分构成的。第一部分是信息安全管理体系的实施指南，相当于 bs7799-1;第二部分是信息安全管理体系规范，相当于 bs7799-2。iso/iec17799 标准的内容涉及 10 个领域，36 个管理目标和 127 个控制措施。10 个领域分别为：

*信息安全政策：信息安全政策为信息安全提供管理方向和指南。同时管理层应制定一套清晰的指导原则，并以此明确表明其对信息安全及在单位内部贯彻实施信息安全政策的支持和承诺。

*安全组织：应建立适当的信息安全管理部门对信息安全政策进行审批，对安全权责进行分配，并协调单位内部安全的实施。如有必要，在单位内部设立特别信息安全顾问并指定相应人选。同时，要设立外部安全顾问，以便跟踪行业走向，监视安全标准和评估手段，并在发生安全事故时建立恰当的联络渠道。在此方面，应鼓励跨学科的信息安全安排，比如，在经理人、用户、程序管理员、应用软件设计师、审计人员和保安人员间开展合作和协调。同时对第三方接触本单位的信息处理设备要进行管制。

*资产分类与管理：所有重大的信息资产都要有记录和主管人员。对资产的负责制度将确保对其进行有效的保护。指定的主管人员要有在此方面的主要职责和管理办法。实施管理的任务可委托给他人，但最后的责任要由资产的主管人员承担，以确保信息资产得到分类和适当水平的保护。

*个人信息安全守则：个人信息安全的权责应当在对员工聘用的阶段就开始实施，还应包括在合同中，并在以后员工的聘用期内时时进行监督。对潜在的待聘员工应加以仔细充分的筛选，特别是从事敏感工作的员工。所有使用信息处理设备的员工或第三方都要签署保密或不泄密协议和岗位职责中的安全责任，以减少人为风险。

*设备及使用环境的信息安全管理：保护信息系统基础设施、设备、媒体免受非法的访问、或自然灾害和环境危害。其目的是保护企业所在地及信息免于未经授权的存取、破坏及入侵。关键或敏感的商业信息处理设备应放置在安全的区域，由安全防御带、适当的安全屏障和准入管制手段加以保护，以防它们物理上被非法进入、