# 网络嗅探及反嗅探的原理及实现

何　焱
(遵义卫生学校 信息中心　贵州 遵义　563002)

**摘　要**: 首先简单地介绍了网络嗅探的原理及其潜在的安全隐患, 然后给出了检测网络中是否有嗅探器嗅探的方法, 最后根据不同的网络安全需求, 提出了几种切实可行、有效消除网络嗅探的方案。

**关键词**: 网络安全; 网络嗅探; SSH; 网络分割
**中图分类号**: TP393108　　**文献标识码**: B　　**文章编号**: 1004-373X (2003) 11-027-02

## Principle and Implementation of Network Sniffer and Antisniffer

HE Yan
(Information Center, the Health School of Zunyi, Zunyi, 563002, China)

**Abstract**: Disscusses the principle of sniffer and it's security risks, then some tips to detect sniffers on the Ethernet are introduced1 Finally, we present solutions of cleaning up the security risks come from sniffer1

**Keywords**: network security; netword sniffer; SSH; compartmentalization

随着 Internet 在教育、科技、医疗、军事等各个领域的普及, 人们对网络的依赖越来越多, 网络通信的安全问题也就显得越来越重要。嗅探器是网络黑客(Cracker) 经常采用、有效的工具之一。所谓嗅探器, 是指在运行以太网协议、TCPöIP 协议、IPX 协议或者其他协议的网络上, 可以攫取网络信息流的软件或硬件。嗅探器不同于一般的键捕获工具, 后者只能捕获当地终端控制台上的按键内容, 而嗅探器所“嗅”到的是动态的以信息包形式 (如 IP 数据包或者以太网包) 封装的信息流　其中可能携带了重要数据或敏感信息。嗅探器可以捕获这些信息包并存档, 利用相应工具可以作进一步分析。

## 1　网络嗅探的原理

嗅探的原理其实很简单。他是一种数据链路层的技术, 利用的是共享式的网络传输介质。共享即意味着网络中的一台机器可以嗅探到传递给本网段 (冲突域) 中的所有机器的报文。例如最常见的以太网就是一种共享式的网络技术, 以太网卡收到报文后, 通过对目的地址进行检查, 来判断是否是传递结自己的, 如果是, 则把报文传递给操作系统; 否则, 将报文丢弃, 不进行处理; 网卡存在一种特殊的工作模式, 在这种工作模式下, 网卡不对目的地址进行判断, 而直接将他收到的所有报文都传递给操作系统进行处理。这种特殊的工作模式, 就称之为混杂模式; 网络嗅探器通过将网卡设置为混杂模式, 并利用数据链路访问技术来实现对网络的嗅探。实现了数据链路层的访问, 我们就可以把嗅探能力扩展到任意类型的数据链路帧, 而不光是 IP 数据报。例如 Tcpdump, Netxray 就是直接访问数据链路层的常用程序。

## 2　嗅探器与网络安全

一些网络诊断工具也属于嗅探器的范畴 (如Unix 的 Traceroute 命令, 可以诊断路由), 也有一些公司专门生产各种各样的嗅探器, 用来诊断网络。但是真正的嗅探器可以检查更低层次传输的信息包。其区别在于: 工具的用途是合法的。嗅探器是由网络人员在不考虑网络安全的情况下开发出来的, 网络黑客可能会用他来做一些危及网络安全的事。嗅探器对网络安全具有很大威胁。一般来说, 因为网络信息流量很大, 存储资源往往显得不足, 所以网络黑客喜欢用嗅探器只捕获每个信息包的前 200～300 B。通常这里面包含用户 ID 和口令, 有了用户的 ID 和口令后, 网络黑客能很容易地进行下一步的入侵, 令网络管理员防不胜防。如果某网络被未经授权者设置了嗅探器, 那么该网络的安全实际上已遭到严重破坏, 特别是 LAN 接入 Internet 的情况下, 被外来者设置了嗅探器将是很糟糕的事情。任何主机通过 FTP, TELNET 或者

收稿日期: 2003-03-17

RLOGIN 等方式联到有嗅探器的系统, 都将有被截获口令的危险。网络安全分析也表明, 嗅探器是网络安全的第二大隐患。

## 3　嗅探器的检测

如前所述, 嗅探器可能带来很严重的安全问题, 因此, 检测网络是否存在嗅探器, 对网络管理员或网络安全管理员来讲, 就变得非常重要。然而, 嗅探器非常难以被发现, 因为他们是被动的程序, 他们并不会留下让别人审核的尾巴。由于嗅探器将网卡设为混杂模式, 而一般正常服务的网卡都不处在该模式下, 因此, 检测嗅探器就等同于检测网络是否存在网卡设为混杂模式的计算机。旧的 Linux 核心可以通过以下特性检测出该机器是否处在混杂模式下: 在正常模式下, 网卡过滤和丢弃那些 MAC 地址不是广播地址并且不是该网卡 MAC 地址的数据包: 如果发送非法目的 MAC 地址 (例如可以是 66: 66: 66: 66: 66: 66) 的数据帧, 而数据帧的数据是一个合法 IP 地址的数据包 (例如 ICMP 数据包), 如果网卡处在正常模式下, 将丢弃该数据帧: 但是如果网卡处在混杂模式下, 网卡会将该数据帧提交给相应的协议栈、系统将对该数据包作出相应的响应, 如果能够检测到该机器发回了响应数据包, 即证明该机器是一个嗅探器。Windows 95ö98ö NT, 操作系统如果处在混杂模式下时, 可以很容易检测出。在正常模式 (非混杂模式) 下, 网卡只将目标地址为自己或是以太网广播地址 (FF: FF: FF: FF: FF: FF) 传递给内核; 当处在混杂模式下时, 驱动程序只检测以太网地址的第一个字节是否是广播地址, 如果是 FF, 则是广播包。可以利用发送目标以太网地址为 FF: 00: 00: 00: 00: 00, 而目标 IP 地址是正常的数据帧, 当微软操作系统的驱动程序收到该数据帧时, 如果处在混杂模式下, 将对该数据帧做出响应, 如果没处在混杂模式下, 将丢弃该数据帧 (注意: 这依赖于驱动程序, 微软的默认驱动程序有这种特性)。还可利用 DNS 测试和网络机器延迟测试来检测某台机器是否处在混杂模式下。

## 4　消除网络监听所应采取的措施

消除嗅探器并不是一件很困难的事情, 一般都根据所传输数据的重要性、安全性以及所需的花费来决定采用什么措施。通常采取加密和网络分割的办法来防止嗅探器的攻击。

### 411　加　密

如果仅仅需要防止远程登录时用户 ID 和口令被截取, 可以在主机上安装一次性口令系统 (OTP)。在使用 OTP 的系统中, 用户在登录时根据主机提出的一个迭代值和一个种子值计算出本次登录的口令。如果需要保护电子邮件免遭窃取, 可以对邮件使用 PGP 加密。PGP 采用 RSA 和 IDEA 混合的加密算法, 对该算法目前还没有找到比穷尽算法更有效的破解办法。上面提到的这两种办法实现较简单, 但是他们也不能完全阻止一个野蛮的监听者对网络上种种信息包的获取。SNP 提供了一种安全的验证协议, TELNET, FTP, RLOGIN 等应用的用户 ID 和口令不再是以文本方式传输。SNP 系统所有传输数据是采用 DES 加密的、监听者所看到的信息包只是一些乱码。目前 SNP 系统可以运行在很多操作系统上。SSH 提供端到端的验证与加密, 他也是应用层的安全通信协议, 是目前国际互联网上最好的安全通信工具之一。SSH 是基于 CöS 模型的, 标准的 SSH 服务端口为 22。SSH 采用 RSA 加密算法建立连接, 验证过程结束后, 所有的信息都采用 IDEA 技术加密, 他是典型的强加密, 适合于所有的通信。SSH 曾一度为加密安全通信的主要协议。如果在网络系统中使用 SSH, 那么用户 ID 和口令被捕获的概率将大大降低。对于 SSH 有商业的和免费的版本, 免费的版本是 UNIX 上的工具, 商用的是用在 Windows 311ö95öNT 上的。目前 SSH 和 SNP 的应用仍然不广泛, 问题主要在于易用性不好, 大多数用户也不愿意去接受新的应用软件。另外, 强加密算法会或多或少地增大系统的负荷。

### 412　网络分割

通常人们所能接受的防止嗅探器攻击的办法是使用安全的网络拓扑结构, 但是这种方法实现很麻烦, 花费也比较大。我们知道, 广播一般只存在于同一根网络总线上, 所以信息包只能被同一网络块 (或网络段) 的嗅探器所捕获。我们可以利用网络分割的技术, 使得网络进一步划分, 减小嗅探器的监听范围, 这样网络的其余部分就免受了嗅探器的攻击。一般可以采用 Switch 划分网段, 使用网桥或者网络路由器来划分子网。实际上旧的 PC 和工作站都可以配置成网桥或者路由器。当然一个网络块应该是由那些互相可以信任的计算机组成。典型的情况是这些计算机在同一房间或者同一办公室。网络分割有很多优点。一名不道德的雇员安装了嗅探器, 由于受到物理限制, 他仅仅能够捕获合作伙伴的工作站的信息流。如果发现了在某一分支有嗅探器, 那么很容易确定是那些人所设置。网络分割要解决的问题是确立信任关系, 只有在此基础上才能设计网络拓扑。(下转第 32 页)

作为远程教学用的课件, 网页有允许实验者将实验虚拟环境所需的汇编程序下载到本地硬盘使用的超链接, 在网页中采用分层的动态技术, 包括层面的变化及移动。网页中的图片、表格以及文字说明将与网页中暂时无关的内容相重叠, 使网页简洁美观调用方便。

冒泡排序法的动态交互演示实验在 html 文件 < body> 内插入一段精巧的 Javascript 程序, 用变量数组跟踪实验者输入的数据, 显示在相应的程序段及内存中, 模拟冒泡排序的算法进行比较, 并把结果显示在对应的寄存器和内存单元中, 同时, 显示地址指针的位置及调用动画箭头指向所换的单元, 增强了演示实验的交互性并把程序对计算机深层的影响直观的呈现出来。

## 4 课件运行方式和运行环境

本课件设计制作完成后可不打包使用, 即在 Authorware 610 环境下运行, 这样可以随时对课件进行修改、调试和完善; 也可以将课件打包成可执行 (1EXE) 文件, 在不安装 Authorware 的 Windows 9xö2000öNT 操作系统下运行, 可避免使用时的误操作; 还可利用 Authorware 610 先进的一键发布及预览功能, 将课件发布成 1aam 格式, 在 WebPlayer 的支持下自动生成 1htm 文件, 便于联网用户 IE 浏览。

打包为可执行的 (1EXE) 文件, 运行环境要求如下: 586 以上多媒体机型、32MB 以上内存、Windows 9Xö2000öNT 操作系统、颜色 256 色以上 (最好是 16 位增强色或 24 位真彩色)。

推荐配置: 主频 PII 233 以上、显存 4MB 以上、光驱 32 倍速以上、声卡、鼠标。

## 5 结 语

本 CAI 课件内容包括微机原理实验及相关知识, 既可作为学生自学课件也可作为远程教学使用, 可适于不同层次学生学习的需要, 加强了实验效果, 增强了实验的真实感。可仿真微机原理实验硬件环境, 提供芯片图形供使用者连线形成硬件连接图, 并提供汇编语言的编辑、编译、链接、调试程序, 使实验者感觉在真实环境下做实验。课件广泛使用各种类型的交互: 热区、按钮、目标区域、双热区等响应, 动态链接实验内容及帮助信息, 捕捉实验者的每一步动作, 实时给出提示或结果。运用大量的图片、动画使信息直观、易于接受。此外, 虚拟实验的方式有效解决了实验设备不足的问题, 而且使实验场所得到了无限的扩展, 提高了实验质量。由于课件的设计过程贯彻了实验设计的原理与方法, 使得课件的设计更加科学化。软硬结合的实验环境和教学手段的设计, 作为一种新型的课件设计思想, 取得了良好的效果。目前, 课件仍在改进, 使之更加灵活、易用。

## 参 考 文 献

[1] 王炳谦 1 微机原理与接口技术实验指导书 (动力系专用) [M] 1 保定: 华北电力大学出版社, 19991

[2] 傅德荣 1CAI 课件设计的原理与方法 [M] 1 北京: 高等教育出版社, 19941

[3] 於志渊 1 动态 Web 网页技术大全 [M] 1 北京: 清华大学出版社, 20001

[4] 黄兴中 1Authorware 入门与提高 [M] 1 北京: 清华大学出版社, 19971

作者简介 姚万业 男, 华北电力大学动力工程系教师, 副教授。

(上接第 28 页)

根据以上介绍的两种方法, 我们便可以挫败嗅探器了。

## 参 考 文 献

[1] Stephen Northcutt1 网络入侵检测分析员手册 [M] 1 余青霓, 等译 1 北京: 人民邮电出版社, 20001

[2] Rebecca Gunley Bace1 入侵检测 [M] 1 陈明奇, 等译 1 北京: 人民邮电出版社, 20011

[3] 胡昌振, 等 1 面向 21 世纪网络安全与防护 [M] 1 北京: 希望电子出版社, 19971

[4] 姚冒群 1 网络攻击的分析及防范策略 [J] 1 计算机应用研究, 1999, (12): 34-351

作者简介 何 焱 女, 1975 年出生, 讲师, 在读研究生。研究方向为网络安全。