浅析计算机网络安全技术

--辽宁思凯科技股份有限公司　　李硕　李晓明

[摘要]：随着计算机网络越来越深入到人们生活中的各个方面，计算机网络的安全性也就变得越来越重要。计算机网络的技术发展相当迅速，攻击手段层出不穷。而计算机网络攻击一旦成功，就会使网络上成千上万的计算机处于瘫痪状态，从而给计算机用户造成巨大的损失。因此，认真研究当今计算机网络存在的安全问题，提高计算机网络安全防范意识是非常紧迫和必要的。

[关键词]：安全问题；相关技术；对策

虽然计算机网络给人们带来了巨大的便利，但由于计算机网络具有联结形式多样性、终端分布不均匀性和网络的开放性、互连性等特征，致使网络易受黑客、恶意软件和其他不轨的攻击，所以网上信息的安全和保密是一个至关重要的问题。加强网络安全建设，是关系到企业整体形象和利益的大问题。目前在各企业的网络中都存储着大量的信息资料，许多方面的工作也越来越依赖网络，一旦网络安全方面出现问题，造成信息的丢失或不能及时流通，或者被篡改、增删、破坏或窃用，都将带来难以弥补的巨大损失。而对于政府等许多单位来讲，加强网络安全建设的意义甚至关系到国家的安全、利益和发展。

一、几种计算机网络安全问题

1、 TCP/IP 协议的安全问题。目前网络环境中广泛采用的 TCP/IP 协议。互联网技术屏蔽了底层网络硬件细节，使得异种网络之间可以互相通信，正因为其开放性，TCP/IP 协议本身就意味着一种安全风险。由于大量重要的应用程序都以 TCP 作为它们的传输层协议，因此 TCP 的安全性问题会给网络带来严重的后果。

2、 网络结构的安全问题。互联网是一种网间网技术。它是由无数个局域网连成的巨大网络组成。当人们用一台主机和另一局域网的主机进行通信时，通常情况下它们之间互相传送的数据流要经过很多机器的重重转发，任何两个节点之间的通信数据包，不仅为这两个节点的网卡所接收，也同时为处在同一以太网上的任何一个节点的网卡所截取。因此，黑客只要接入以太网上的任一节点进行侦测，就可以捕获发生在这个以太网上的所有数据包，对其进行解包分析，从而窃取关键信息。加之互联网上大多数数据流都没有进行加密，因此黑客利用工具很容易对网上的电子邮件、口令和传输的文件进行破解，这就是互联网所固有的

安全隐患。

3、 路由器等网络设备的安全问题。路由器的主要功能是数据通道功能和控制功能。路由器作为内部网络与外部网络之间通信的关键设备，严格说来，所有的网络攻击都要经过路由器，但有些典型的攻击方式就是利用路由器本身的设计缺陷展开的，而有些方式干脆就是在路由器上进行的。

二、计算机网络安全的相关技术

计算机网络安全的实现有赖于各种网络安全技术。从技术上来说，网络安全由安全的操作系统、安全的应用系统、防病毒、防火墙、入侵检测、网络监控、信息审计、通信加密、灾难恢复、安全扫描等多个安全组件组成，一个单独的组件无法确保信息网络的安全性。目前成熟的网络安全技术主要有：防火墙技术、数据加密技术、入侵检测技术、防病毒技术等。

1、 防火墙技术。所谓“防火墙”则是综合采用适当技术在被保护网络周边建立的用于分隔被保护网络与外部网络的系统。“防火墙”一方面阻止外界对内部网络资源的非法访问，另一方面也可以防止系统内部对外部系统的不安全访问。实现防火墙的主要技术有：数据包过滤、应用级网关、代理服务和地址转换。

2、 数据加密技术。从密码体制方面而言，加密技术可分为对称密钥密码体制和非对称密钥密码体制，对称密钥密码技术要求加密、解密双方拥有相同的密钥，由于加密和解密使用同样的密钥，所以加密方和解密方需要进行会话密钥的密钥交换。会话密钥的密钥交换通常采用数字信封方式，即将会话密钥用解密方的公钥加密传给解密方，解密方再用自己的私钥将会话密钥还原。对称密钥密码技术的应用在于数据加密非对称密钥密码技术是加密、解密双方拥有不同的密钥，在不知道特定信息的情况下，加密密钥和解密密钥在计算机上是不能相互算出的。加密、解密双方各只有一对私钥和公钥。非对称密钥密码技术的应用比较广泛，可以进行数据加密、身份鉴别、访问控制、数字签名、数据完整性验证、版权保护等。

3、 入侵检测技术。入侵检测系统可以分为两类，分别基于网络和基于主机。基于网络的入侵检测系统主要采用被动方法收集网络上的数据。目前，在实际环境中应用较多的是基于主机的入侵检测系统，它把监测器以软件模块的形式直接安插在了受管服务器的内部，它除了继续保持基于网络的入侵检测系统的功能和优点外，可以不受网络协议、速率和加密的影响，直接针对主机和内部的信息系统，同时还具有基于网络的入侵检测系统所不具备的检查特洛伊木马、监视特定用户、监视与误操作相关的行为变化等功能。

4、 防病毒技术。随着计算机技术的不断发展，计算机病毒变得越来越复杂和高级，其扩散速度也越来越快，对计算机网络系统构成极大的威胁。在病毒防范中普遍使用的防病

毒软件，从功能上可以分为网络防病毒软件和单机防病毒软件两大类。单机防病毒软件一般安装在单台 PC 上，它们主要注重于所谓的“单机防病毒”，即对本地和本工作站连接的远程资源采用分析扫描的方式检测、清除病毒。网络防病毒软件则主要注重网络防病毒，一旦病毒入侵网络或者从网络向其它资源感染，网络防病毒软件会立刻检测到并加以删除。

三、建议采取的几种安全对策

1、 网络分段。网络分段通常被认为是控制网络广播风暴的一种基本手段，但其实也是保证网络安全的一项重要措施。其目的就是将非法用户与敏感的网络资源相互隔离，从而防止可能的非法侦听。

2、 以交换式集线器。代替共享式集线器对局域网的中心交换机进行网络分段后，以太网侦听的危险仍然存在。这是因为网络最终用户的接入往往是通过分支集线器而不是中心交换机，而使用最广泛的分支集线器通常是共享式集线器。这样，当用户与主机进行数据通信时，两台机器之间的数据包还是会被同一台集线器上的其他用户所侦听，所以应该以交换式集线器代替共享式集线器，使单播包仅在两个节点之间传送，从而防止非法侦听。

3、 VLAN 的划分。为了克服以太网的广播问题，除了上述方法外，还可以运用 VLAN 技术，将以太网通信变为点到点通信，防止大部分基于网络侦听的入侵。在集中式网络环境下，通常将中心的所有主机系统集中到一个 VLAN 里，在这个 VLAN 里不允许有任何用户节点，从而较好地保护敏感的主机资源。在分布式网络环境下，可以按机构或部门的设置来划分 VLAN。各部门内部的所有服务器和用户节点都在各自的 VLAN 内，互不侵扰。VLAN 内部的连接采用交换实现，而 VLAN 与 VLAN 之间的连接则采用路由实现。当然，计算机网络安全不是仅有很好的网络安全设计方案就万事大吉，还必须要有很好的网络安全的组织结构和管理制度来保证。要通过组建完整的安全保密管理组织机构，制定严格的安全制度，指定安全管理人员，随时对整个计算机系统进行严格的监控和管理。

参考文献

[1]王达.网管员必读———网络安全[M].北京：电子工业出版社,2007.

[2]张敏波.网络安全实战详解[M].北京：电子工业出版社,2008.

[3]谢希仁.计算机网络（第 5 版）[M].北京：电子工业出版社,2008.