# 计算机网络安全与对策*

李 辉
(潍坊学院, 山东 潍坊 261061)

**摘 要**: 网络已经成为信息社会的基础设施, 是进行信息交流的基本工具。而网络上信息的安全和保密是网络得以发展的重要保障。文章论述了影响计算机网络系统安全的几种因素和加强计算机网络 系统安全管理的对策建议。

**关键词**: 计算机网络; 安全性; 对策建议
**中图分类号**: TP393. 08 **文献标识码**: A **文章编号**: 1671-4288( 2007) 02-0054-02

随着计算机网络技术的飞速发展和应用的广泛深入, 网络已经成为信息社会的基础设施, 是进行信息交流的基本工具, 各高校也纷纷将原先的单机机房, 改建成网络机房, 解决教师和学生的网络课教学及上网需要, 以充分利用现有的计算机资源, 而网络上信息的安全和保密是网络得以发展的重要保障, 了解网络中存在的不安全因素, 掌握网络安全的防范措施已成为当务之急。

## 1 影响计算机网络系统安全的因素

计算机网络的安全性, 是一个系统的概念, 是由数据运行的安全性、通信的安全性和管理人员的安全意识三部分组成。任何一方面出现问题都将影响整个网络系统的正常运行。

1. 1 计算机网络软、硬件技术的不完善 由于人类认识能力和技术发展的局限性, 在设计硬件和软件的过程中, 难免会留下种种技术缺陷, 由此造成信息安全隐患, 如 Internet 作为全球使用范围最广的信息网, 自身协议的开放性虽极大地方便了各种计算机入网, 拓宽了共享资源。但 TCP/ IP 协议在开始制定时没有考虑通信路径的安全性, 缺乏通信协议的基本安全机制, 没有加密、身份认证等功能; 在发送信息时常包含源地址、目标地址和端口号等信息。由此导致了网络上的远程用户读写系统文件、执行根和非根拥有的文件通过网络进行传送时产生了安全漏洞。

1. 2 计算机病毒的影响 计算机病毒利用网络作为自己繁殖和传播的载体及工具, 造成的危害越来越大。Internet 带来的安全威胁来自文件下载及电子邮件, 邮件病毒凭借其危害性强、变形种类繁多、传播速度快、可跨平台发作、影响范围广等特点, 利用用户的通讯簿散发病毒, 通过用户文件泄密信息, 邮件病毒已成为目前病毒防治的重中之重。

1. 3 计算机网络存在着系统内部的安全威胁 计算机网络系统内部的安全威胁包括以下几个方面: ① 计算机系统及通信线路的脆弱性。系统软硬件设计、配置及使用不当。! 人为因素造成的安全泄漏, 如网络机房的管理人员不慎将操作口令泄漏, 有意或无意地泄密、更改网络配置和记录信息, 磁盘上的机密文件被人利用, 临时文件未及时删除而被窃取。

1. 4 物理电磁辐射引起的信息泄漏 计算机附属电子设备在工作时能经过地线、电源线、信号线将电磁信号或谐波等辐射出去, 产生电磁辐射。电磁辐射物能够破坏网络中传输的数据, 这种辐射的来源主要有两个方面: ① 网络周围电子设备产生的电磁辐射和试图破坏数据传输而预谋的干扰辐射源。 网络的终端、打印机或其他电子设备在工作时产生的电磁辐射泄漏, 这些电磁信号在近处或者远处都可以被接收下来, 经过提取处 理, 重新恢复出原信息, 造成信息泄漏。

1. 5 缺少严格的网络安全管理制度 网络内部的安全需要用完备的安全制度来保

* 收稿日期: 2006 # 04 # 13
作者简介: 李辉( 1978- ) , 女, 山东潍坊人, 潍坊学院实验室与设备管理处助教。

障, 管理的失败是网络系统安全体系失败的非常重要的原因。网络管理员配置不当或者网络应用升级不及时造成的安全漏洞、使用脆弱的用户口令、随意使用普通网络站点下载的软件、在防火墙内部架设拨号服务器却没有对账号认证等严格限制、用户安全意识不强、将自己的账号随意转借他人或与别人共享等,都会使网络处于危险之中。

## 2 加强计算机网络系统安全管理的对策建议

面对网络安全的脆弱性,应切实加强计算机网络的安全管理,网络安全是对付威胁、克服脆弱性、保护网络资源的所有措施的总和,涉及政策、法律、管理、教育和技术等方面的内容。网络安全是一项系统工程, 针对来自不同方面的安全威胁,需要采取不同的安全对策。

2 2　计算机网络系统的物理安全管理　计算机网络系统物理安全管理的目的是保护

路由器、交换机工作站、网络服务器、打印机等硬件实体和通信线路免受自然灾害、人为破坏和搭线窃听攻击,确保网络设备有一个良好的电磁兼容工作环境。抑制和防止电磁泄漏是物理安全的一个主要问题。

2 1. 1　对传导发射的防护　主要采取对电源线和信号线加装性能良好的

滤波器, 减小传输阻抗和导线值的交叉藕合。

2 1. 2　对辐射的防护

这类防护措施分为两种: 一是采用各种电磁屏蔽措施,如对设备的金属屏蔽和各种接插件的屏蔽,同时对网络机房的下水管、暖气管和金属门窗进行屏蔽和隔离; 二是干扰的防护措施,即在计算机系统工作的同时,利用干扰装置产生一种与计算机系统辐射相关的伪噪声向空间辐射来掩盖计算机系统的工作频率和信息特征。

2 2　计算机网络系统的访问控制策略　访问控制是网络安全防范和保护的主要策

略,它的主要任务是保证网络资源不被非法使用和非常访问。

2 2 1　入网访问控制　它为网络访问提供了第一层访问控制,它控

制哪些用户能够登录到服务器并获取网络资源,控制准许用户入网的时间和准许他们在哪台工作站入网。

2 2 2　网络的权限控制　它是针对网络非法操作所提出的一种安全保

护措施。用户和用户组被赋予一定的权限, 网络控制用户和用户组可以访问哪些目录、子目录、文件和其他资源, 可以指定用户对这些文件、目录、设备能够执行哪些操作。

2 2 3　网络服务器安全控制　包括可以设置口令锁定服务器控制台,以防

止非法用户修改。删除重要信息或破坏数据; 可以设定服务器登录时间限制、非法访问者检测和关闭的时间间隔。

2 2 4　属性安全控制　它能控制以下几个方面的权限:　向某个文件

写数据、拷贝一个文件、删除目录或文件、查看目录和文件、执行文件、隐含文件、共享、系统属性等。网络的属性可以保护重要的目录和文件,防止用户对目录和文件的误删除、执行修改、显示等。

2 3　防火墙技术　防火墙技术是建立在现代通信网络技术和信

息安全技术基础上的应用性安全技术,是在两个网络之间实行控制策略的系统,通常安装在单独的计算机上,与网络的其余部分隔开,它使内部网络与 Int ernet 之间或与其他外部网络互相隔离,限制网络互访,用来保护内部网络资源免遭非法使用者的侵人,执行安全管制措施,记录所有可疑事件。利用防火墙技术,经过仔细的配置,一般能够在内外网络之间提供安全的网络保护,降低网络安全的风险。目前使用的防火墙产品可分为两种类型:包过滤型和应用网关型。

2 4　数据加密技术　数据加密技术是保障信息安全的最基本最核

心的技术措施和理论基础, 由加密算法来具体实施。由于数据在传输过程中有可能遭到侵犯者的窃听而失去保密信息,如当一个企业在传送涉及到自己的商业秘密的数据时,一定要用密文传送,也就是利用技术手段 把重要的数据 变为乱码传送, 到达目的地后再用相同或不同的手段还原。

2 5　鉴别技术

鉴别技术主要是在信息交流过程中防止信息被非法伪造、篡改和假冒的一种技术。如果黑客进人了计算机系统,发布虚假信息或更改真实的信息,通过鉴别技术即可做出判断。

2 5 1　报文鉴别

是指在两个通信者之间建立 (下转第 42 页)

包括自动化立体仓库软件包、生产线监测系统软件包、同步控制算法软件模块、张力控制算法软件模块、船闸控制系统软件包、船闸船只最优调度算法软件等等。

## 2 基于现场总线的先进控制系统市场前景分析

### 2.1 市场需求

目前, 国内各行业竞争激烈。企业逐步认识到只有不断引人新技术才能使企业得到持续稳定地发展。企业有追求新技术、改造现有系统的需求。现场总线技术是未来自动化技术发展的主流, 基于现场总线的先进控制系统以其明显的技术优势和价格优势, 在分布式控制系统市场中将逐步替代 PLC 产品。

### 2.2 企业效益

2.2.1 对现场设备制造商 参与基于现场总线的先进控制系统开发的现场设备制造商将本企业传统产品提高了一个技术水平。由于现场总线技术的开放性, 企业开发的现场总线产品可以集成到任何现场总线控制系统中。

2.2.2 对自动化系统集成商 应用现场总线的先进控制系统的自动化系统集成商有条件以系统为平台,利用自身在行业领域中的优势,开发出具有专用技术的控制系统,使系统集成增值, 增加利润并扩大市场份额。

## 结束语

现场总线技术以其标准化、开放性使参与其中的企业收益; 国内企业应吸取在 PLC、DCS 技术和产业化方面发展的经验教训, 把握机遇, 结成技术及市场同盟, 开发出拥有自主知识产权、基于现场总线技术的控制系统, 并在优势行业上应用推广。

# Advanced Control System Based on Fieldbus

HAN Xing-hai

*(Weifang University, Weifang 261061, China)*

Abstract: This paper use Fieldbus for background, describe framework of Control System Based on Fieldbus, and analyse market forground of Control System.

Keywords: fieldbus, form, foreground

责任编辑: 肖恩忠

---

(上接第 55 页) 通信联系之后, 每个通信者对收到的信息进行检证, 以保证所收到的信息是真实的过程。

2.5.2 身份鉴别 主要指在网络系统对用户身份真实性的鉴别。

2.5.3 数字鉴别 信息接收和发送双方在收到和发出信息时的身份验证技术。可使信息发收双方不能根据各自利益互相修改签名后的文档和推卸责任, 当发生争执时可由第三方仲裁。

### 2.6 加强网络安全管理,逐步完善网络系统安全管理规章制度

对网络安全的脆弱性, 除了在网络设计上增加安全服务功能, 完善系统的安全保密措施外, 建立和实施严密的网络机房计算机安全管理制度与策略是真正实现网络安全的基础。只有把安全管理制度与安全管理技术手段结合起来, 整个网络的安全性才有保障。

责任编辑: 肖恩忠