计算机网络技术

授课教师：李 灿
联系方式：57862787
lic@jsnu.edu.cn
课程网站：sslic.cn/cnet
教 研 室：12#-407A（轨道交通系）

第10章 网络安全

本章内容

- 网络安全的基本概念
- 信息安全技术
- 防火墙技术
- 网络病毒

10.1 网络安全的基本概念

- 什么是网络安全？
- 网络安全主要解决的问题：
  - 数据保密
  - 认证

数据保密与认证

- **数据保密：**

  采取复杂多样的措施对数据加以保护，防止数据被有意或无意地泄露给无关人员

- **认证（信息认证和用户认证）**
  - 信息认证：信息从发送到接收整个通路中没有被第三者修改和伪造
  - 用户认证：是指用户双方都能证实对方是这次通信的合法用户
  - 通常在一个完备的保密系统中既要求信息认证，也要求用户认证

OSI/RM各层的网络安全措施

- 物理层
  - 可以在包容电缆的密封套中充入高压的氖气
- 链路层
  - 可以进行所谓的链路加密，即将每个帧编码后再发出，当到达另一端时再解码恢复出来
- 网络层
  - 可以使用防火墙技术过滤一部分有嫌疑的数据报
- 在传输层上甚至整个连接都可以被加密

10.1.1 网络安全：定义

- 网络安全：网络系统的硬件、软件及其系统中的数据受到保护，不受偶然的或者恶意的原因而遭到破坏、更改、泄露，系统连续可靠正常地运行，网络服务不中断。

① 运行系统安全，即保证信息处理和传输系统的安全

② 网络上系统信息的安全

③ 网络上信息传播的安全，即信息传播后果的安全

④ 网络上信息内容的安全，即我们讨论的狭义的“信息安全”

10.1.1 网络安全：特征

- **保密性**：

  信息不泄露给非授权的用户、实体或过程，或供其利用的特性

- **完整性**：

  数据未经授权不能进行改变的特性，即信息在存储或传输过程中保持不被修改、不被破坏和丢失的特性

- **可用性**：

  可被授权实体访问并按需求使用的特性，即当需要时应能存取所需的信息，网络环境下拒绝服务、破坏网络和有关系统的正常运行等都属于对可用性的攻击

- **可控性**：

  对信息的传播及内容具有控制能力

10.1.1 网络安全：主要威胁

- 非授权访问（Unauthorized Access）
  - 非授权用户的入侵
- 信息泄露（Disclosure of Information）
  - 将有价值的和高度机密的信息暴露给无权访问该信息的用户的所有问题
- 拒绝服务（Denial of Service）
  - 使系统难以或不可能继续执行任务的所有问题

10.1.1 网络安全：关键技术

- 主机安全技术
- 身份认证技术
- 访问控制技术
- 密码技术
- 防火墙技术
- 病毒防治技术
- 安全审计技术
- 安全管理技术

10.1.1 网络安全：分类

- 计算机安全分类

1）实体安全：包括机房、线路、主机等

2）网络安全：包括网络的畅通、准确以及网上信息的安全

3）应用安全：包括程序开发运行、I/O、数据库等的安全

- 网络安全分类

  - 基本安全类：访问控制、授权、认证、加密以及内容安全
  - 管理与记账类安全：安全策略的管理、实时监控、报警以及企业范围内的集中管理与记账
  - 网络互联设备：路由器、通信服务器、交换机等，网络互联设备安全正是针对上述这些互联设备而言的，它包括路由安全管理、远程访问服务器安全管理、通信服务器安全管理以及交换机安全管理等
  - 连接控制类：负载均衡、可靠性以及流量管理等

10.1.2 威胁网络安全的因素

安全威胁的类型

- 非授权访问
- 假冒合法用户
- 数据完整性受破坏
- 病毒
- 通信线路被窃听
- 干扰系统的正常运行，改变系统正常运行的方向，以及延时系统的响应时间

10.1.2 威胁网络安全的因素

- 计算机系统本身的弱点
  - 操作系统的创建进程机制
  - 远程过程调用（**RPC**）服务以及它所安排的无口令入口
  - 存在超级用户
  - 硬件或软件故障
  - 协议安全的脆弱性
  - 数据库管理系统安全的脆弱性

10.1.3 网络安全解决方案

- 一个完整的网络信息安全系统至少包括三类措施：

1. 社会的法律政策

   企业的规章制度及网络安全教育等外部环境

2. 技术方面的措施

   如防火墙技术、防病毒，信息加密、身份确认以及授权等

3. 审计与管理措施

   包括技术与社会措施

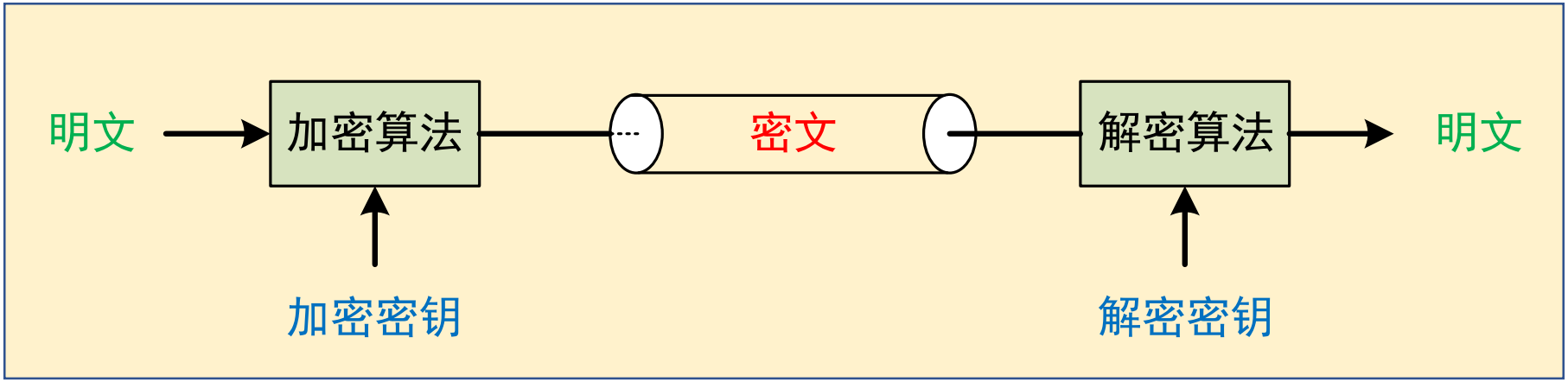
10.1.3 网络安全解决方案

- 网络安全系统提供安全的常用方法：
  - 用备份和镜像技术提高数据完整性
  - 病毒检查
  - 补丁程序，修补系统漏洞
  - 提高物理安全
  - 安装因特网防火墙
  - 废品处理守则
  - 仔细阅读日志
  - 加密
  - 执行身份鉴别，口令守则
  - 捕捉闯入者

10.2 信息安全技术

- 数据加密
- 用户认证
- 数字签名
- 加密技术应用案例

10.2.1 数据加密



1. 基本概念：网络入侵

- 消极入侵：

  入侵者只是窃听而已，并不对数据造成破坏

- 积极入侵：

  入侵者会截获密文，篡改数据甚至伪造假数据送入网中

1. 基本概念：密码分析和密码学

- 密码分析：

  破译密码的技术

- 密码学：

  设计密码和破译密码的技术

1. 基本概念：基本加密模型

- 密码学的一条基本原则：

  必须假定破译者知道通用的加密方法，即加密算法**E**是公开的

- 基本加密模型：

  加密算法公开且相对稳定，而作为参数的密钥是保密的，并且易于更换

1. 基本概念：密码分析问题分类

- 从破译者的角度来看，密码分析所面对的问题的变型：
  - 当仅有密文而无明文时，称为“只有密文”问题
  - 当已拥有了一批相匹配的明文和密文时，称为“已知明文”问题
  - 当能够加密自己所选的一些明文时，称为“选择明文”问题

1. 基本概念：安全的密码系统

- 一个密码系统仅能经得起“只有密文”的攻击还不能算是安全的，因为破译者完全可以从一般的通信规律中猜测出一部分的明文，从而就会拥用一些匹配的明文和密文，这对破译工作将大为有用
- 真正安全的密码系统应是，即使破译者能够加密任意数量的明文，也无法破译密文

2. 传统加密技术

替代密码

替代密码就用一组密文字母来代替一组明文字母以隐藏明文，但保持明文字母的位置不变

换位密码

换位有时也称为排列，它不对明文字母进行变换，只是将明文字母的次序进行重新排列

C	O	M	P	U	T	E	R	明文 pleaseexecutethelatestScheme
1	4	3	5	8	7	2	6	
p	l	e	a	s	e	e	x	
e	c	u	t	e	t	h	e	密文 PELHEHSCEUTMLCAEATEEXECDETTBSESA
l	a	t	e	s	t	s	c	
h	e	m	e	a	b	c	d	

2. 传统加密技术

秘密密钥算法

- 在传统加密算法的基础上，充分利用计算机的处理能力，将算法内部的变换过程设计的非常复杂，并使用较长的密钥，使得攻击者对密文的破译变得非常困难。
- 甚至，在攻击者即使掌握了加密算法的本身，也会由于不知道密钥而得不到明文。由于这种体制将算法和密钥进行了分离，并且算法的保密性完全依赖于密钥的安全性，因此，被称为秘密密钥加密体制。

3．现代加密技术

- 侧重于极为复杂的加密算法的设计

10.3 防火墙技术

10.3.1 基本概念

- 防火墙（Firewall）

  在两个网络之间执行访问控制策略的硬件或软件系统，目的是保护网络不被他人侵扰

  - 本质上，它遵循的是一种数据进行过滤的网络通信安全机制，只允许授权的通信，而禁止非授权的通信
  - 通常，防火墙就是位于内部网或Web站点与因特网之间的一台路由器或计算机

10.3.1 基本概念

- 部署防火墙的理由：
  - 防止入侵者干扰内部网络的正常运行
  - 防止入侵者删除或修改存储再内部网络中的信息
  - 防止入侵者偷窃内部的秘密信息
- 防火墙应具备的功能：
  - 所有进出网络的通信流都应该通过防火墙
  - 所有穿过防火墙的通信流都必须有安全策略和计划的确认和授权
  - 理论上说，防火墙是穿不透的

10.3.1 基本概念

- 内部网需要防范的三种攻击
  - 间谍：试图偷走敏感信息的黑客、入侵者和闯入者
  - 盗窃：盗窃对象包括数据、Web表格、磁盘空间和CPU资源等
  - 破坏系统：通过路由器或主机／服务器蓄意破坏文件系统或阻止授权用户访问内部网（外部网）和服务器

10.3.2 防火墙体系结构

1. 双重宿主主机体系结构
2. 主机过滤体系结构
3. 子网过滤体系结构
4. 堡垒主机的安全防护

10.3.3 防火墙类型

- 按软硬件形式：
  - 软件防火墙、硬件防火墙、芯片级防火墙
- 按防火墙技术：
  - 包过滤型、状态检测型、应用代理型
- 按防火墙结构：
  - 单一主机防火墙、路由器集成式防火墙、分布式防火墙
- 按防火墙的应用部署位置：
  - 边界防火墙、个人防火墙、混合防火墙
- 按防火墙性能：
  - 百兆级防火墙、千兆级防火墙

1. 包（分组）过滤型防火墙

- 包过滤（Packet Filtering）

  防火墙最基本的实现形式，它控制哪些数据包可以进出网络而哪些数据包应被网络拒绝

- 包过滤防火墙通常是放置在因特网与内部网络之间的一个具备包过滤功能的简单路由器，这是因为包过滤是路由器的固有属性

- 包过滤允许或阻止数据包通过路由器的依据：
  - 包的源地址及源端口
  - 包的目的地址及目的端口
  - 包的传送协议，如FTP、SMTP、rlogin等

1. 包过滤型防火墙：优缺点

- **优点**：
  - 简单、易于实现、对用户透明、路由器免费提供此功能
  - 仅用一个放置在内部网与因特网边界上的包过滤路由器就可保护整个内部网络
- **缺点**：
  - 编制逻辑上严密无漏洞的包过滤规则比较困难
  - 对编制好的或者复杂的规则进行测试维护也较麻烦
  - 包过滤规则的判别会降低路由器的转发速度
  - 对包中的应用数据无法过滤
  - 总假定包的头部信息合法有效
  - 以上这些缺点使得包过滤技术通常不单独使用，而是作为其他安全技术的一种补充

2. 状态监测型防火墙

- 采用动态设置包过滤规则的方法

  避免了静态包过滤所具有的问题

- 特点：

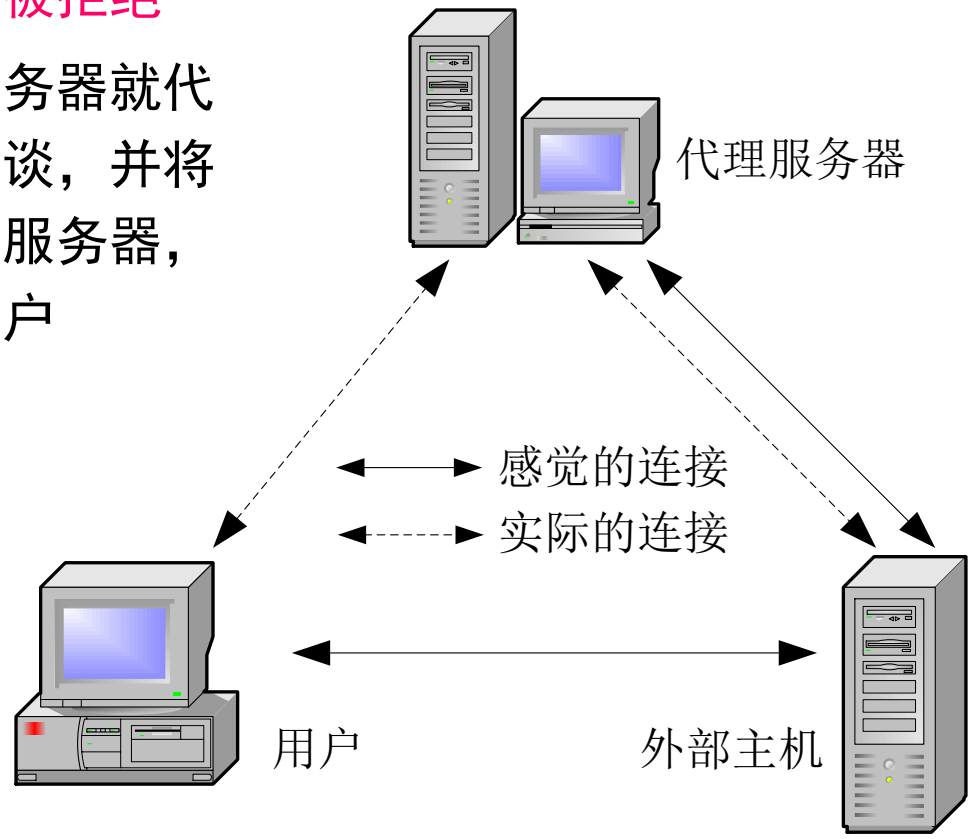
  对通过其建立的每一个连接都进行跟踪，并且根据需要可动态地在过滤规则中增加或更新条目

3. 应用代理型防火墙

- 应用代理型防火墙工作在OSI/RM的应用层
- 特点：
  完全“阻隔”了网络通信流，通过对每种应用服务编制专门的代理程序，实现监视和控制应用层通信流的作用
- 代理服务：
  指定一台有访问因特网能力的主机作为网络中客户端的代理，从而与因特网中的主机进行通信

3. 应用代理型防火墙

- **工作过程**：
  - 代理服务器判断从客户端来的请求并决定哪些请求允许传送而哪些应被拒绝
  - 当某个请求被允许时，代理服务器就代表客户与真正的服务器进行交谈，并将从客户端来的请求传送给真实服务器，将真实服务器的回答传送给客户



3. 应用代理型防火墙：优缺点

- 优点：
  - 安全
  - 避免了入侵者使用数据驱动类型的攻击方式入侵内部网
- 缺点：
  - 速度相对比较慢

4. 选择防火墙的原则

- 防火墙自身的安全性
- 考虑特殊的需求
  - IP地址转换（IP Address Translation）
  - 双重DNS
  - 虚拟企业网络（VPN）
  - 病毒扫描功能
  - 特殊控制需求

10.4 网络病毒

- **什么是计算机病毒？**
  - 计算机病毒是一种“计算机程序”，它不仅能破坏计算机系统，而且还能够传播、感染到其他系统
  - 通常隐藏在其他看起来无害的程序中，能复制自身并将其插入其他程序，执行恶意行动

10.4.1 计算机病毒分类

- 文件病毒
- 引导扇区病毒
- 多裂变病毒
- 秘密病毒
- 变异病毒
- 宏病毒

10.4.2 宏病毒及网络病毒

- **宏**：

  软件设计者为了在使用软件工作时，避免一再的重复相同的动作而设计出来的一种工具

  - 它利用简单的语法，把常用的动作写成宏，当再工作时，就可以直接利用事先写好的宏自动运行，去完成某项特定的任务，而不必再重复相同的动作

- **宏病毒**：

  利用宏命令编写成的具有复制、传染能力的宏

  - 宏病毒是一种新形态的计算机病毒，也是一种跨平台的计算机病毒，可以在DOS、Windows、UNIX、Linux、Mac OS系统中散播

10.4.2 宏病毒及网络病毒

宏病毒特征

① 宏病毒会感染.doc文档和.dot模板文件

② 宏病毒的传染通常是Word在打开一个带宏病毒的文档或模板时，激活宏病毒；病毒宏将自身复制到Word通用（Normal）模板中，以后在打开或关闭文件时宏病毒就会把病毒复制到该文件中

③ 多数宏病毒包含AutoOpen、AutoClose、AutoNew和AutoExit等自动宏，通过这些自动宏病毒取得文档（模板）操作权

④ 宏病毒中总是含有对文档读写操作的宏命令

⑤ 宏病毒在.doc文档、.dot模板中以.BFF（Binary File Format）格式存放，这是一种加密压缩格式，不同Word版本格式可能不兼容

10.4.2 宏病毒及网络病毒

- 宏病毒的防治和清除方法

① 使用选项“提示保存Normal模板”

② 不要通过Shift键来禁止运行自动宏

③ 查看宏代码并删除

④ 使用DisableAutoMacros宏

⑤ 使用Word的报警设置

⑥ 设置Normal.dot的只读属性

⑦ Normal.dot的密码保护

10.4.2 宏病毒及网络病毒

- 病毒入侵网络的途径：
- 局域网
  - 病毒入侵局域网的主要途径是通过工作站传播到服务器硬盘，再由服务器的共享目录传播到其他工作站
  - 还有很多病毒可以通过特殊的网络协议在局域网内传播，如ARP病毒
- 因特网
  - 木马病毒（Trojan horse virus）
  - 蠕虫病毒（Worm virus）
  - 恶意软件（Malicious software）
  - 电子邮件病毒

10.4.2 宏病毒及网络病毒：防治办法

- 采取技术上和管理上的措施，计算机病毒是完全可以防范的
  - 目前最有效的防治办法是购买商业化的病毒防御解决方案及其服务
    享受专业公司提供的不断升级的防病毒产品及服务
  - 比较成熟的病毒防御软件（有利有弊）
  - 个人用户的上网习惯

本章小结

- 网络安全的基本概念
- 信息安全技术
  - 数据加密
- 防火墙
  - 三种类型
- 网络病毒
  - 宏病毒
  - 病毒入侵途径

作业

- 第407页：

☺☺☺☺