第十二章 安全通信和网络攻击

12.1 网络与协议安全机制

TCP/IP是主要协议，也存在许多安全缺陷

12.1.1 安全通信协议

- 为特定应用通信信道提供安全服务的协议被称为安全通信协议
- 常见的安全通信协议：
  - IP简单秘钥管理（SKIP）：保护无会话数据报协议的加密工具，SKIP被设计为与IPSec相结合，并且工作在OSI模型的第三层上，能够对TCP/IP协议族的任何子协议进行加密
  - 软件IP加密：工作在第三层IP安全协议，使用封装协议来提供身份认证、完整性和机密性
  - 安全远程过程调用（S-RPC）：**身份认证服务，只防止远程系统上未经授权的情况下执行代码的手段**
  - 安全套接字层（SSL）：保护WEB服务器和WEB浏览器之间的通信，是一个面向会话的协议，提供机密性和完整性
  - 传输层安全（TLS）：功能类似于SSL，但是更健壮的认证和加密协议，TLS能加密UDP和会话初始协议（SIP）连接
  - **安全电子交易（SET）**：互联网上进行交易传输时使用的安全协议，RSA加密以及数据加密标准（DES）

12.1.2 身份认证协议

- 远程系统和服务器之间开始建立连接之后，应当是验证远程用户，该操作被称为身份认证
  - **挑战握手身份认证协议（CHAP）**：CHAP对用户名和密码加密，在建立通话会话持续期间，CHAP定期对远程系统重新进行身份认证，从而认证远程客户端的持久性
  - **密码身份认证协议（PAP）**：基于PPP的标准身份认证协议，以**明文的形式传递用户名和密码**，仅简单的提供客户端向认证服务器传输登录凭证的手段
  - **可扩展身份认证协议（EAP）**：一个身份认证框架，允许自定义身份认证安全解决方案

12.2 安全的语音通信

- 常规的专用分支交换（PBX）或POTS/PSTN语音容易被截获

12.2.1 互联网语音协议（VoIP）

- VoIP是一种将语音封装成IP数据包，并支持音频电话通过TCP/IP网络进行连接的技术
- VoIP安全问题：
  - 呼叫ID可以被伪造，黑客可以执行语音钓鱼（VoIP钓鱼）攻击或者在网络中进行语音垃圾邮件（SPIT）攻击
  - 呼叫管理系统和VoIP电话本身的漏洞可能受到OS攻击和DOS攻击
  - 通过欺骗发动中间人攻击
  - 类似VLAN中的802.1x认证证伪和VoIP跳跃（跳过验证通道）
  - 不加密的VoIP流量可以通过解码的方式被窃听

12.2.2 社会工程学

- 社会工程学是不认识的人获得组织内部某个人信任的一种方式，组织内的人是的公司容易受到社会工程学攻击
- 防止社会工程学的唯一途径就是教会用户如何应对和沟通只有语音的通信

12.2.3 伪造和滥用

- 许多PBX系统都会被恶意攻击者的攻击用于躲避收费和隐藏自己的身份
- 飞客行为是一种针对电话系统的特定攻击类型
- 常见飞客工具：
  - 黑盒用于操纵线电压，以便窃取长途服务
  - 红盒用于模拟硬币存入付费电话时的声音
  - 蓝盒用于模拟与电话网络主干系统直接互动的2600Hz声音
  - 白盒用于控制电话系统

12.3 多媒体协作

- 多媒体协作是使用不同的多媒体通信解决方案来支持远程协作

12.3.1 远程会议

- 远程会议技术用于让任何产品名称、硬件或软件可以和远程关系人之间相互交互

12.3.2 即时消息

- 即时消息（IM）是一种机制，允许两个用户在互联网上的任何位置进行实时文字聊天
- 及时消息的缺陷：
  - 有很多漏洞
  - 容易遭受数据包监听
  - 缺乏加密和用户隐私

12.4 管理电子邮件的安全性

- 电子邮件是一种罪广泛和常用的互联网服务
- Sendmail是Unix系统中最常用的SMTP服务器，Exchange是Microsoft系统中最常用的SMTP服务器
- SMTP被设计为邮件中继系统，希望避免SMTP服务器成为开放中继，开放中继是一种在接受和中继电子邮件之前并不对发送者进行身份认证的SMTP服务器

12.4.1 电子邮件安全性的目标

- 增强的电子邮件可能满足下面列出的一个或多个目标
  - 提供不可否认性
  - 限制只有预定的接受者能够访问邮件
  - 维护邮件的完整性
  - 对邮件源进行身份认证和校验
  - 验证邮件的传输
  - 对邮件的内容或附件的敏感度进行分类
- 如果对电子邮件进行备份，需要让用户意识到这种情况

12.4.2 理解电子邮件的安全问题

- 电子邮件不采用加密，使得电子邮件容易被截获和偷听
- 电子邮件是病毒、蠕虫、特洛伊木马、破坏性宏文件以及其他恶意代码利用的最常用传输机制
- 在验证源上面，电子邮件几乎没有提供任何方法
- 电子邮件本身也可以作为一种攻击机制，如Dos

12.4.3 电子邮件安全解决方案

- 安全多用途互联网邮件扩展（S/MIME）：通过公钥加密和数字签名为电子邮件提供身份认证和隐私保护。
- S/MIME提供两种类型的邮件：
  - 签名的邮件：提供完整性和对发送者的身份认证
  - 安全封装的邮件：提供完整性、对发送者的身份认证以及机密性
- MIME对象安全服务（MOSS）：利用MD2、MD5、RSA公钥以及数据加密标准（DES），从而提供身份认证和加密服务
- 隐私增强邮件（PEM）：使用RSA、DES和X.509提供身份认证、完整性、机密性和不可否认性
- 电子邮件验证标准（DKIM）：一种手段，确保合法邮件被组织通过域名身份认证来发送

- 良好的隐私（PGP）：使用多种加密算法对文件和电子邮件进行加密的公钥-私钥密码系统

如果附件是电子邮件通信的必须部分，需要依赖对用户的培训和反病毒工具进行保护

12.5 远程接入安全管理

- 远程访问使深处远方的客户端能够建立与某个网络的通信会话

12.5.1 计划远程接入安全

- 列出远程安全策略时，务必解决以下问题：
  - 远程连接技术：每一样远程连接都有自己的问题
  - 传输保护：加密协议、加密连接系统、加密的网络服务和应用程序存在多种形式，根据需求选用适当的安全服务组合，包括VPN、SSL、TLS、SSH、IPSec以及L2TP
  - 身份认证保护：为了保护登录凭证的安全，需要使用某种身份认证协议，甚至授权采用集中的远程访问身份认证系统，可能包裹密码认证协议（PAP）、挑战握手认证协议（CHAP）、扩展认证协议（EAP）以及扩展的PEAP或者LEAP、远程认证拨号用户服务（RADIUS）以及终端访问控制访问控制系统（TACACS+）
  - 远程用户支持： 远程发昂文用户可以定期寻求技术支持

12.5.2 拨号协议

- 在建立远程连接时，必须使用某些协议来管理连接的实际创建方式，并未其他协议创立工作于其上的通用通信基础
- 拨号协议的主要例子：
  - 点对点协议（PPP）：全双工协议，用于各种非LAN连接上传输TCP/IP数据包
  - 网络串行线路协议（SLIP）：支持异步串行连接上的TCP/IP，很少使用

12.5.3 集中化的远程身份认证服务

- 集中化的远程身份认证服务提供了远程客户端和专用网络之间的安全保护层
- 远程认证拨号用户服务（RADIUS），用于集中完成远程拨号连接的身份认证，使远程的访问服务器将拨号用户的登录凭证发送给RADIUS服务器进行身份认证。Radius协议的三个基本功能：
  - 对需要访问网络的用户或设备进行身份验证
  - 对已通过身份验证的用户或设备授予资源访问的权限
  - 对已授权的访问进行审计
- 终端访问控制器访问控制系统（TACACS+）:替换RADIUS

12.6 虚拟专用网络

- 虚拟专用网络是一条通信隧道，可以在不可信的中间网络上提供身份认证和数据通信的点对点传输，大多数VPN使用加密技术来保护封装的通信数据
- VPN在不可信的中间网络上提供了机密性和完整性，并不保证可用性

12.6.1 隧道技术

- 隧道技术：通过将协议包封装到其他协议包中来保护协议包的内容
- 如果封装协议涉及加密，那么不必担心丢失机密性和完整性

12.6.2 VPN的工作原理

- VPN连接能够被建立在其他任何网络通信链接上
- VPN可以连接两个单独的系统或两个完整的网络

12.6.3 常用VPN协议

常用VPN协议：PPTP（IP网络）、L2F(数据链路层)、L2TP（数据链路层）和IPSec（IP网络）

1. 点对点隧道协议
    - 点对点隧道协议（PPTP）是从拨号协议点对点协议开发出来的一种封装协议，在两个系统之间创建一条点对点隧道，并封装PPP包
    - 身份认证协议包括：MS-CHAP（微软挑战握手身份认证协议）、CHAP（挑战握手协议）、PAP(密码身份认证协议)、EAP(扩展身份认证协议)、SPAP（Shiva密码身份认证协议）
2. 二层转发协议和二层隧道协议
    - 二层隧道协议（L2TP）源于PPTP和L2F的组合，在通信的断电之间建立一条点对点隧道，缺乏内置的加密方案，依赖IPSec作为安全机制，支持TACAS+和RADIUS
3. IP安全协议
    - 目前最常用的协议IPSec，只能用于IP通信，提供安全的身份认证以及加密的数据传输
    - IPSec主要的组件或功能：
        - 身份认证头（AH）：提供**身份认证、完整性以及不可否认性**
        - 封装安全有效载荷（ESP）：提供加密，从而保护**机密性**，执行**有限的身份认证**操作，工作在第三层，在传输模式中对数据进行加密，在隧道模式整个IP包都加密。

表 12.1　VPN 协议的主要特征

VPN 协议	自带身份认证保护？	自带数据加密？	支持的协议	支持拨号连接？	同时存在的连接数
PPTP	是	否	只支持 IP	是	单个点对点连接
L2F	是	否	只支持 IP	是	单个点对点连接
L2TP	是	否(可以使用 IPSec)	支持任何协议	是	单个点对点连接
IPSec	是	是	只支持 IP	否	多个连接

12.6.4 虚拟局域网

- 在网络上进行逻辑隔离而不改变其物理拓扑
- VLAN与安全相关的优势：
  - 控制和限制广播流量。阻断子网和VLAN中的广播
  - 隔离网络分段的流量
  - 减少网络监听的脆弱性
  - 防止广播风暴

12.7 虚拟化

- 虚拟化技术用来在单一主内存中承载一个或多个操作系统
- 虚拟化的好处
  - 备份比同等安装在本地硬盘上的系统更容易和更快速
  - 恶意代码或感染很难影响主机操作系统

12.7.1 虚拟化软件

- 虚拟化应用程序是一种软件，一个虚拟应用被打包或者封装，使它具备移动性和在不用完整安装原有的操作系统的情况下运行
- 虚拟桌面至少包括三种不同类型的技术：
  - 一种远程工具，允许用户访问远程的计算机系统、并允许查看和控制远程桌面、键盘、鼠标
  - 虚拟应用概念的卡欧战，封装多个应用和一些桌面形式
  - 扩展或扩展桌面

12.7.2 虚拟化网络

- 虚拟化网络时将硬件和软件网络组件组合成单一合成实体
- SDN（软件定义网络）是一种独特的网络操作、设计和管理方法，旨在从控制层分离基础设施层
- 虚拟化网络的另一个概念SAN，将多个单独的存储设备组合成单一综合的网络访问存储容器

12.8 网络地址转换

- NAT是一种将报头的内部地址转成公共的IP地址，从而在互联网上传输的机制
- NAT的优点：
  - 始终只使用一个或者几个租用的公共IP地址将整个网络连接到互联网
  - 始终能够在互联网通信的情况下，定义专用IP地址用于专用网络
  - NAT能通过互联网隐藏IP地址方案和网络拓扑结构
  - NAT还通过限制连接提供保护

12.8.1 专用IP地址

- 10.0.0.0 ~ 10.255.255.255（整个A类范围）
- 172.16.0.0 ~ 172.31.255.255（16个B类范围）
- 192.168.0.0 ~ 192.168.255.255（255个C类范围）

12.8.2 状态NAT

进行NAT操作时，会在内部客户端生产的请求、客户的内部IP地址以及联系的互联网服务的IP地址之间维护一个映射。

12.8.3 静态NAT与动态NAT

- 静态NAT：特定的内部客户端的IP地址永久映射到特定的外部公共IP地址，允许外部实体与专用玩过内部的系统进行通信
- 动态NAT：允许多个内部客户端使用较少的租用公共IP，该方法将互联网访问成本降到最低

12.8.4 自动私有IP寻址

- APIPA为每个失败的DHCP客户端委派位于169.254.0.1到169.254.255.254内的一个IP

12.9 交换技术

- 两个系统通过多个中间网络连接时，一个系统向另一个系统传输数据包的任务是非常复杂的

12.9.1 电路交换

- 两个通信方会创建一条专用的物理路径，在会话过程中持续保护，电路交换使用永久的物理连接

12.9.2 分组交换

- 报文或者通信先被分为若干小段，然后通过中间网络发送至目的地，分组交换不具有排他性

表 12.2　电路交换与分组交换的比较

电路交换	分组交换
连续通信	突发通信
已知的固定延迟	可变延迟
面向连接	无连接
易受连接损耗的影响	易受数据损耗的影响
主要用于语音通信	用于任何通信类型

12.9.3 虚电路

- 虚电路是一种在两个指定端点之间分组交换网上创建的逻辑路径或电路
- 分组交换虚电路：永久虚电路（PVC）、交换虚电路（SVC）

12.10 WAN技术

- WAN连接用来把远端网络、节点或单个设备连接在一起，适当的连接管理和传输加密对于确保安全连接是必要的
- 专线：一种长期保留以供指定客使用的线路，使用保持畅通，随时等待数据传输通信
- 综合数字业务（ISDN）是一种完全数字化的电话网，能够同时支持语音通信和高速数据通信
    - **基本速率接口（BRI）**为客户提供的连接具有两个B信道和一个D信道
    - **主速率接口（PR）**为客户提供连续具有2至23个64Kbps的B信道和一个64Kbps的信道

12.10.1 WAN连接技术

- 边界连接设备（信道服务单元/数据服务单元 CSU/DSU）：将LAN信号转换成WAN运营网络锁使用的格式

12.10.2 X.25 WAN连接

- 使用永久虚电路在两个系统或网络之间特定的点对点连接

12.10.3 帧中继连接

- 帧中继是一种使用分组交换技术在通信中断之间建立虚电路的第二层连接机制
- CIR(承诺信息速率)：服务商向客户保证的最小带宽

12.10.4 ATM

- 异步传输模式（ATM）是一种心愿交换WAN通信技术，是一种面向连接的分组交换技术

12.10.5 SMDS

- 交换式多兆位数据服务（SMDS）是一种无连接的分组交换技术，用于连接多个LAN，从而组成城域网（WAN）

12.10.6 专门的协议

- WAN连接技术需要使用专门的协议来支持各种各样特殊的系统或设备
- 同步数据链路控制（SDLC）：用在专门租用线路的永久物理连接上，运行在* SI第二层
- 高级数据链路控制（HDLC）：专门针对同步串行连接而设计，支持全双工，支持点对点和点对多点，使用轮询技术，工作在* SI第二层，提供流控制、差错检测与校验
- 高速串行接口（HSSI）：定义了复用器和路由器如何连接告诉网络运营商服务，工作在* SI第一层

12.10.7 拨号封装协议

- 点对点协议（PPP）：用于支持在拨号或点对点连接上传输IP通信数据
- PPP最初设计用于支持身份认证的CHAP和PAP，新版还支持MS-CHAP,EAP以及SPAP

12.11 各种安全控制特性

12.11.1 透明性

- 安全控制或访问机制对于用户来说是不可见的，安全机制越透明，用户越难避开安全机制，甚至无法差距安全机制的存在

12.11.2 验证完整性

- 为了验证数据传输的完整性，可以使用散列总数的检验和
- CRC（循环冗余校验）：也可以作为完整性工具使用

12.11.3 传输机制

- 传输日志是一种关注与通信的审计形式
- 传输错误校验是面向连接的或面向会话的协议和服务内置的一种能力

12.12 安全边界

- 安全边界是任何两个具有不同安全要求或需求的区域、子网或环境之间的交线
- 安全边界还存在于物理环境和逻辑环境之间，为了提供逻辑安全，必须采用与物理安全性不同的安全机制
- 安全边界始终应当清楚的定义
- 物理中的安全防线常常是逻辑环境中安全防线的反映
- 在讲安全策略转换为实际的控制时，必须分别考虑所有的环境和安全边界

12.13 网络攻击与对策

12.13.1 DoS和DDoS

- 拒绝服务攻击是一种资源消耗型攻击，以阻碍系统上的合法活动为主要目的
- 拒绝服务攻击的方法：
  - 利用硬件或软件的漏洞进行攻击
  - 通过巨量的垃圾网络流量以泛洪的方式充满受害者的通信信道
- 针对Dos攻击的防御措施：
  - 添加防火墙、路由器和入侵检测来检测Dos流量和自动阻断端口过滤基于元和目的地址的数据包
  - 与服务提供商保持良好沟通
  - 外部系统上禁用echo回复
  - 边界系统上禁用广播特性
  - 阻断伪造数据包进入或离开网络
  - 保持所有系统已安装来自供应商的最新安全更新补丁
  - 考虑第三方商用Dos保护/响应服务

12.13.2 偷听

- 偷听是为了复制目的而对通信信息进行简单的侦听
- 维护物理接入的安全性，从而防止未授权的人员访问你的IT基础设施能够对付偷听
- 对通信传输使用加密和一次性身份认证降低偷听的有效性和及时性

12.13.3 假冒/伪装

- 假冒或伪装是指假装成某人或某事，从而获得对系统的未授权访问
- 对付假冒攻击的解决方法包括：使用一次性填充和令牌身份认证系统

12.13.4 重放攻击

- 重放攻击是假冒攻击的分支，可以利用偷听捕获的网络通信进行攻击
- 使用一次性身份认证机制和序列回话身份标识来防范重放攻击

12.13.5 修改攻击

- 修改攻击能够更改捕获的数据包，然后将其放回系统中
- 针对修改重放攻击的对策包括数字签名验证与数据包校验 与验证

12.13.6 地址解析协议欺骗

- ARP映射可能受到欺骗攻击，欺骗为请求的IP地址系统提供假的MAC地址，从而将通信重定向到另一个目的地。

12.13.7 DNS投毒、欺骗和劫持

- DNS投毒和DNS欺骗被称为解析攻击，攻击者更改DNS系统中域名到IP地址的映射并将流量定向到假冒系统或简单的执行拒绝服务时，DNS投毒就发生了
- DNS劫持漏洞，唯一解决的办法就是升级DNS到域名系统安全扩展（DNSSEC）

12.13.8 超链接欺骗

- 超链接欺骗既可以采用DNS欺骗的形式，也可以简单的在发送给客户端的HTML代码中修改超链接URL
- 对付超链接欺骗攻击的防护手段包括防止DNS欺骗、保持系统更新补丁