第十一章 网络安全架构与保护网络组件

11.1 OSI模型

基于OSI模型的协议采用封装的机制，通过每一层从上一层接收到数据后，封装会给数据添加一个报头，并且还可能会添加一个报尾，然后才将数据传输到下一层。

- 数据从OSI模型的应用层向下移动至物理层时，在每一层都会发生**封装**。
- 数据从OSI模型的物理层向上移动至应用层时，在每一层发生的逆向操作称为**解封装**。

图 11.4 OSI 模型的数据名称

1. 物理层

物理层从数据链路层接收帧，并把帧转换为可以通过物理连接介质传送的比特。

物理层的协议：

- EIA
- X.21
- 高速串行接口（HSSI）
- 同步光网络（SONET）
- V.24和V.35

2. 数据链路层

数据链路层负责将来自网络层的数据包格式化为可以进行传输的适当格式。

工作在数据链路层的网络硬件设备包括交换机和桥。

数据链路层的协议：

- 串行线路网络协议（SLIP）
- 点对点协议（PPP）
- **地址解析协议（ARP）：将IP地址解析为MAC地址。**
- **反向地址解析协议（RARP）：将MAC地址解析为IP地址。**
- 二层转发协议（L2F）
- 二层隧道协议（L2TP）：L2TP（第二层隧道协议）可使用 IPsec（网际协议安全）来提供流量加密，确保通过 L2TP VPN 流量的机密性。
- 点对点隧道协议（PPTP）：PPTP（点对点隧道协议）以明文形式发送会话的初始数据包，可能包括用户名和散列密码。PPTP 支持 EAP，并被用来封装 PPP 数据包。
- 综合服务数字网络（ISDN）

3. 网络层

网络层负责向数据中添加路由和寻址信息。

网络层负责提供路由或传递信息，但不负责保证传输已进行验证（这个工作由传输层负责）。

网络层还管理着错误检测和节点数据通信（也就是通信控制）。

工作在网络层的硬件设备包括路由器和桥式路由器。路由协议：距离矢量（RIP、IGRP和BGP）和链路状态（OSPF）。

网络层的协议：

- 网络控制报文协议（ICMP）
- 路由信息协议（RIP）
- 开放式最短路径优先（OSPF）
- 边界网关协议（BGP）
- 网络组管理协议（IGMP）
- 网际协议（IP）
- 网际协议安全（IPSec）
- 互联网分组交换协议（IPX）
- 网络地址转换（NAT）
- 网络简单秘钥管理协议（TKIP）

4. 传输层

传输层负责管理连接的完整性并控制会话。

传输层的协议：

- 传输控制协议（TCP）
- 用户数据报系协议（UDP）
- 顺序数据包交换（SPX）
- 安全套接字层（SSL）
- 传输层安全（TLS）

5. 会话层

会话层负责两台计算机之间建立、维护和终止通信会话。单工、半双工、全双工。

会话层的协议：

- 网络文件系统（NFS）
- 结构化查询语言（SQL）
- 远程过程调用（RPC）

6. 表示层

表示层负责将从应用层接受的数据转换为遵从OSI模型的任何系统能理解的格式，还负责加密和压缩。

表示层的格式标准：

- 美国信息交换标准代码（ASCII）
- 扩充二进制编码的十进制交换码（EBCDIC）
- 标签图像文件格式（TIFF）
- 联合图像专家组（JPEG）
- 运动图像专家组（MPEG）
- 音乐设备数字接口（MIDI）

7. 应用层

应用层负责将协议栈与用户的应用程序、网络服务或操作系统连接在一起，准许应用程序和协议栈进行通信。

有一种网络设备（或服务）工作在应用层：应用层网关，作为协议转换工具。

应用层的协议：

- 超文本传输协议（HTTP）
- 文件传输协议（FTP）
- 行式打印机后台程序（LPD）

- 简单邮件传输协议（SMTP）
- 远程登录（Telnet）
- 普通文件传输协议（TFTP）
- 电子数据交换（EDI）
- 邮局协议第三版（POP3）
- 互联网消息访问协议（IMAP）
- 简单网络管理协议（SNMP）
- 网络新闻传输协议（NNTP）
- 安全远程过程调用（S-RPC）
- **安全电子交易（SET）支付、电子钱包。**

11.2 TCP/IP模型

TCP/IP模型为四层：应用层：传输层（主机到主机层）、网际层（互联网层）和网络接入层

图 11.5　OSI 模型与 TCP/IP 模型的对比

TCP的设计目的是便于使用而不是安全，因此容易遭受攻击。 TCP/IP可以使用两个系统之间的VPN链接进行安全保护或采用TCP包装，通过用户ID和系统ID的基础上限制对端口和资源的访问。

1. 传输层协议
    - 传输控制协议（TCP）在OSI模型的第四层上运作，这个面向连接的协议能够支持全双工通信，使用可靠的会话。

- 用户数据报协议（UDP）也在OSI模型的第四层上运作，面向无连接的，尽力而为的通信协议。

2. 网络层协议和IP网络基础

- IP为数据包提供路由寻址功能，IP不保证传送数据包以正确的顺序传送数据包，也不保证只进行一次传送，所以IP上使用TCP获得可靠的和受控的通信会话
- ICMP：用于确定某个网络或特定链接的健康状况，遗憾的是ICMP的功能被各种基于贷款的拒绝服务攻击利用，
- ping of death攻击、smurf攻击和ping flood泛洪攻击
  - ping of death攻击：发送一个畸形的大于65535字节（大于最大IPV4数据包大小）的数据包给一个计算机并试图让其崩溃。
  - smurf攻击：Woodlly Attacker向一个具有大量主机和因特网连接的网络的广播地址发送一个欺骗性Ping分组（echo 请求），这个目标网络被称为反弹站点，而欺骗性Ping分组的源地址就是Woodlly希望攻击的系统。
  - ping flood泛洪攻击是一个基本的拒绝服务攻击。
- IGMP：网咯管理协议允许系统支持多播
- ARP与反向ARP，使用ARP缓存污染的技术滥用活动

3. 常见的应用层协议

- 远程登录（Telnet），TCP端口23，支持命令和运行应用，不支持文件传输
- 文件传输协议（FTP），TCP端口20和21，支持文件交换的网络应用
- 普通文件传输协议（TFTP），UDP端口69，支持文件交换的网络应用，不要求认证
- 简单邮件传输协议（SMTP），TCP端口25，客户端向邮件服务器以及从一个邮件服务器向另一个邮件服务器发送邮件
- 邮局协议（POP3），TCP 端口100，将邮件服务器收件箱中的邮件传送至邮件客户端
- 互联网消息访问协议（IMAP），TCP端口143，用于将邮件服务器收集箱中的邮件传输至邮件客户端，比POP3安全
- 动态主机配置协议（HTTP），TCP端口80，用于从web服务器向WEB浏览器传送WEB页面元素
- 安全套接字层（SSL），TCP端口443,原本设计用于支持安全的web通信，还能保护应用层协议通信安全
- 行式打印后台程序（LPD），TCP端口515，用于管理打印作业以及向打印机发送打印作业的网络服务
- X视窗，TCP端口6000-6063，用于支持不同系统之间共享文件的网络服务
- 网络文件系统（NSF），TCP端口2049，文件共享服务
- 简单网络管理协议（SNMP），UDP161 ，用于从中间监控站轮询设备来收集网络健康和状况信息

分层协议的应用

- 优点：
  - 可以在更高层使用更为广泛的协议
  - 封装可以和不同的层进行合作
  - 在更为复杂的网络中支持灵活性和弹性
- 缺点：
  - 允许隐蔽信道
  - 过滤机制可被绕过
  - 逻辑上实现的网络边界可以被逾越（VLAN封装欺骗）

TCP/IP的脆弱性

不正确的实现TCP/IP协议堆栈很容易遭受缓冲区溢出攻击、SYN泛洪、DOS攻击、碎片攻击、过长数据包攻击、欺骗攻击、中间人攻击、劫持攻击以及编码错误攻击，遭受监控或修改提案等被动攻击。

- 圣诞树攻击：Xmas，畸形TCP报文，设置一个数据包上所有可能的TCP标志，因此“像点亮圣诞树一样点亮了它”。
- Land攻击：把TCP SYN包的源地址和目的地址都设置成一个受害者的IP，这将导致受害者向它自己的地址发送SYN-ACK消息结果这个地址又发回ACK消息并创建一个空连接，每一个这样的连接都将保留直到超时。
- Fraggle攻击：类似于smurf攻击只是使用UDP应答消息而非ICMP。

域名解析

最基础的三层：

- 第三层或底层，是MAC地址层。MAC地址或硬件地址是“永久”的物理地址。
- 第二层或中间层，是IP地址层。IP地址是在MAC地址上“临时”赋予的逻辑地址。
- 最顶层是域名。域名或计算机名是在IP地址上“临时”赋予的友好转换约定。

11.3 汇聚协议

汇聚协议是专业或专有协议和标准协议的融合。

- 以太网光纤通道（FCoE）：光纤通道是网络存储解决方案（SAN）或网络附加存储形式（NAS），光纤通道作为网络层或OSI第三层协议，替换IP作为标准的以太网网络负载
- MPLS（多协议标签交换）：一种高通过、高性能的网络技术，基于最短路径的标签而不是更长的网络地址传输
- 互联网小型计算机系统接口（iSCSI）:基于IP的网络存储标准，支持独立的文件存储、传输，以及对局域网、广域网的检索或公共网络连接，是光纤通道的低成本替代方案

- IP语音（VoIP）:网络上传输语音和/或数据的一种隧道机制
- 软件定义网络（SDN）：一种独特的对网络进行操作、设计和管理的方法，还提供一种直接怼中央位置进行网络设计的新方法，另一种SDN的思考是其有效的网络虚拟化

11.4 内容分发网络

CDN是资源服务的集合，被部署在互联网的许多数据中心提供低延迟、高性能和所承载内容的高可用性。

大多数CDN关注于服务器的物理分布，然而基于客户的CDN也是可能的。这通常被称为P2P（点对点）。最被广泛认可的P2P CDN是BitTorrent。

11.5 无线网络

无线网络是因为易于部署和相对低廉的成本，称为一种连接企业和家庭系统的流行方法。

缺点：容易被远程窃听、数据包嗅探、新的DoS和入侵形式。数据泄露是数据通过电磁信号进行传输。（TEMPTEST）

保护无线接入点

- 无线覆盖单元是物理环境中无线设备可以接入到无线接入点的区域，无线覆盖可导致环境中的安全泄露
- 部署无线网络时，应该部署接入点并使用基础设施模式而不是点对点模式
- 基础设施变化模式：独立模式、有限扩展模式、企业扩展模式和桥接模式
  - 独立模式：无线接入点连接无线客户端但没有提供任何有线资源
  - 有线扩展模式： 无线接入点连接无线客户端到有限网络
  - 企业扩展模式：多个无线接入点（WAP）用来连接巨大的物理区域到同一个有线网络
  - 桥接模式：无线连接用于连接两个有线网络的情况

保护SSID

- 无线网络分配的服务标识符（SSID），为了区分无线网络。
- 保护SSID的方法：
  - SSID广播应禁用保持无线网络的私密性
  - 使用WP2作为可靠的身份认证和加密解决方案

使用加密协议

- WEP（有限等效保密），采用RC4的流密码算法，是对称流加密算法，在发布的同时就被破解（**依赖于单个预定义的共享静态秘钥**）
- WPA（WEP的替代品），基于**LEAP**和**TKIP**的加密体系并同行使用安全加密用于认证，攻击者可以简单的在WPA网络上运行暴力猜测以发现密码，不提供长期可靠的安

全

- WPA2（基于AES），目前认为是安全的，使用CCMP（计数器模式密码块链接消息认证协议），基于AES的加密方法。**到目前为止，还没有实际的攻击能破坏正确配置的WPA2无线网络加密。**
- 802.1X/EAP：基于端口的网络访问控制协议，确保客户端在没有发生正确认证时不能和资源发生通信联系
  - **EAP（可扩展认证协议）：是认证框架而不是具体的认证机制**
- PEAP（受保护的可扩展认证协议）：通过TLS隧道封装EAP方法，提供了认证和潜在的加密功能
- **LEAP（轻量级可扩展认证协议）**：Cisco专有，用于WAP替代TKIP，**避免使用该协议**
- MAC过滤器：无线接入点阻断那些未授权的设备，但是仅仅在小型的、静态的环境中使用
- TKIP（临时秘钥完整性协议）：被设计为替代WEP而不需要更换无线硬件，WPA使用该协议
- CCMP（计数器模式密码块链接验消息认证协议）：用于取代WEP和TKIP/WPA，使用AES加密和128的秘钥，是首选的标准安全协议

天线的确定

1. 天线类型
   - 全向天线，标准的直杆或杆天线是一种全向天线，可以在垂直于天线本身的方向是发送和接受信号。在大多数基站和客户端设备可以发现这种天线。
   - 定向天线，专注于某个主要方向的发送和接收能力，Yagi天线、cantenna天线、面板天线和抛物面天线。
2. 调整功率水平控制
   - 现场勘测和调整天线位置后，无线信号仍然无法令人满意，需要调整功率。
3. 使用强制门户
   - 一种认证技术，将新连接的无线web客户端重定向到强制门户访问控制页面。

4. 一般的Wi-Fi安全措施

(1) 改变默认的管理员密码。
(2) 关闭 SSID 广播。
(3) 变更 SSID 到特定的方式。
(4) 如果无线客户端比较少且是静态的，启用 MAC 过滤。
(5) 考虑使用静态 IP 地址，或配置保留的 DHCP(仅适用于小型部署)。
(6) 开启支持的身份认证和加密的最高形式。如果不提供 WPA2，那么使用 WPA 和 WEP 提供非常有限的保护也比未加密的网络好得多。
(7) 把无线视为远程访问，并使用 802.1x 进行访问管理。
(8) 把无线视为外部接入，把 WAP 和有线网络用防火墙进行隔离。
(9) 把无线视为攻击者的入口，用 IDS 监控所有 WAP 到有线网络的通信流量。
(10) 需要对无线客户端和 WAP 之间的通信进行加密，换句话说，需要 VPN 连接。

11.6 保护网络组件

网络被分为内部网和外部网。

- 内部网：一种专用网络，被设计用于集成与建立互联网上的相同信息服务。
- 外部网：互联网和内部网之间的中间网络。隔离区（DMZ）或边界网络。

网络隔离的好处：

- 提高性能
- 减少通信
- 提高安全性

11.6.1 网络接入控制

- 网络接入控制（NAC）是一种访问控制环境中严格遵守和实施安全策略的概念，目标如下：
  - 预防/减少0-day攻击
  - 加强网络通信的安全策略
  - 使用验证完成访问控制
- NAC可以通过进入前评估方式和进入后评估方式：
  - 进入前评估方式需要系统满足当前的安全要求才被允许与网络进行通信
  - 进入后评估方式基于用户的活动允许访问或拒绝访问，是预定义的授权矩阵

11.6.2 防火墙

- 防火墙是管理和控制网络通信的必要方式
- 防火墙被用于阻止或过滤通信，大多数防火墙提供广泛的日志记录、审计和监控性能以及报警和基本的入侵检测系统功能
- 防火墙不能组织通过其他已授权通信信道传送的病毒或恶意代码，不能防止未授权但由用户无意或有意造成的数据泄露

- 防火墙故障往往由于人为错误和不当配置 造成的
- 防火墙的基本类型有4中，静态的数据包过滤防火墙、应用级网关防火墙、电路级网关防火墙以及状态监测防火墙
    - **第一代 静态的数据包防火墙**：通过检查报文头部的数据进行通信过滤，容易受到虚假数据包的欺骗，是第一代防火墙，工作在OSI模型的第三层，也被成为屏蔽路由器或常用路由器
    - **第二代 应用级网关防火墙**：被成为代理防火墙，基于传送或接收数据的网络服务来过滤通信，每种应用类型都必须具有自己唯一的代理服务器，对网络性能会产生负面影响，被称为第二代防火墙，工作在应用层
    - **第二代 电路级网关防火墙**：用于在可信合作伙伴之间建立通信会话，工作在会话层，SOCKS是电路级方管防火墙的通用实现，只基于通信电路的终点名称来许可或拒绝转发策略，属于第二代防火墙
    - **第三代 状态监测防火墙**：对网络通信的状态或环境进行评估，能够为已授权的用户和活动授予广泛的访问权限，并且积极的监视和组织未授权的用户和活动，被视为第三方防火墙，工作在网络层和传输层
- 多宿主防火墙：防火墙至少具有两个过滤通信的接口
- 防火墙部署的体系结构：防火墙体系结构一般有三种：单层、双层、和三层

11.6.3 终端安全

- 终端安全的概念是指每个单独设备必须维护本地安全
- 终端安全应视为在每个单独主机上提供足够安全的努力

11.6.4 其他网络设备

- 中继器、集中器和放大器：用于加强线缆上的通信信号以及连接使用相同协议的网段，工作在OSI的第一层，连接两侧系统都处于相同的冲突域和广播域
- 集线器： 用于连接多个系统以及连接使用相同协议的网段，工作在OSI模型第一层上，连接系统两侧都是统一冲突域和广播域
- 调制解调器：在模拟信号和数字信号之间进行覆盖和调制
- 桥：用于两个网络连接在一起，以便连接使用相同协议的网段，工作在OSI模型第二层，两侧系统位于相同的广播域，不同的冲突域
- 交换机：能够有效的进行流量传递、建立隔离的冲突域以及提高数据总体的吞吐量，使用VLAN可以隔离广播域，工作在OSI第三层
- 路由器：控制网络上的通信流，工作在OSI模型第三层
- 桥式路由器：一种路由器和桥组合的设备
- 网关： 能够连接使用不同网络协议的网络，工作在OSI模型的第七层
- 代理：不需要在协议之间进行转换的网关
- LAN扩展：一种远程访问的多层交换机

11.7 布线、无线、拓扑和通信技术

11.7.1 网络布线

- 同轴电缆：同轴电缆分为细缆（10Base2）和粗缆（10Base5）
- 同轴电缆常见问题：
  - 弯出超出最大半径幅度，从而破坏中心导线
  - 部署同轴电缆的长度超过推荐的最大长度
  - 在同轴电缆末端没有争取使用50欧姆电阻器
- 基带和宽带线缆
- 基带线缆一次只能传输一个单独的信号，绝大多数网络连线采用基带线缆
- 宽带线缆可以同时传输多个信号

表 11.7　常用网络线缆连接类型的重要特性

类型	最大速率	距离	安装难度	受 EMI 影响程度	成本
10Base2	10Mbps	185 米	中等	中等	中等
10Base5	10Mbps	500 米	高	低	高
10Base-T(UTP)	10Mbps	100 米	低	高	很低
STP	155Mbps	100 米	中等	中等	高
10Base-T/10Base-TX	100Mbps	100 米	低	高	低
1000Base-T	1Gbps	100 米	低	高	中等
光纤	2Gbps 以上	2 公里以上	很高	不受影响	很高

- 双绞线：与同轴电缆相比，双绞线更加灵活，双绞线氛围屏蔽双绞线（STP）和非屏蔽双绞线（UTP）
- 双绞线的常见问题
  - 使用错误的双绞线线缆类型来完成高吞吐率的网络连接
  - 部署的双绞线线缆长度超过推荐的最大长度
  - 具有显著干扰的环境中使用UTP
- 导线
  - 每种线缆类型定义最大长度，距离长的线缆常常可以通过使用中继器或集中器得到补充
  - 针对导线基础上的网络线缆，存在一种备选方案，那就是光纤，传输速度快，不会受到窃听和干扰

11.7.2 网络拓扑

- 环型网络拓扑：每次只有一个系统可以传输数据，通过令牌实现
- 总线型拓扑：系统采用冲突避免机制，总线型的好处所有不存在单点故障，但是中央干线仍然存在单点故障隐患
- 星型拓扑：采用一个集中式连接设备没个系统都通过一个专用的网段连接到中央集线器
- 网状型拓扑结构：为系统提供冗余，多个网段出现故障也不会对连通性造成严重影响

11.7.3 无线通信与安全性

1. 无线的一般概念
    - 扩频：多个频率同时发生
    - 跳频扩频（FHSS）：以串行方式传输数据，同时不断改变所使用的频率
    - 直接序列扩频（DSSS）：以并行的方式同时利用所有可用频率，提高更高的吞吐率，允许接收方重构数据
    - 正交频分复用（OFDM）：利用允许传输进行更紧密压缩的数字多在波调制模式，使用更小的频率组，提供更大的数据吞吐率
2. 蜂窝电话
    - 蜂窝电话：使用无线电波频率组的编写设备与蜂窝电话运营商的网络以及其他蜂窝电话设备或互联网设备交互
    - 蜂窝电话 重点：
        - 蜂窝电话提供商网络上的通信，不管是语音、文字还是数据都不一定是安全的
        - 特定的无线嗅探装备能够截获蜂窝电话传输的信息
        - 如果蜂窝电话联通互联网或办公网，攻击者甚至还可以获得其他的攻击方式、访问和破坏手段
        - 蜂窝电话的重要技术WAP，不可能从服务提供商那里得到真正的端对端保护
3. 蓝牙
    - 无线配对不安全
    - 蓝牙劫持能够在不知情的情况下配对
    - 蓝牙窃听允许黑客远程控制蓝牙设备的特征和功能
4. 无绳电话
    - 信号极少加密，很容易被偷听
5. 移动设备
    - 移动手机和其他移动设备证显示出不断增加的安全风险
    - 移动设备的遗失以为着个人和企业机密的破坏
    - 移动设备已成为黑客和恶意代码的攻击目标
    - 移动设备无法避免偷听

11.7.4 LAN技术

1. 以太网
    - 以太网是一种共享介质的LAN技术，也称为广播技术，广播域是一个物理的系统组，冲突域包含若干系统组
    - 以太网可以支持全双工模式，由同轴电缆或者双绞线连接，常见为星型和总线型
2. 令牌环
    - 令牌环采用令牌传递机制来控制哪些系统可以在网络介质上传输数据
    - 令牌环可通过使用多占访问组件（MAU）部署物理星型结构，内部设备使用逻辑令牌连接

3. 光纤分布式数据接口（FDDI）
    - 光纤分布式数据接口使用两个环的告诉令牌传递技术，双环设计允许实现自愈，主要用于大型企业网络的主干
4. 辅助技术
    - 大多数网络并非只包含一种技术，而是包含众多技术
5. 模拟和数字
    - 传输分为两种类型：模拟和数字
        - 使用频率、幅度、相位等发生连续信号时，就是进行模拟通信
        - 使用非连续的电子信号以及状态改变或开关脉冲，出现数字信号
    - 模拟和数字优缺点：
        - 长距离传输时，数字信号比模拟信号可靠
        - 模拟信号具有无限多的变化被用于信号编码
6. 同步和异步
    - 同步通信依赖于定时或时钟机制，基于独立的时钟或数据流内嵌的时间标记，能够支持非常告诉的数据传送
    - 异步通信依赖于停止和开始定界位来管理数据的传输
7. 基带和宽带
    - 基带技术只能支持单个通信信道，以太网就是基带技术
    - 宽带技术能支持多个同时发生的信号，宽带是一种模拟信号形式
8. 广播、多播和单波
    - 广播技术支持与所有可能的接受者进行通信
    - 多播技术支持多个特定的接受者进行通信
    - 单波技术只支持与某个特定接受者的单一通信
9. LAN介质访问
    - 载波侦听多路存取（CSMA）
    - 带有冲突避免的载波侦听多路存取（CSMA/CA）
    - 带有冲突检测的载波侦听多路存取（CSMA/CD）
    - 令牌传递：持有令牌的主机有权传输数据，如FDDI
    - 轮询：主系统一次轮询或了解每个丛书系统是否需要传输数据，SDLC使用了轮询