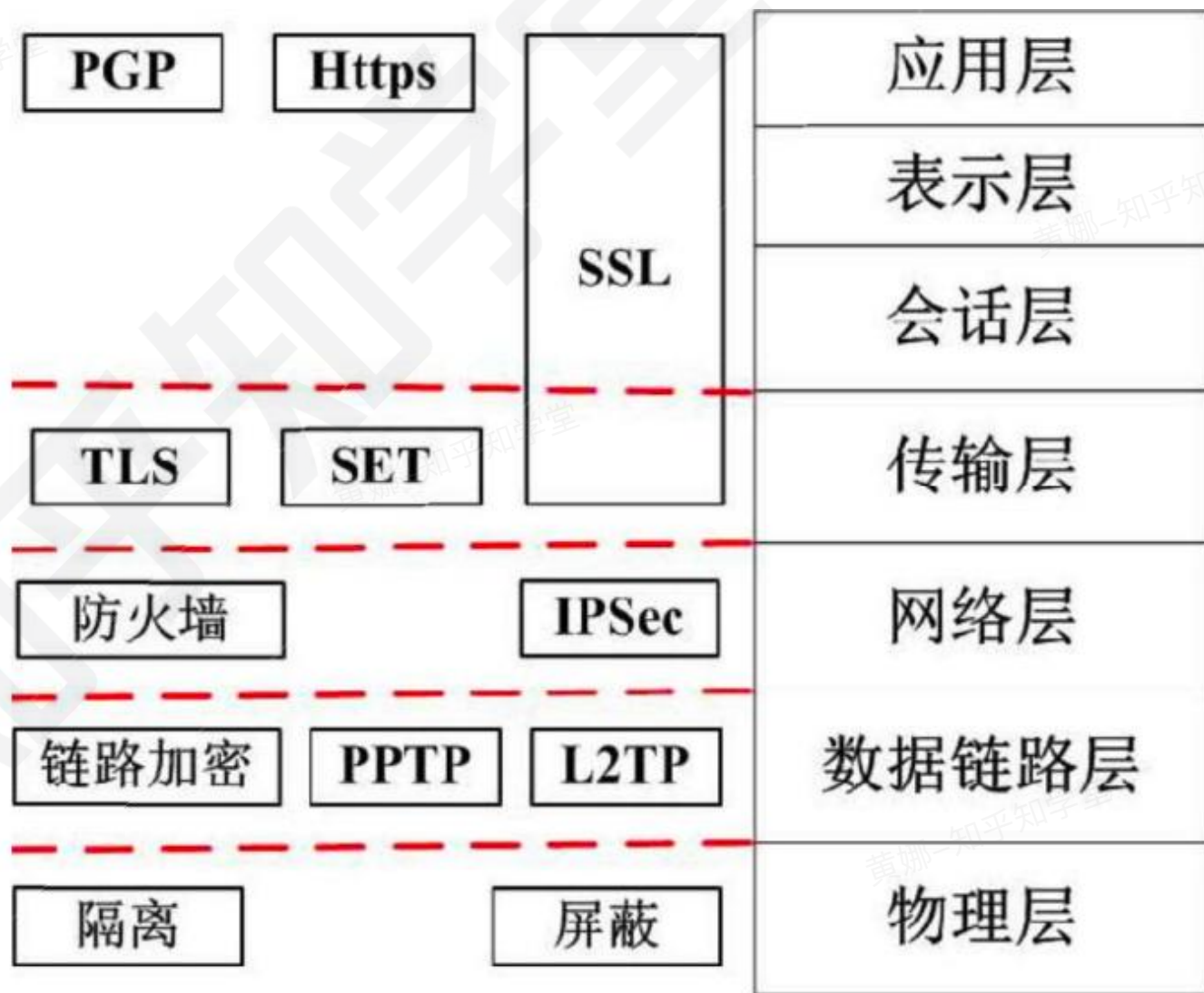


· 07 ·

网 络 安 全 协 议

📁 网络安全协议

- ◆ 物理层主要使用物理手段，隔离、屏蔽物理设备等，其它层都是靠协议来保证传输的安全，具体如下图所示：



网络安全协议

- ◆ **SSL协议**：安全套接字协议，被设计为**加强Web安全传输(HTTP/HTTPS/)**的协议，安全性高，和HTTP结合之后，形成HTTPS安全协议，端口号为**443**。
- ◆ **SSH协议**：安全外壳协议，被设计为**加强Telnet/FTP安全的传输协议**。
- ◆ **SET协议**：**安全电子交易协议**主要应用于**B2C模式(电子商务)**中保障支付信息的安全性。SET协议本身比较复杂，设计比较严格，安全性高，它能保证信息传输的机密性、真实性、完整性和不可否认性。SET协议是PK1框架下的一个典型实现，同时也在不断升级和完善，如SET 2.0将支持借记卡电子交易。
- ◆ **Kerberos协议**：是一种**网络身份认证协议**，该协议的基础是**基于信任第三方**，它提供了在**开放型网络中进行身份认证的方法**，认证实体可以是用户也可以是用户服务。这种认证不依赖宿主机的操作系统或计算机的IP地址，不需要保证网络上所有计算机的物理安全性，并且假定数据包在传输中可被随机窃取和篡改。

网络安全协议

◆ **PGP协议**：使用**RSA公钥证书**进行身份认证，使用**IDEA (128位密钥)** 进行数据加密，使用**MD5**进行数据完整性验证。

◆ 发送方A有三个密钥：A的私钥、B的公钥、A生成的一次性对称密钥；

◆ 接收方B有两个密钥：B的私钥、A的公钥。



考试真题

下面可提供安全电子邮件服务的是()。

A.RSA

B.SSL

C.SET

D.S/MIME

答案：D

解析：MIME(Multipurpose Internet Mail Extensions)中文名为：多用途互联网邮件扩展类型。
S/MIME(Secure Multipurpose Internet Mail Extensions)是对MIME在安全方面的扩展。

网络管理员通过命令行方式对路由器进行管理，要确保ID，口令和会话内容的保密性，应采取的访问方式是()。

A.控制台

B.AUX

C.TELNET

D.SSH

答案：D

考试真题

以下关于第三方认证服务的叙述中，正确的是()。

- A. Kerberos认证服务中保存数字证书的服务器叫CA
- B. 第三方认证服务的两种体制分别是Kerberos和PKI
- C. PKI体制中保存数字证书的服务器叫KDC
- D. Kerberos的中文全称是“公钥基础设施”

答案：B

THE END

功不唐捐，玉汝于成！

• 开 启 新 征 程 •

