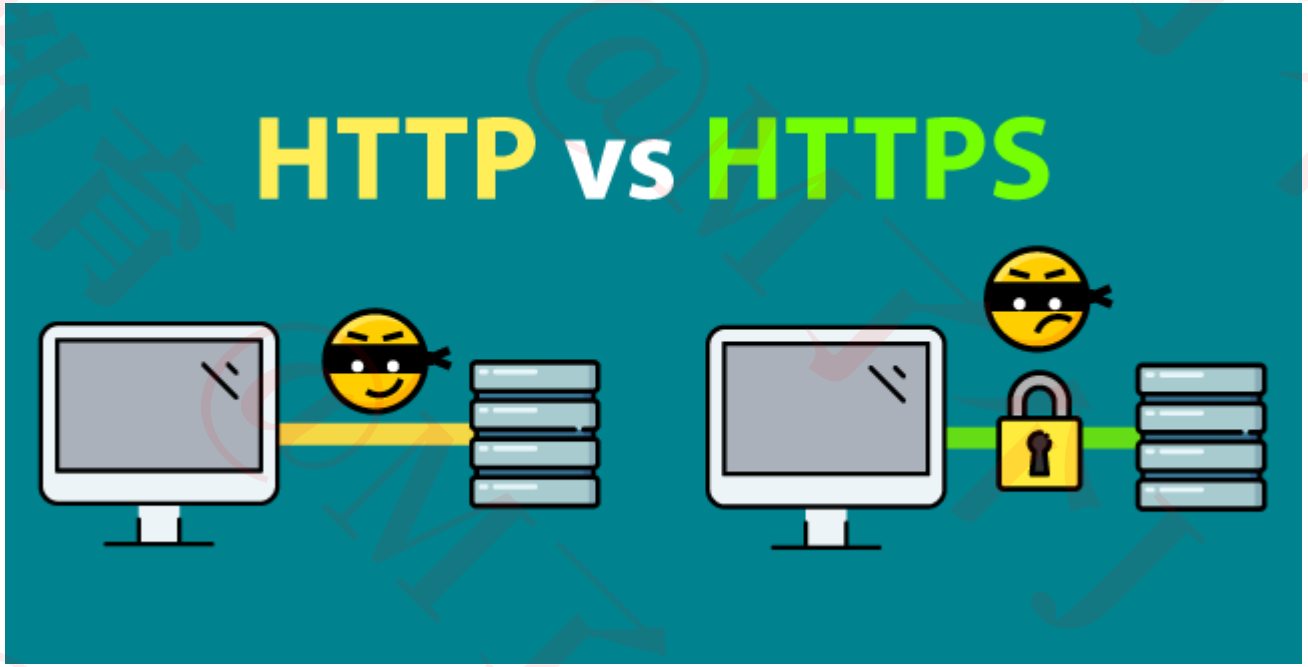
SSL/TLS

- HTTPS是在HTTP的基础上使用SSL/TLS来加密报文，对窃听和中间人攻击提供合理的防护



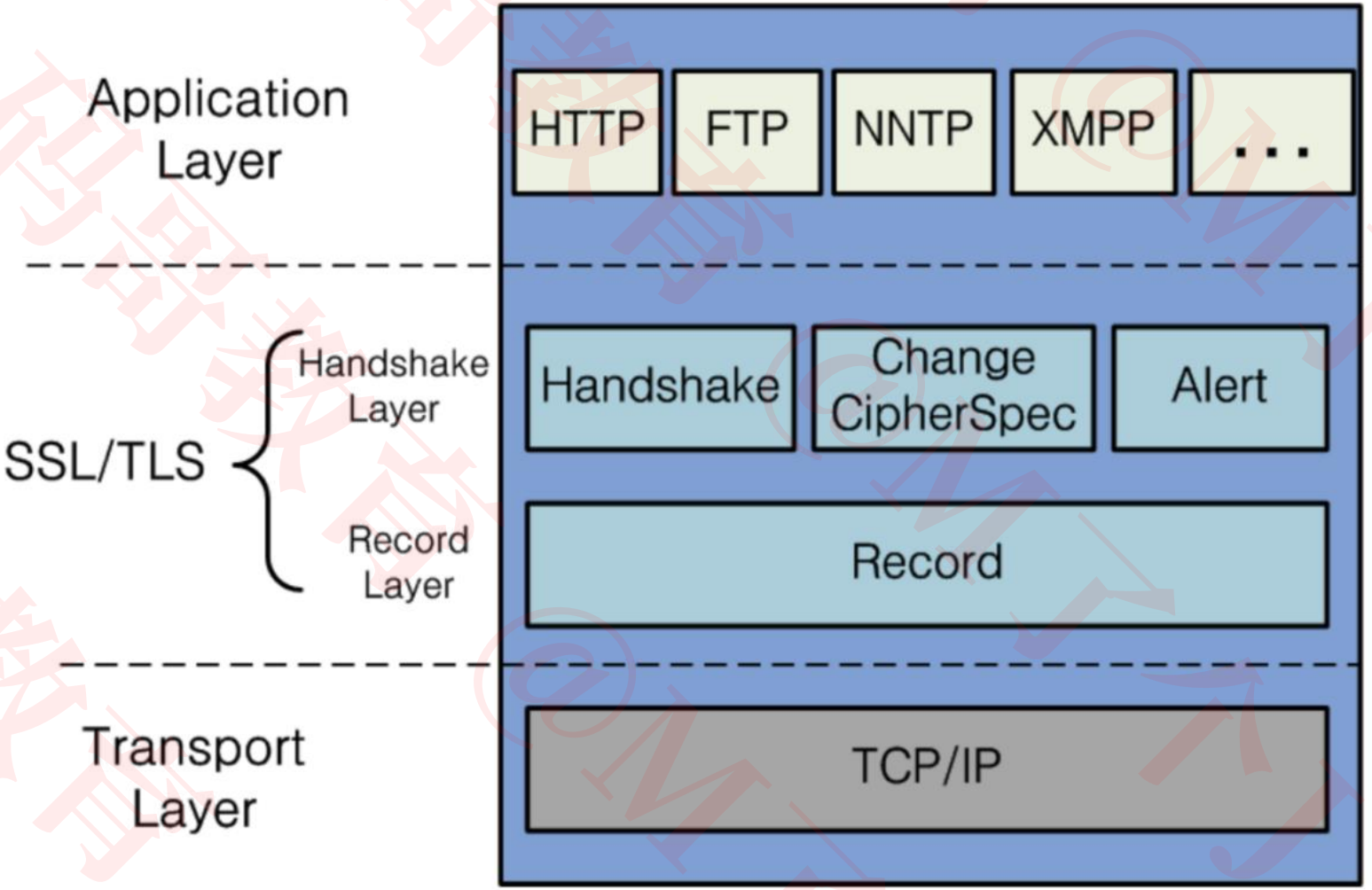
- SSL/TLS也可以用在其他协议上，比如
  - FTP → FTPS
  - SMTP → SMTPS

SSL/TLS

- TLS（**T**ransport **L**ayer **S**ecurity），译为：传输层安全性协议
  - 前身是SSL（**S**ecure **S**ockets **L**ayer），译为：安全套接层

- 历史版本信息
  - SSL 1.0：因存在严重的安全漏洞，从未公开过
  - SSL 2.0：1995年，已于2011年弃用（RFC 6176）
  - SSL 3.0：1996年，已于2015年弃用（RFC 7568）
  - TLS 1.0：1999年（RFC 2246）
  - TLS 1.1：2006年（RFC 4346）
  - TLS 1.2：2008年（RFC 5246）
  - TLS 1.3：2018年（RFC 8446）
  - ✓有没有发现：TLS的RFC文档编号都是以46结尾

SSL/TLS – 工作在哪一层



OpenSSL

- OpenSSL是SSL/TLS协议的开源实现，始于1998年，支持Windows、Mac、Linux等平台
  - Linux、Mac一般自带OpenSSL
  - Windows下载安装OpenSSL：https://slproweb.com/products/Win32OpenSSL.html

- 常用命令
  - 生成私钥：openssl genrsa -out mj.key
  - 生成公钥：openssl rsa -in mj.key -pubout -out mj.pem

- 可以使用OpenSSL构建一套属于自己的CA，自己给自己颁发证书，称为“自签名证书”