网络攻击与防御课程内容回顾

基础

- **CIA模型**
  - 机密性、完整性、可用性
  - **常见网络攻击影响了哪个方面?**

- **网络协议**
  - HTTP, **TLS, DNS**

- **虚拟化网络**
  - 三种模式：Bridge, NAT, host-only
  - 三种模式使用场景

常见网络攻击

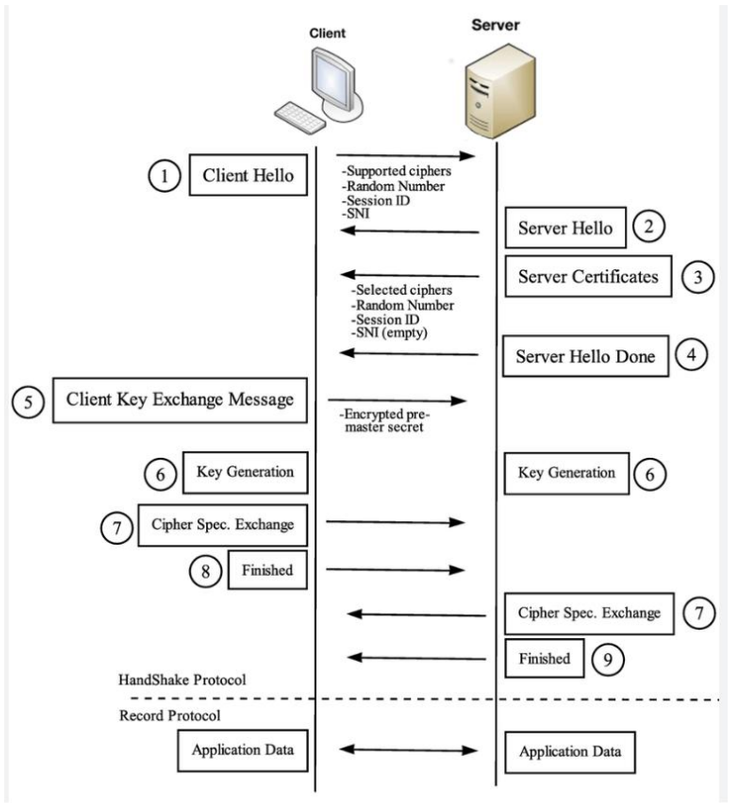
- 网络扫描
  - TCP SYN扫描、HTTP慢速攻击
- 口令破解
  - **Hash算法安全性**(MD5/SHA1/SHA256)
  - 哪种算法最安全、最不安全?
- 明文嗅探
  - 加密协议(SSL/TLS)，非加密协议，**TLS握手过程**

TLS协议(TLS 1.2)

- **TLS 1.2完整握手过程**

- **TLS重要握手包作用及关键字段**
  - Client Hello, Server Hello, Certificate

- 加密套件
  - 给定一个加密套件，使用的算法有哪些?



TLS 1.2参考资料

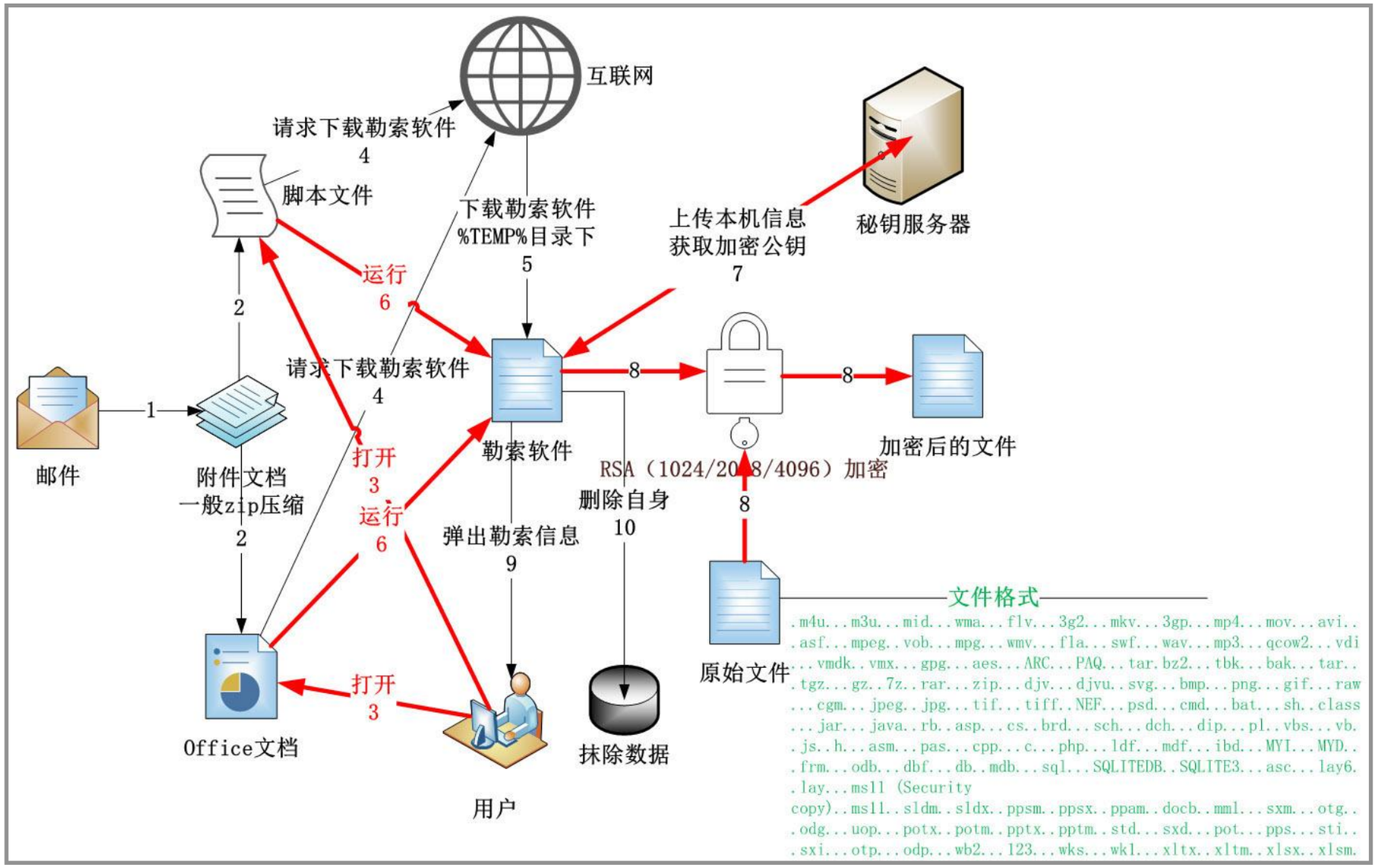
https://zhuanlan.zhihu.com/p/421446218

基于Wireshark抓包浅谈对HTTPS的理解（TLS、SSL、数字证书、数字签名）//重点读
https://juejin.cn/post/6970608722544427039

恶意代码

- 恶意代码分类与命名方法
- 病毒、木马、蠕虫、勒索软件
  - 各类恶意代码的工作原理、特点和区别
  - 典型恶意代码：熊猫烧香、WannaCry等

WannaCry工作流程

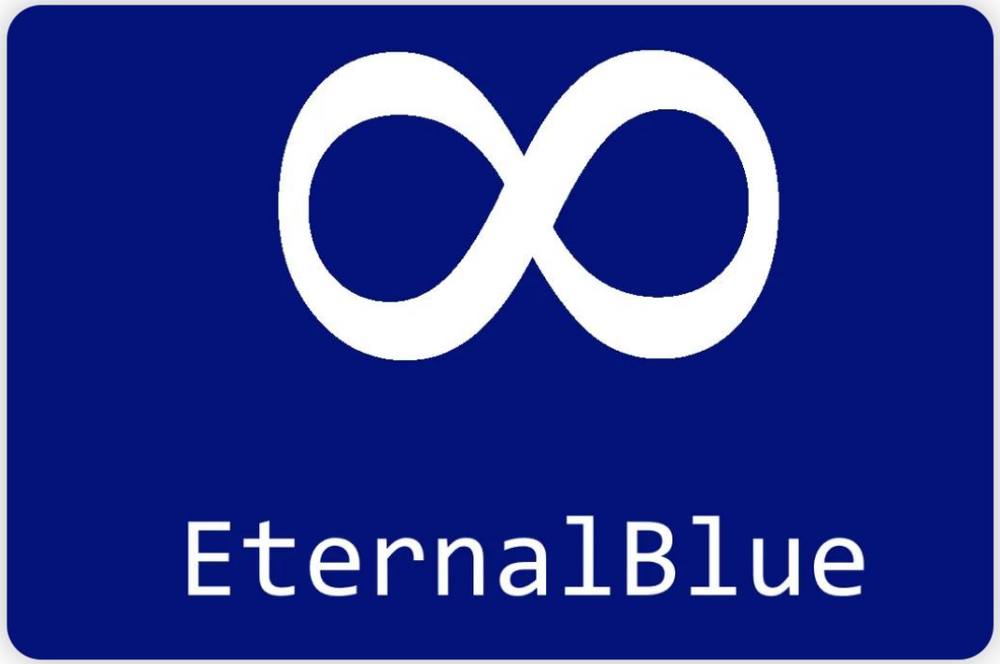


漏洞

- **常见权威漏洞库**
  - 中国国家信息安全漏洞库(CNNVD)、CVE等
- **CVE编号命名规则**
  - CVE–XXXX–YYYY
  - MS–XX–XX

永恒之蓝漏洞

- **CVE-2017-0144, MS17-010**
- **栈溢出漏洞**
- 受该漏洞影响软件
  - Windwos内核，SMB协议
  -



心血漏洞

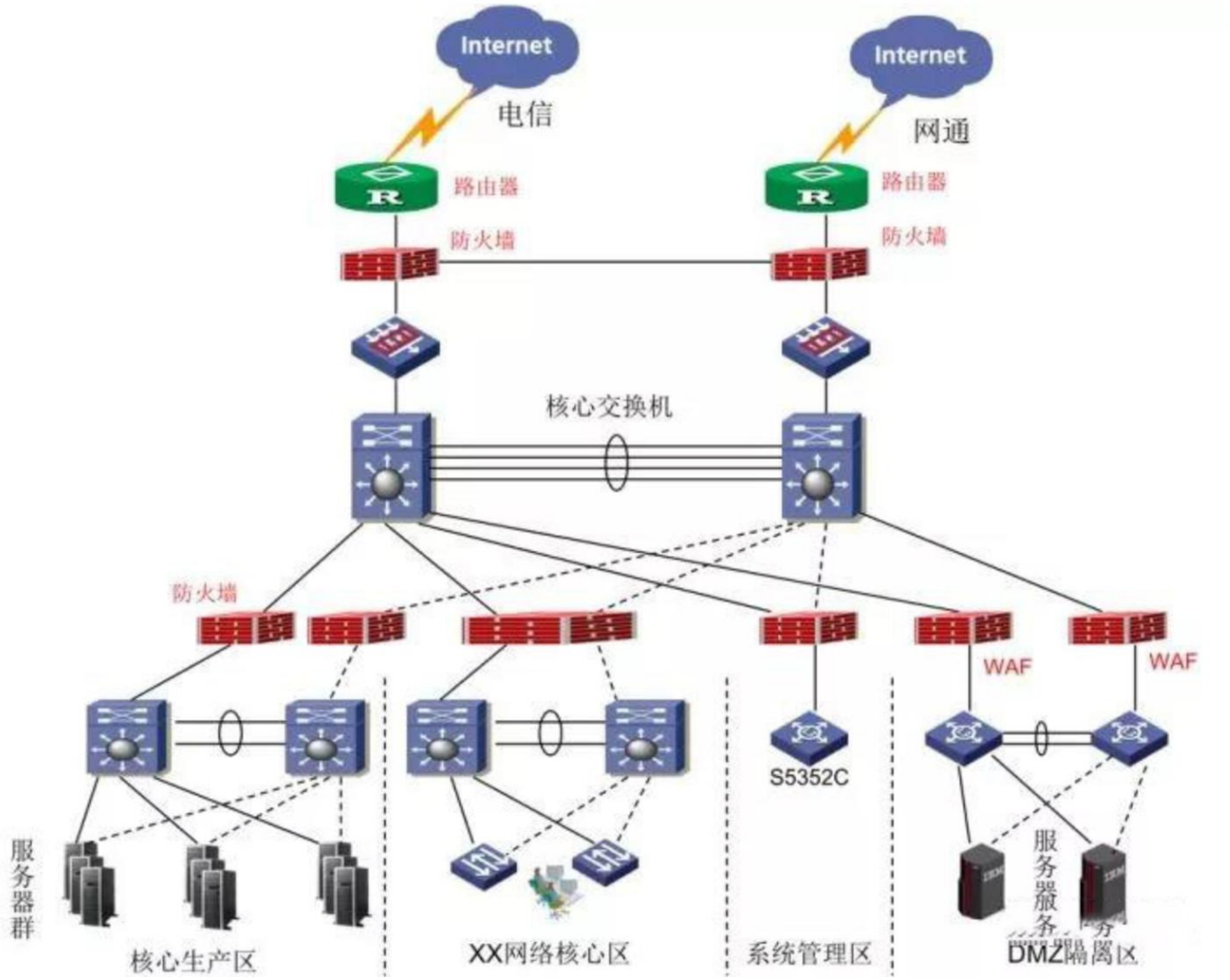
- CVE-2014-0160
- 受该漏洞影响软件
  - Openssl (1.01 version or before)

缓冲区溢出

- **函数调用与栈布局**
  - 参数入栈，开辟栈空间，函数返回
  - **对应汇编指令**
- **三种经典防御机制**
  - **Stack canary**，地址随机化(ASLR), DEP(栈不可执行)
  - **三种防御工作原理**(特别是canary)

企业网络结构

- **典型网络结构，南北向和东西向流量**
- **网络设备与安全设备部署位置**



防火墙

- **防火墙工作原理、使用场景**
- **部署位置**

IDS

- **工作原理**
- **部署位置**
- **防火墙和IDS区别**
  - 防火墙：串联设备，可阻断攻击，通常部署在防火墙后
  - IDS：旁路设备，只能监测攻击，通常从交换机引网络流量