计网安全框架

Markdown

```markdown
# 计算机网络安全（华中科技大学）

## 第一部分 网络安全基础
### 第1讲 引言
*   引言
    *   传统信息安全手段
        *   物理措施
        *   行政措施
    *   信息安全的两次重大变革
        *   计算机安全
        *   网络安全
*   网络安全现状
    *   中国互联网络发展现状
    *   CNCERT互联网安全威胁报告
    *   典型安全事件
        *   2010 震网病毒
        *   2015年乌克兰电网遭受攻击
        *   2021年滴滴出行App被下架
        *   2022年西北工业大学遭受网络入侵
        *   2023年武汉地震监测中心遭受网络入侵
        *   2024年黎巴嫩BP机爆炸事件
        *   2025年国家授时中心遭受网络攻击
        *   美国对华智能网联汽车禁令
*   网络安全威胁与防护措施
    *   信息安全的基本目标
        *   保密性
        *   完整性
        *   可用性
        *   合法使用
    *   基本安全威胁
        *   信息泄漏
        *   拒绝服务
        *   完整性破坏
        *   非法使用
    *   安全攻击的分类
        *   被动攻击
            *   窃听
            *   流量分析
        *   主动攻击
            *   伪装
            *   重放
            *   消息篡改
```

```
            *   拒绝服务
    *   网络攻击的常见形式
        *   口令窃取
        *   欺骗攻击
        *   缺陷和后门攻击
        *   认证失效
        *   协议缺陷
        *   信息泄漏
        *   指数攻击
        *   拒绝服务攻击
    *   网络安全防护措施
        *   物理安全
        *   人员安全
        *   管理安全
        *   媒体安全
        *   辐射安全
        *   生命周期控制
*   网络安全策略
    *   定义与等级
        *   安全策略目标
        *   机构安全策略
        *   系统安全策略
    *   授权
    *   访问控制策略
        *   基于身份（角色）的策略
        *   基于任务的策略
        *   多等级策略
        *   强制性访问控制策略
        *   自主性访问控制策略
    *   责任
*   网络安全体系结构
    *   研究目的
    *   应用目的
    *   开放系统互连(OSI)安全体系结构
        *   安全服务
            *   认证
            *   访问控制
            *   数据保密性
            *   数据完整性
            *   不可否认性
        *   安全机制
            *   加密
            *   数字签名
            *   访问控制
            *   数据完整性
            *   认证交换
            *   流量填充
            *   路由控制
```

```
            *   公证
*   五 网络安全模型
    *   安全模型
        *   信息安全模型
        *   信息安全模型的作用
    *   安全理论模型
        *   P2DR2模型
            *   Policy (安全策略)
            *   Protection (防护)
            *   Detection (检测)
            *   Response (响应)
            *   Restore (恢复)
    *   网络安全模型—实例
        *   网络传输安全模型
        *   网络访问安全模型
```

Plain Text

```
第2讲 Internet协议的安全性
├── 2.1 网络层协议
│   ├── 01 IP协议的安全性
│   │   ├── 安全问题
│   │   │   ├── IP地址欺骗攻击 (源/目的地址欺骗)
│   │   │   ├── IP定向广播攻击
│   │   │   ├── 数据监听与窃听 (未加密)
│   │   │   ├── 数据篡改 (仅首部校验)
│   │   │   ├── IP源路由欺骗
│   │   │   └── IP分片攻击
│   │   │       ├── 大包分片攻击 (Ping of Death, Jolt2)
│   │   │       ├── 极小碎片攻击 (Tiny Fragment)
│   │   │       ├── 分片重叠攻击 (Teardrop)
│   │   │       └── 分片DoS攻击
│   │   └── 防范措施
│   │       ├── 地址欺骗：抛弃基于地址的信任，进行包过滤
│   │       ├── 定向广播：路由器关闭定向广播转发
│   │       ├── 监听/篡改：采用加密和完整性校验机制 (如IPSec)
│   │       ├── 源路由：路由器关闭源路由功能
│   │       └── 分片攻击：强制丢弃分片、路径MTU探测、不分片标记、先重组再过滤
│   ├── 02 ARP协议的安全性
│   │   ├── 安全问题：ARP缓存中毒 (ARP欺骗/重定向)
│   │   │   └── 攻击方式：使用伪造的ARP请求/响应/免费ARP
│   │   └── 防范措施
```

```
25 │   │       ├── 设置静态ARP项
26 │   │       └── 交换机配置802.1x协议进行身份验证
27 │   ├── 03 ICMP协议的安全性
28 │   │   ├── 安全问题
29 │   │   │   ├── ICMP DoS攻击（如Smurf攻击）
30 │   │   │   └── ICMP重定向攻击
31 │   │   └── 防范措施：必要的ICMP限制（平衡服务与安全），如允许PING、traceroute、路径MTU，阻止其他类型
32 │   └── 04 路由协议的安全性
33 │       ├── 涉及协议：RIP, OSPF, BGP
34 │       ├── 安全问题
35 │       │   ├── 缺乏认证，易受欺骗（如伪造路由更新）
36 │       │   ├── 协议设计缺陷（如RIP使用UDP）
37 │       │   └── BGP缺乏可信路由认证
38 │       └── 防护措施
39 │           ├── 配置被动接口、访问控制列表（ACL）
40 │           ├── 增加路由验证机制（如MD5认证）
41 │           ├── 使用具有防火墙功能的路由器
42 │           └── 考虑使用IS-IS协议（防外部注入）
43 ├── 2.2 运输层协议
44 │   ├── 01 TCP协议的安全性
45 │   │   ├── 安全问题
46 │   │   │   ├── SYN Flood攻击（连接建立阶段）
47 │   │   │   ├── TCP序列号攻击与会话劫持（数据阶段，缺乏加密认证）
48 │   │   │   └── 针对拥塞机制的攻击（数据阶段）
49 │   │   └── 防范措施
50 │   │       ├── SYN Flood防御：SYN Proxy, SYN Cache, SYN Cookie, Safe Reset
51 │   │       ├── 序列号攻击防御：采用更安全的序列号生成算法（如RFC 1948），上层加密
52 │   │       └── 拥塞攻击防御：网关检测异常流量
53 │   └── 02 UDP协议的安全性
54 │       ├── 安全问题：UDP Flood攻击、易受欺骗攻击
55 │       └── 防护措施：对源地址和端口特别小心，重要应用需认证
56 └── 2.3 应用层协议
57     ├── 01 DHCP协议
58     │   ├── 安全问题：假冒DHCP Server、中间人攻击、DoS攻击（耗尽IP地址）
59     │   └── 防范措施：交换机端口信任与802.1x认证；记录并检查MAC地址
60     ├── 02 域名系统（DNS）
61     │   ├── 安全问题：DNS欺骗、缓存中毒、重定向
62     │   └── 防范措施：避免基于名称的认证；采用DNSSec
63     ├── 03 FTP协议
64     │   ├── 安全问题
65     │   │   ├── 明文传输
66     │   │   ├── 两种数据连接模式（PORT/PASV）带来防火墙策略复杂
67     │   │   ├── FTP反弹攻击
68     │   │   ├── 用户权限问题
69     │   │   └── 匿名FTP风险
70     │   └── 防范措施
71     │       ├── 使用SFTP（SSH）替代
```

```
    |       ├── 限制使用PASV模式，规范PORT命令
    |       ├── 遵循最小权限原则
    |       └── 严格控制匿名访问
    ├── 04 远程登录 (Telnet)
    |   ├── 安全问题：明文传输、弱认证、易被会话劫持
    |   └── 替代方案：使用SSH (支持加密和强认证)
    └── 05 电子邮件安全性
        ├── 相关协议
        |   ├── SMTP (发送)
        |   ├── POP3/IMAP (收取)
        |   └── MIME (多用途邮件扩展)
        ├── 安全问题
        |   ├── SMTP：明文、无源验证、命令滥用 (VRFY, EXPN, TURN)、邮件炸弹、垃圾邮件、开放中继
        |   ├── POP3：明文传输 (USER命令)、APOP可能被字典攻击、常以root运行
        |   └── MIME：类型标识错误或缺失、分部攻击、病毒传播载体
        └── 安全增强协议
            ├── PEM
            ├── PGP
            └── S/MIME (商业环境首选)
```

Markdown

```
# 网络扫描与网络监听（第三讲）

## 一、网络扫描
### 01 网络扫描概述
- **定义**：向指定对象发送特定网络报文，根据反馈判断、评估对象的相关信息和状态的网络技术。
- **目的**：发现指定目标的潜在漏洞。
- **与系统安全扫描对比**：
  - **网络安全扫描**：主动式策略，基于网络，模拟攻击行为，可能对系统造成破坏。
  - **系统安全扫描**：被动式策略，基于主机，检查系统设置、口令等，不会对系统造成破坏。
- **扫描策略**：
  - **主动扫描**：连续端口扫描，源地址一致，时间间隔短。
  - **隐蔽扫描**：非连续端口扫描，源地址不一致，时间间隔长且无规律。
- **使用场景**：
  - **安全运维人员**：漏洞扫描、渗透测试。
  - **恶意黑客**：入侵攻击。
- **常用工具**：Nmap、X-Scan、Nessus。

### 02 主机扫描
- **目的**：确定目标网络上的主机是否可达，映射网络拓扑结构。
- **传统技术**：
```

```
  - ICMP Echo (ping) 扫描：发送ICMP Echo Request，等待Reply。
  - ping sweep扫描：使用ICMP ECHO轮询多个主机（如fping）。
  - 广播ICMP扫描：向广播地址发送ICMP ECHO报文（仅适用于Unix主机）。
  - 非ECHO的ICMP扫描：使用TimeStamp Request、Address Mask Request等（如hping3）。
- **高级技术**：
  - ICMP错误报文探测：利用异常IP包头或错误数据分片触发ICMP错误消息。
  - traceroute探测路径路由器：发送TTL递增的UDP报文。
  - 超长包探测路由器：构造长度超过MTU且设置DF标志的数据包。
- **对策**：使用检测工具、设置ICMP过滤规则、使用IDS。

### 03 端口扫描
- **目的**：确定目标主机开放的TCP/UDP端口，关联服务进程。
- **类型**：
  - **开放扫描**：TCP Connect扫描（调用connect()函数）。
  - **半开扫描**：TCP SYN扫描（发送SYN包，根据SYN|ACK或RST回复判断）。
  - **隐蔽扫描**：TCP FIN扫描（发送FIN包，根据RST回复判断）。
- **UDP端口扫描**：发送UDP数据包，根据ICMP端口不可达错误判断。
- **对策**：使用状态检测防火墙、禁止不必要的服务。

### 04 操作系统探测
- **目的**：探测目标主机的操作系统类型及版本。
- **探测方式**：
  - **主动探测**：发送特殊包并监控应答，速度快、可靠性高，但易被发现。
  - **被动探测**：通过Sniff收集数据包分析，速度慢、可靠性低，但隐蔽性好。
- **技术路线**：
  - **应用层探测**：通过telnet、SSH等服务的banner信息识别。
  - **TCP协议栈指纹探测**：利用IP TTL、TCP Window-size、TCP ISN等差异识别。
- **对策**：及时打补丁、修改OS源代码改变特征、禁止不必要的服务。

### 05 应用服务探测
- **目的**：识别服务软件类型和版本，发现特定漏洞。
- **步骤**：
  - **服务识别**：
    - 基于端口识别（如21/ftp、22/SSH、80/HTTP）。
    - 基于Banner信息识别（建立TCP连接获取Welcome Banner）。
    - WEB网站指纹识别（服务器类型、容器、脚本类型、数据库类型）。
  - **漏洞扫描**：
    - **原理扫描**：构造漏洞利用数据包，根据响应判断漏洞存在（误报率低）。
    - **版本扫描**：基于Banner信息查询漏洞数据库（误报率高）。
- **对策**：禁止不必要的服务、正确配置并升级服务软件、修改应用源代码改变banner特征。

## 二、网络监听
### 01 网络监听概述
- **概念**：监视网络流量、状态、数据，捕获并分析传输的数据。
- **用途**：
  - **网络管理员**：监视网络状态、定位故障、作为入侵检测数据源。
  - **网络程序员**：分析程序网络行为、调试程序。
```

```
  - **攻击者**：窃取敏感数据、收集网络信息。
- **威胁**：
  - **敏感信息泄露**：明文协议（如telnet、FTP、POP3）传输的口令等被窃取。
  - **后续入侵准备**：获取局域网IP、MAC、拓扑结构、应用信息。

### 02 网络监听原理
- **网卡工作模式**：
  - **普通模式**：只接收目的MAC为自身或广播的帧。
  - **混杂模式**：接收所有帧，可实现监听。
- **总线式以太网监听**：同轴电缆或集线器环境下，所有站点接收广播帧。
- **交换式以太网监听**：
  - **正常情况**：交换机根据MAC表转发，无法监听。
  - **攻击手段**：MAC Flooding、ARP欺骗、ICMP重定向。
- **广域网光纤分流监听**：通过分光器镜像流量。
- **WIFI监听**：利用802.11安全缺陷（如WEP破解、假冒热点）。
- **协议分析**：逐层解析数据包（链路层→网络层→传输层→应用层），提取信息。

### 03 网络监听防范
- **监听发现**：
  - 检测网卡是否处于混杂模式。
  - 通过ping测试或发送大量不存在MAC地址的包判断。
- **防范措施**：
  - **网络分段**：逻辑或物理隔离非法用户与敏感资源。
  - **交换机替代集线器**：减少单播包被监听的风险。
  - **划分VLAN**：控制广播域范围。
  - **静态设置**：静态ARP、MAC-端口映射（灵活性差）。
  - **加密技术**：使用SSH、HTTPS、IPSec等加密通信。

### 04 网络监听工具
- **tcpdump**：命令行抓包工具，基于libpcap，需root权限。
- **Wireshark**：图形化网络数据包分析器，前身为Ethereal。

### 05 网络监听开发
- **基于原始套接字**：使用raw socket绕过协议栈，需自行设置网卡为混杂模式。
- **基于PCAP库**：使用libpcap（Linux）/winpcap/npcap（Windows）开发跨平台监听程序。
- **基于内核协议栈**：利用Netfilter子系统注册HOOK回调函数处理报文。
```

Markdown

```
# 防火墙技术（第四讲）

## 一、防火墙概述
1. **防火墙的概念**
```

    - 原义：建筑中防止火灾蔓延的墙体
    - 引申：网络安全边界过滤控制机制
2. **基本要求**
    - 必经之路
    - 授权放行
    - 入侵免疫
3. **动作**
    - 允许（ACCEPT）
    - 拒绝（REJECT）：有反馈
    - 丢弃（DROP）：无反馈
4. **默认策略**
    - 默认允许
    - 默认拒绝/丢弃：更安全
5. **分类**
    - 按形态：硬件防火墙、软件防火墙
    - 按保护对象：网络防火墙、个人防火墙
6. **性能指标**
    - 吞吐量（带宽）
    - 时延（快慢）
    - 丢包率（稳定性）
    - 并发连接数（容量）
7. **作用**
    - 网络安全中心“扼制点”
    - 集中强化安全策略
    - 监视网络安全性
8. **局限性**
    - 不能防范不经过它的攻击
    - 不能防范来自内部网络的攻击
    - 不能防范策略配置不当引起的威胁
    - 不能防范物理接触破坏
    - 不能防范对自身漏洞的攻击
9. **安全区域**
    - Local（防火墙自身）
    - Trust（受信任区域）
    - DMZ（非军事化区域）
    - Untrust（不受信任区域）
    - 安全级别：Local > Trust > DMZ > Untrust
10. **工作模式**
    - 路由模式（网关模式）
    - 透明模式（桥模式）
    - 混合模式

二、包过滤防火墙
1. **基本概念**
    - 处理对象：数据包
    - 最基础的防火墙技术
2. **工作机制**
    - 在网络层和传输层检查数据包

3. **包过滤规则**
   - 组成：条件、动作
   - 检查原则：顺序逐条检查、首条命中、每个数据包单独检查
   - 检查对象：源/目的IP地址、传输层协议、源/目的端口、TCP ACK标志、IP分片
   - TCP ACK控制连接方向
   - 规则制定策略：按地址、服务、连接方向、时间、用户过滤，日志记录
   - 设置步骤：建立安全策略 → 转化为逻辑表达式 → 重写并设置规则
4. **配置实例**
   - 网络拓扑与安全策略
   - 逻辑表达式与规则列表
5. **优缺点**
   - 优点：对网络性能影响小、成本低、对用户透明
   - 缺点：规则配置复杂、易受IP欺骗、缺乏状态感知能力
6. **Linux Netfilter架构**
   - Netfilter框架与Hook点
   - Hook函数返回值

三、状态检测防火墙
1. **包过滤的问题**
   - 效率低：规则顺序匹配，数据包重复检查
   - 易用性差：需配置双向规则，动态端口难处理
   - 安全性低：只检查首部，不检查数据
2. **解决思路—状态检测**
   - 建立连接状态表
   - 效率：首包查规则表建连接，后续包查状态表
   - 易用性：单向配置规则，双向检查状态表；自动处理动态端口
   - 安全性：追踪连接数据流，可检查数据
3. **状态检测表（连接表）**
   - 包含所有通过防火墙的连接信息
   - 信息：源/目的IP、协议类型、传输层信息、连接状态、超时时间
4. **TCP状态检测**
   - 基本流程与简化TCP状态机
5. **非TCP状态检测**
   - UDP、ICMP建立虚拟连接
   - 虚拟UDP状态机
6. **连接表的组织**
   - 非线性数据结构（hash表），快速匹配
7. **连接的老化和长连接**
   - 老化时机：TCP正常/异常超时，UDP/ICMP无通信超时
   - 特殊情况：FTP大文件、数据库长间隔查询 → 长连接或连接关联
8. **多通道协议支持**
   - 以FTP为例：监视控制连接，自动创建预连接
9. **优缺点**
   - 优点：速度更快、安全性提升、配置更简单、对用户透明
   - 缺点：对病毒防护不足，存在内网信息泄露风险

四、应用代理防火墙
1. **应用代理的提出**

```
    - 面向数据包技术的不足：内核协议栈功能受限，数据直传有风险
    - 解决思路：数据过滤提升到应用层，断开客户端与服务器的直接连接
2. **工作机制**
    - 客户端与服务器代理交互，服务器代理与客户端代理交互
3. **透明代理**
    - 客户端无感知，协议栈包过滤配合实现
4. **应用代理的功能**
    - 基本访问控制
    - 应用数据检查：协议符合性、用户合法性、深度内容检查、数据对象缓存
5. **优缺点**
    - 优点：按协议内容过滤、可调用其他安全功能、屏蔽内网信息
    - 缺点：只支持特定服务（可扩展性不高）、性能较低

## 五、防火墙技术发展
1. **发展历程**
    - 包过滤防火墙（1989）
    - 基于状态检测
    - 基于ASIC
    - UTM统一威胁管理（2004）
    - 多核+分布式架构
    - NGFW下一代防火墙（2008）
    - AI防火墙（2009之后）
2. **统一威胁管理（UTM）**
    - 定义：集成多种安全功能的统一管理平台
    - 功能：FW、IDS、IPS、AV等串行连接
    - 特点：整合应用网关和IPS
    - 优点：成本降低、降低工作强度和技术复杂度
    - 缺点：模块串联检测效率低，性能消耗大
3. **下一代防火墙（NG Firewall）**
    - 全面应对应用层威胁的高性能防火墙
    - 工作范围：2-7层
    - 核心处理：会话管理、应用识别、内容检测
    - 功能：FW、IDS、IPS、AV、WAF
    - 优点：增加Web应用防护，并行处理机制效率更高，性能更强，管理更高效
4. **WEB应用防火墙（WAF）**
    - 工作范围：应用层（7层）
    - 目的：防止基于应用层的攻击影响Web应用系统
    - 主要技术原理：代理服务、特征识别、算法识别
    - 常见功能：网络层访问控制、HTTP协议校验、防篡改、防注入等
```

Markdown

```
# 入侵检测技术（第五讲）

```

```
## 一、 入侵检测系统概述
### 1.1 IDS发展简史
-
1980年代初：开山之作《Computer Security Threat Monitoring and Surveillance》
- 1984~1986：IDES (入侵检测专家系统)
- 1990：NSM (Network Security Monitor)
- 1999：CIDF (Common Intrusion Detection Framework)

### 1.2 IDS工作流程
1. 信息收集
    - 系统和网络日志
    - 网络流量
    - 非正常的目录和文件改变
    - 非正常的程序执行
2. 信息分析
    - 模式匹配
    - 统计分析
    - 完整性分析
3. 安全响应
    - 记录日志
    - 告警信息
    - 阻断攻击

### 1.3 IDS分类
1. 依据检测方法
    - 异常检测模型 (Anomaly Detection)
    - 误用检测模型 (Misuse Detection)
2. 依据信息来源
    - 基于主机的入侵检测 (HIDS)
    - 基于网络的入侵检测 (NIDS)
    - 混合型
3. 依据体系结构和运行方式
    - 集中式 / 分布式
    - 脱机分析型 / 联机分析型

### 1.4 IDS评价标准
- 功能、性能、可用性
- 误报率 (false positive)
- 漏报率 (false negative)

## 二、 IDS原理和主要方法
### 2.1 异常检测
- 假设前提：入侵行为是异常活动的子集
- 用户轮廓：行为参数及其阈值的集合
- 检测过程：量化 → 监控 → 修正 → 判定 → 比较
- 特点：能检测未知入侵，但误报率高
- 具体方法：
  - 统计分析异常检测
```

```
    - 神经网络异常检测
    - 模式预测、数据挖掘、马尔可夫过程、时间序列分析等

### 2.2 误用检测
- 假设前提：入侵行为都有可被检测到的特征
- 检测过程：监控 → 判定 → 提取特征 → 匹配
- 特点：误报率低、漏报率高
- 具体方法：
    - 专家系统误用检测
    - 特征分析误用检测 (事件序列、数据模板)
    - 模型推理误用检测

## 三、 NIDS、HIDS、DIDS
### 3.1 基于网络的入侵检测系统 (NIDS)
- 特点：成本低、实时检测、独立于操作系统
- 关键技术：
    - IP碎片重组技术
    - TCP流重组技术
    - TCP状态检测技术
    - 网络协议分析技术
    - 零复制技术
    - 蜜罐/蜜网技术
- 实例：SNORT
- 部署位置：
    - DMZ区
    - 外网入口
    - 内网主干
    - 关键子网

### 3.2 基于主机的入侵检测系统 (HIDS)
- 用于保护单台主机
- 检测内容：
    - 网络连接检测
    - 主机系统检测 (日志系统、文件系统、进程记录)
- 关键技术：文件和注册表保护、网络安全防护、WEB保护、文件完整性分析
- 实例：TripWire
- 与NIDS对比：
    - NIDS：侦测速度快、视野宽、隐藏性好
    - HIDS：检测准确度高、视野集中、对加密/交换环境适用

### 3.3 分布式入侵检测系统 (DIDS)
- 组成构件：
    - 数据采集构件
    - 通信传输构件
    - 入侵检测分析构件
    - 应急处理构件
    - 用户管理构件
- 管理功能：
```

```
    - 日志检索
    - 探测器管理
    - 规则管理
    - 日志报表
    - 用户管理

## 四、 IDS发展趋势
### 4.1 IDS面临的问题
- 攻击手段复杂化、加密化
- 网络流量增长导致分析难度大
- 不适当的自动响应机制
- 对IDS自身的攻击
- 交换网络限制了数据可见性

### 4.2 IDS发展方向
- 宽带高速实时检测技术
- 大规模分布式检测技术
- 数据挖掘技术
- 更先进的检测算法
- 入侵响应技术
- 计算机免疫技术
- 神经网络技术
- 遗传算法

### 4.3 入侵防御系统（IPS）
- 产生背景：应用层攻击增多，IDS无法直接阻断，防火墙联动有滞后
- 与IDS关系：技术同源，但部署方式和设计出发点不同
- 部署方式对比：IPS在线部署，IDS旁路部署
- 设计出发点对比：IPS要求无误报、实时、不影响业务；IDS要求无漏报、准实时
- 解决的问题：
    - IDS：总体威胁趋势分析、流量及连接分析、安全事件分析
    - IPS：阻拦已知攻击、提供虚拟补丁、速率/流量控制、行为管理

### 4.4 扩展检测和响应（XDR）
- 发展史：IDS → SIEM → SOAR → XDR
- 模型架构：集成终端、网络、云等多维度安全组件，具备大数据处理、机器学习、自动化编排能力
- 核心优势：
    - 高质量数据集成（统一广泛的数据、事件上下文信息）
    - 强大的算法分析能力（人工智能检测、告警关联降噪）
- 终端APT攻击检测：
    - 传统方法问题：缺乏上下文、告警疲劳
    - 数据组织形式：终端溯源图（有向无环图记录系统实体和事件）
    - 检测算法：基于白名单（行为建模）和基于黑名单（如HOLMES）的方法
    - 现有问题：运行成本高、告警质量差、语义鸿沟
```

Markdown

```markdown
# VPN技术（第六讲）
## 一、VPN概述
### 1.1 VPN的概念
- 虚拟专用网 (Virtual Private Network)
- 将物理上分布在不同地点的网络通过公用网络连接而构成逻辑上的虚拟子网
### 1.2 VPN的特点
- 费用低
- 安全保障
- 服务质量和灵活性保证 (QoS)
- 可扩充性
- 可管理性
### 1.3 VPN的分类
- Access VPN (远程访问VPN)
- Intranet VPN (企业内部VPN)
- Extranet VPN (企业扩展VPN)
### 1.4 VPN的关键技术
- 隧道技术
- 密码技术
- 密钥管理技术
- 身份认证技术
- 访问控制技术
### 1.5 隧道协议与VPN
- 主要隧道协议
  - 第2层隧道协议：PPTP、L2TP、L2F
  - 第3层隧道协议：IPSec、GRE
  - 第4层隧道协议：SSL、TLS
## 二、IPSec VPN
### 2.1 IP安全概述
- IPSec (IP Security)
- 弥补IPv4在协议设计时缺乏安全性考虑的不足
### 2.1.1 IPSec安全体系结构
- IPSec协议族
- 主要协议：AH、ESP、IKE
- 体系结构图
### 2.1.2 IPSec的功能
- 实现VPN通信
- 保证数据来源可靠
- 保证数据完整性
- 保证数据机密性
### 2.1.3 IPSec核心数据
- SA (安全关联)
- SAD (安全关联数据库)
- SP (安全策略)
- SPD (安全策略数据库)
### 2.1.4 IPSec工作模式
```

```
- 传输模式 (Transport Mode)
- 隧道模式 (Tunnel Mode)
### 2.2 IPSec工作原理
- 出站处理
- 入站处理
### 2.3 IPSec中的主要协议
- AH协议 (认证)
- ESP协议 (加密)
- IKE协议 (密钥管理)
### 2.4 IPSec VPN其他
- 构成模块
- VPN的部署
- IPSec VPN的缺陷
- IPSec的实现 (如FreeS/WAN, Openswan, strongSwan)
## 三、TLS VPN
### 3.1 SSL VPN概述
- SSL VPN / TLS VPN
- 特点：无需客户端软件，使用浏览器即可访问
### 3.2 TLS协议原理
- TLS协议组成
  - 握手协议
  - 记录协议
  - 告警协议
### 3.2.1 TLS握手协议
- 功能
- 过程
  - 无客户端认证的全握手过程
  - 有客户端认证的全握手过程
  - 会话恢复过程
### 3.2.2 TLS记录协议
- 功能
- 报文格式
### 3.2.3 TLS告警协议
- 功能
### 3.3 SSL VPN的实现方式
- 基于Web代理的SSL VPN
- 基于端口转发的SSL VPN
- 基于隧道的SSL VPN
### 3.4 SSL VPN与IPSec VPN的比较
- 身份验证
- 加密
- 全程安全性
- 可访问性
- 费用
- 安装
- 用户易用性
- 支持的应用
- 用户群体
```

```
- 可伸缩性
- 穿越防火墙
## 四、总结
- VPN的概念、分类
- VPN的关键技术
- IPSec VPN
  - 主要协议（AH，ESP，IKE）
  - 运行模式（隧道模式，传输模式）
  - 核心术语（SA，SAD，SP，SPD）
- SSL VPN
  - 特点
  - TLS协议（握手，告警，记录）
  - 实现机制（基于Web，端口转发，隧道方式）
```

Markdown

```
# 身份认证（第7讲）

## 01 身份认证概述
- **7.1 身份认证概述**
  - 必要性
    - 防止身份欺诈
    - 通信和数据系统的安全性
    - 计算机的访问和使用
    - 安全区的出入
  - 目标：实现安全、准确、高效和低成本的数字化认证
  - 认证与授权
    - 认证（Authentication）：证明一个对象的身份
    - 授权（Authorization）：决定把什么特权附加给该身份
- **7.1.2 身份证明系统的组成**
  - 示证者：出示证件的人
  - 验证者：检验证件的合法性和正确性
  - 攻击者：窃听并伪装示证者骗取验证者的信任
  - 可信者（必要时）：参与纠纷调解
  - 认证类型
    - 实体认证：对通信主体的认证，识别通信双方的真实身份，防止假冒
    - 消息认证：对通信数据的认证，验证收到的消息确实是来自真正的发送方且未被修改的消息
- **7.1.2 身份证明系统的要求**
  - 1. 最大可能正确识别合法示证者
  - 2. 不具有可传递性
  - 3. 最大可能防止攻击者伪装欺骗
  - 4. 计算有效性
  - 5. 通信有效性
  - 6. 秘密参数能安全存储
```

```
  - 7. 交互识别
  - 8. 第三方实时参与
  - 9. 第三方的可信性
  - 10. 可证明安全性
- **7.1.3 身份证明的基本分类**
  - 1. 身份验证 (Identity verification)：你是否是你所声称的你?
  - 2. 身份识别 (Identity recognition)：我是否知道你是谁?
- **7.1.4 实现身份证明的基本途径**
  - 所知：个人掌握的知识，如口令、秘密
  - 所有：个人所具有的东西，如身份证、护照等
  - 个人特征：人所具有的特征，如指纹、笔迹等
  - 通过这三者之一或组合实现
  - 服务质量评价指标：拒绝率 (FRR)、漏报率 (FAR)
- **7.1.7 身份证明系统的设计**
  - 美国国家标准局 (NBS) 的自动身份验证技术的评价指南提出了12个需要考虑的问题：
    - 1. 抗欺诈能力
    - 2. 伪造容易程度
    - 3. 对设陷的敏感性
    - 4. 完成识别的时间
    - 5. 方便用户
    - 6. 识别设备及运营的成本
    - 7. 设备使用的接口数目
    - 8. 更新所需时间和工作量
    - 9. 所需计算机系统的处理工作
    - 10. 可靠性和可维护性
    - 11. 防护器材费用
    - 12. 分配和后勤支援费用
  - 主要考虑
    - 设备系统强度
    - 用户可接受性
    - 系统成本

## 02 口令认证系统
- **7.2.1 口令认证系统概述**
  - 定义：根据已知事物验证身份的方法，被广泛使用
  - 选择原则：易记；难以猜中或发现；能抵御蛮力破解攻击
  - 防止泄露的措施：
    - 个人身份和口令用软件加密
    - 采用通行短语 (Pass Phrases) 代替口令，通过密钥碾压 (Key Crunching) 技术生成较短的随机性密钥
  - 口令分发系统的安全性
    - 通常采用邮寄方式
    - 银行系统通常采用夹层信封
  - 使用口令时的注意事项
    - 防止别人骗取口令
    - 系统常常限定尝试输入口令的次数
    - 有时需双向验证，用户也要检验系统口令
- **7.2.2 一种双方互换口令的安全验证方法**
```

```
    - 甲乙分别以P、Q作为护字符
    - 为验证，双方彼此知道对方的口令，并通过一个单向函数f进行响应
- **7.2.3 口令的控制措施**
    - 1. 系统消息
    - 2. 限制试探次数
    - 3. 口令有效期
    - 4. 双口令系统
    - 5. 最小长度
    - 6. 封锁用户系统
    - 7. 根口令的保护
    - 8. 系统口令的生成
- **7.2.3 口令的检验**
    - 口令的检验
        - 用户选择口令，程序检验，若易于猜中须重新选择
        - 可猜中性与安全性之间折中
    - 易猜测的口令
        - 使用用户名或其变换形式作为口令
        - 使用自己或者亲友的生日作为口令
        - 使用常用的英文单词作为口令
        - 使用5位或5位以下的字符作为口令
    - 安全的口令
        - 位数 > 6位
        - 大小写字母混合
        - 字母与数字混合
        - 口令有字母、数字以外的符号
- **7.2.4 口令的安全存储**
    - 一般方法
        - 以口令加密方式存储
        - 存储口令的单向杂凑
    - UNIX系统中的口令存储
        - 口令为8个字符：7bit ASCII码 (56bit) + 12bit填充 (用户输入口令的时间)
        - 第一次输入64bit全0进行加密，再以第一次的加密结果为输入，迭代25次
        - 最后一次变换成11个字符作为口令密文
        - 检验时用户发送ID和口令
    - 用智能卡令牌 (Token) 产生一次性口令
        - 本质上是由一个随机数生成器产生的，可以由安全服务器用软件生成
        - 一般用于第三方认证
        - 即使口令被截获也难以使用
        - 用户需要输入PIN码 (持卡人知道) 难以用来进行违法活动
        - 美国的Secure Dynamics Inc.的Secure ID和RSA公司的SecurID令牌

## 03 一次性口令认证
- **7.3 一次性口令认证**
    - 背景：信息化水平的提高，电子商务的普及，成为黑客的攻击对象
    - 攻击的主要方式：窃取系统口令文件和窃听网络连接，以获取用户ID和口令
    - 攻击的主要目的：设法得到用户ID和用户密码
    - OTP (One Time Password) 认证：确保在每次认证中所使用的口令不同，以对付重放攻击
```

    - OTP的主要思路：在登录过程中加入不确定因素，使每次登录过程中传送的信息都不相同，以提高登录过程安全性
    - OTP认证机制：
        - 挑战/响应机制
        - 口令序列机制
        - 时间同步机制
        - 事件同步机制
- **7.3.1 挑战/响应机制**
    - 流程
        - 1. 用户发起认证请求
        - 2. 服务器返回挑战值
        - 3. 用户输入挑战值到令牌
        - 4. 令牌计算并显示一次性口令
        - 5. 用户输入OTP，传给服务器
        - 6. 服务器返回认证结果
    - 优缺点
        - 优点
            - 可以保证很高的安全性
            - 没有同步的问题
            - 一个认证卡可以支持不同的认证服务器系统
        - 缺点
            - 需多次手工输入，易造成失误
            - 客户端和服务器交互次数多
- **7.3.2 口令序列机制**
    - 原理
        - 口令序列（S/key）机制是挑战/响应机制的一种实现
        - 在口令重置前，允许用户登录n次，那么主机需要计算出Fn(x)，并保存该值，其中F为一个单向函数
        - 用户第一次登录时，需提供Fn-1(x)。系统计算F(Fn-1(x))，并验证是否等于Fn(x)。如果通过则重新存储Fn-1(x)。下次登录时，则验证Fn-2(x)，依此类推
        - 计算顺序：F1(x) → F2(x) … Fn-1(x) → Fn(x)
        - 使用顺序：n → n-1 → … → 2 → 1
    - 说明
        - 为方便用户使用，主机把Fn-1(x)~F1(x)计算出来，编成短语打印在纸条上。用户只需按顺序使用这些口令登录即可
        - 纸条一定要保管好，不可遗失
        - 由于n有限，用户用完这些口令后，需重新生成新口令序列
    - 缺点
        - 只支持服务器对用户的单方面认证，无法防范假冒的服务器欺骗合法用户
        - 当迭代值递减为0或用户的口令泄露后必须对S/key系统重新进行初始化
- **7.3.3 时间同步机制**
    - 流程
        - 1. 用户启动令牌
        - 2. 令牌生成口令Rc
        - 3. 用户将动态口令Rc传送给服务器
        - 4. 服务器根据登录ID，取出密钥K，根据当前时间和K生成Rs，比较Rc与Rs
        - 5. 服务器返回认证结果
    - 优缺点

```
167     - 优点
168       - 用户使用简单、方便，不用频繁输入数据
169       - 通信数据小，服务器计算量不大
170     - 缺点
171       - 时间同步比较困难，软件认证卡采用PC的时间，很可能随时被修改，常常需要与服务器重新对时
172       - 对设备的时钟精度要求比较高，设计成本较高
173       - 安全性不如挑战/响应机制
174 - **7.3.4 事件同步机制**
175   - 流程
176     - 以用户使用次数作为随机因素
177     - 触发令牌上的按钮 → 一个口令 → Counter加一和预先注入的Key一起生成一个口令 → 令牌与服务器计数器一致 → 将一次性口令传给服务器 → 找到对应的Key和Counter，运算匹配，返回结果，匹配则counter加1 → 返回认证结果
178   - 重同步方法
179     - 用户和服务器很容易失去同步
180     - 解决：设置窗口值ewindow
181     - 令牌Counter远远超前于服务器Counter，靠窗口值rwindow重同步
182     - 令牌计数器超出ewindow范围启用rwindow机制
183     - 超过rwindow则只能去注册中心办理重同步业务
184   - 优缺点
185     - 优点
186       - 用户操作简单
187       - 一次认证过程通信量小
188       - 可以防止小数攻击
189       - 系统实现较简单，对时钟精度没要求
190     - 缺点
191       - 服务器计算量稍大
192 - **7.3.5 几种一次性口令实现机制的比较**
193   - 时间同步和事件同步的优势比较明显，目前市场上很多公司的产品采用的大都是基于时间同步和事件同步的方案
194   - 比较表：
195     | 机制 | 通信量 | 系统实现复杂度 | 机制安全性 | 服务器计算量 |
196     |------|--------|----------------|------------|--------------|
197     | 挑战/响应 | 较大 | 较简单 | 较好 | 较大 |
198     | S/key | 较大 | 较简单 | 较差 | 较大 |
199     | 时间同步 | 较小 | 较复杂 | 较好 | 较小 |
200     | 事件同步 | 较小 | 较简单 | 较好 | 适中 |
201
202 ## 04 生物特征身份认证技术
203 - **7.4 生物特征身份认证技术**
204   - 背景
205     - 安全性要求高时，护字符和持证等提供的安全性不能满足要求
206     - 新的生物统计学 (Biometrics) 方法正在成为实现个人身份认证最简单而安全的方法
207   - 优点
208     - 可信度高
209     - 个人特征因人而异，难以伪造
210     - 随身携带，不易丢失
```

```
    - 生物识别依据人类自身所固有的生理或行为特征
        - 生理特征：与生俱来，多为先天性的，如指纹、视网膜、面容、掌纹、声音、手形等
        - 行为特征：则是习惯使然，多为后天性的，如笔迹、步态、签名等
    - 最可靠的生物识别方式：视网膜识别、指纹识别
- **7.4.1 手书签字验证**
    - 依据：每个人的签名动作和字迹具有明显的个性，手书签名可作为身份验证的可靠依据
    - 发展：机器自动识别手书签字的研究，是模式识别的重要课题之一
    - 应用举例
        - 英国物理实验室的VERISIGN系统
        - IBM公司的加速度动态识别方法
        - Cadix公司的笔迹识别系统（软件Penop）
    - 可能的伪造签字类型
        - 不知真迹时按得到的信息随手签的字
        - 已知真迹时的模仿签字或映描签字
- **7.4.2 指纹验证**
    - 依据：没有两个人（包括孪生儿）的指纹完全相同，且指纹形状不随时间变化，提取方便
    - 应用举例
        - 美国Fingermatrix公司指纹阅读机 (Ridge Reader)
        - 个人接触证实PTV-Personal Touch Verification系统
        - Identix公司的Identix System
        - FBI已成功将小波理论应用于压缩和识别指纹图样
        - 自动指纹身份识别系统 (AFIS)
- **7.4.3 语音验证**
    - 依据：每个人的语音都各有其特点，而人对于语音的识别能力是很强的，适用于个人身份认证
    - 发展：机器自动识别语言认证的研究，是语言识别的重要课题之一
    - 应用举例
        - 美国Texas仪器公司曾设计一个16个字集的系统
        - 美国AT&T公司为一种语音口令系统 (VPS)
        - 科大讯飞的语音识别
        - 语声纹识别技术可用于防止黑客进入语音函件和电话服务系统
- **7.4.4 视网膜图样验证**
    - 依据：人的视网膜血管图样（即视网膜脉络）具有良好的个人特征
    - 应用举例
        - 视网膜血管图样的身份识别系统
        - 系统的成本较高，目前仅在军事系统和银行系统中采用
- **7.4.5 虹膜图样验证**
    - 依据：具有个人特征，可以提供比指纹更细致的信息
    - 发展：视网膜血管图样的身份识别系统
    - 应用举例
        - 可用于安全入口、接入控制、信用卡、POS、ATM、护照等的身份认证
        - 美国IriScan Inc.已研发出此种产品
- **7.4.6 脸型验证**
    - 依据：用照片识别人脸轮廓（还可扩展到对人耳形状的识别）
    - 发展：脸型自动验证系统，用图像识别、神经网络和红外扫描探测人脸的“热点”进行采样、处理并提取图样信息
    - 应用举例
        - 高铁站的人脸识别
        - 支付宝的人脸支付
```

```
  - 优点与不足
    - 优点
      - 难以仿冒的使用者认证技术
      - 随身携带，方便
    - 缺点
      - 较昂贵
      - 不够稳定 （辨识失败率高）
      - 服务器计算量稍大

## 05 基于证书的认证
- **7.5.1 简介**
  - 基于证书比基于口令的认证机制更安全
  - 基于证书的认证采用公私钥密码机制，破解难度更大
- **7.5.2 基于证书认证的工作原理**
  - 1. 生成、存储和发布数字证书
    - CA为每个用户生成数字证书，将其发给相应的用户
    - 数据库存储证书的副本，便于用户登录时验证用户的证书
  - 2. 用户发出登录请求
    - 登录服务器时，用户发送用户名和数字证书至服务器
  - 3. 服务器随机生成挑战值
    - 服务器收到登录请求，验证用户证书是否有效
    - 若有效，则生成一个随机挑战值
    - 服务器将随机挑战值传送到用户计算机
  - 4. 用户对随机挑战值签名
    - 用户计算机用用户的私钥对随机挑战值进行数字签名
    - 用户计算机将数字签名发给服务器
  - 5. 服务器验证用户的签名
    - 服务器的用户认证程序从用户数据库取得用户公钥
    - 服务器用用户的公钥验证此签名，并恢复出挑战值的杂凑值
    - 服务器将这两个随机挑战值的杂凑值进行比较
  - 6. 服务器向用户返回相应的消息
    - 根据上述验证是否通过，服务器向用户返回相应的消息，以通知用户认证是否成功
    - 此后，用户可使用网上银行业务开始电子商务活动
- **USB Key认证**
  - 软硬件相结合
    - USB Key是一种USB接口的硬件设备，它内置单片机或智能卡芯片，可以存储用户的私钥或数字证书，利用USB Key内置的密码学算法实现对用户身份的认证
    - 私钥只能用于计算，不能取出
    - 工行叫U盾，农行叫K宝，建行叫网银盾，光大银行叫阳光网盾

## 06 智能卡技术及应用
- **7.6.1 智能卡技术概述**
  - 身份认证的工具
    - 令牌
    - 磁卡
    - 智能卡 （IC卡）
    - ID卡
  - 嵌有磁条的塑卡数据易于被转录
```

```
  - 智能卡将微处理器芯片嵌在塑卡上代替无源存储磁条，安全性比无源卡有了很大提高
- **7.6.2 智能卡的工作原理框图**
  - (框图内容略，主要描述智能卡的硬件组成和工作原理)
- **7.6.3 智能卡的设计**
  - 智能卡发行时都要经过个人化 (Personalization) 或初始化 (Initialization) 阶段
  - 个人化的几个方面
    - 软/硬件逻辑的格式化
    - 写入系统和个人信息
    - 在卡上印制名称、照片
  - 智能卡安全设计的方面
    - 芯片的安全技术
    - 卡片的安全制造技术
    - 软件的安全技术
    - 安全密码算法
    - 安全可靠协议的设计
    - 管理系统的安全设计
    - 智能卡防复制、防伪造
- **7.6.4 智能卡的应用**
  - 目前的应用方面
    - 电子货币、电子商务
    - 劳动保险、医疗卫生
    - 银行系统
    - 在付费电视系统
    - 制作电子护照、二代身份证、公交一卡通、校园一卡通、电话/电视计费卡、个人履历记录、电子门禁系统等
  - 扩大的应用范围
    - 个人签字、指纹、视网膜图样等信息就可能存入智能卡，成为身份验证的更有效手段
```