期末总结

by flrs

> 课程：计算机网络安全技术（2023秋）

---

1 Why Learn Network Security

三网合一：计算机网络、电信网络、有线电视网

计算机网络：

- 逻辑功能上：资源子网（计算机系统）、通信子网（通信链路、网络节点）
- 物理连接上：计算机系统、通信链路、网络节点

Enigma

arpanet：不采用传统电话网集中式结构，提出分组交换技术的概念 ~1960

---

2 Cryptography

置换：明文元素重新排列

代换：元素映射成其它元素

密码编码学系统三个独立特征：

1. 转化明文为密文的运算类型
2. 所用的密钥数
3. 处理明文的方法

古典密码，代换：

1. Caesar密码：c = (m + 3) mod 26
2. 密钥词密码：密钥词前置，其余按顺序，代换
3. Playfair：5x5 左至右 上至下 I/J共格 相同加填充 同行向右 同列向下 错开行优先
4. Hill密码：加密：C=KP mod 26，解密：$P=K^{-1}C$，完全隐蔽单字母频率特性
5. Vigenere密码：密钥词+Caesar密码
6. Vernam密码：基于二进制、异或、一次一密（OTP）

代换密码减少明文语法模式和结构：

- 多个字母一起加密
- 多表代换

古典密码，置换：

1. 栅栏技术：对角线顺序写入，行顺序读出
2. 按行写成矩阵块，按列打乱，列的次序为密钥
3. 多步置换

对称密钥：S-DES

S盒：1、4位决定行，2、3位决定列，输出位对应二进制

LS-1/2：前5位和后5位分别循环左移1/2位

流密码：连续处理输入元素，每次输出一个元素（每次加密1位/字节，Vigenere密码和Verman密码）

分组密码：每次处理一个输入分组，相应地输出一个输出分组（整体加密，得到与明文组等长的密文组）

Feistel：乘积密码逼近简单代换密码、交替使用代换和置换

- $L_i = R_{i-1}$
- $R_i = L_{i-1} \wedge F(R_{i-1}, K_i)$
- 代换作用在左半部分，通过轮函数F作用在数据右半部分后，与左半部分异或
- 每轮迭代轮函数相同，子密钥 K_i 不同

- 代换之后，交换数据左右两半完成置换
- 分组长度和密钥长度、迭代轮数、子密钥产生算法、轮函数

扩散：明文统计特征消散，每个明文尽可能影响多的密文，gpt：常用置换实现

混淆：密文和密钥统计关系更加复杂，gpt：常用代换实现

DES加解密区别：迭代子密钥顺序交换

3DES：两个密钥，三重加密 DES(a) DES-1(b) DES(a)

Blowfish：与古典Feistel不同，数据左右同时执行运算

RC5：适于软硬件，迭代次数和密钥长度可变，三个参数

AES：不是Feistel结构，每轮代换和置换并行

公钥密码：基于数学函数（单向陷门函数），而不是代换和置换

组成：明文、加密算法、公钥/私钥、密文、解密算法

大规模网络，层次式KDC

RSA：加解密、数字签名、密钥交换，大数因子分解

Diffie-Hellman：用于密钥交换，计算离散对数非常困难

DSA：用于数字签名，基于计算离散对数

事实上的标准：RSA

公钥密码和私钥密码不能简单说安全性高低、不能相互取代、密钥分配均不简单

---

3 Authentication

散列函数 h = H(m) 特性：

- 报文m大小任意
- 产生的h长度固定
- 单向性：给定 m，计算 h = H(m) 是容易的，反之是困难的
- 抗弱碰撞性：给定 m，找到另外的 m' 使 H(M) = H(m') 是计算上不可行的
- 抗强碰撞性：寻找任何相异的(x, y)，使得 H(x) = H(y) 是计算上不可行的

Hash 函数公式：

- CV0 = IV = 初始 n 位值
- CVi = f(CVi-1, Yi-1) 1<=i<=L
- H(M) = CVL（其中输入 M 由 Y0，Y1，...，Yl-1 组成）

必须先计算 FCS 再加密，才能提供认证

MAC码提供认证：

- 与明文有关的认证：先计算 MAC 再加密
- 与密文有关的认证：先加密再计算MAC

传输模式：主要为上层协议提供保护，同时增加了IP包载荷的保护

- 典型的传输模式用于两台主机之间进行的端到端通信
- 传输模式的ESP加密和认证（可选）IP载荷，不包括报头
- 传输模式的AH认证IP载荷和报头的选中部分

隧道模式(Tunnel Mode)对整个IP包提供保护

- 当IP包加上AH/ESP域后，整个数据包和安全域被当作一个新的IP载荷，并拥有一个新的外部IP报头
- 新的IP数据包利用隧道在网络中传输，途中的路由器不能检查内部IP报头
- ESP在隧道模式中加密和认证（ 可选）整个内部IP包，包括内部IP报头
- AH在隧道模式中认证整个内部IP包和外部IP报头的选中部分

AH提供对IP头的完整性保护，而ESP不提供这个保护

ESP有ESP头和ESP尾，AH只有AH头

---

4 CIA-WLAN-VPN

安全目标：

- Confidentiality（保密性、机密性）：防被动攻击
- Integrity（完整性）：防主动攻击（更关心检测而不是阻止攻击）
- Availability（可用性）：防拒绝服务攻击

两个特殊的认证服务：

- 对等实体认证：面向连接、实体真实
- 数据源认证：面向无连接、确认数据源、不保护完整性

ALOHA：世界最早的无线电计算机通信网 1971

威胁：重放、重路由、错误路由、删除消息和网络泛洪

无限局域网加密认证技术：

- 无加密认证（SSID，MAC）
- 有线等效加密技术WEP：同一个SSID同一个密钥，初始化向量过短，不含序列号，静态
- WPA（Wi-Fi Protected Access）

WPA1 TKIP（企业版802.1x 个人版PSK）：Michael、RC4

IEEE 802.1x 针对以太网 客户/服务器模式 和上层认证协议EAP配合实现用户认证和密钥分发

WPA2：AES对称加密、CCMP消息认证

VPN解决方案：

- 基于数据链路：L2TP，仅对终端实体认证，而不认证数据报文
- 网络层：IPsec/IKE，IP级安全
- 传输层：SSL，零客户端，B/S结构（视频会议非B/S结构 无法通过SSL VPN建立和开展）

---

5 IPsec-IKE

IKE = ISAKMP格式 + Oakley模式 + SKEME密钥交换，自动地为参与通信的实体协商安全关联SA，还可以维护安全关联数据库SADB

- 第一阶段 协商创建IKE SA
- 第二阶段 建立IPsec SA
- 一个IKE SA可为多个IPsec SA提供服务

DH密钥交换算法，具有完善的前向安全性（PFS），密钥没有派生关系

安全关联数据库SADB：定义SA

安全策略数据库SPDB：使用SA

主要用局限于为IPsec通信双方建立SA

---

6 SSL-HTTPS

端口号：HTTP：80 HTTPS：443

HTTPS 不能防止ARP欺骗、DNS欺骗、数据篡改

---

7 SET

SET：针对信用卡支付的网上交易而设计的支付规范

双签名的目的是为了连接两个发送给不同接收者的报文