网络安全

1 密码体制

- 对称密钥密码体制：加密解密的密钥相同
  - DES - 分组（一组64位）→分组加密→串接，密钥56+8（奇偶校验）位
- 公钥密码体制：加密（公钥PK，公开）解密（私钥SK，保密，且不能根据公钥算出私钥）的密钥不同，又称非对称密钥密码体制；加密解密算法公开
  - 原因：密钥分配、数字签名
  - RSA
- 加解密互逆：加密解密运算对调结果相同；公钥密码体制加解密不互逆

2 鉴别

2.1 报文鉴别

包含：鉴别报文的发送者（对每一个收到的报文都要鉴别），鉴别报文的完整性

实现方式：

1. 数字签名
   - 流程：发送者使用私钥对报文加密形成数字签名，接收者使用发送者的公钥解密签名
   - 作用：实体鉴别、报文鉴别、不可否认
2. 密码散列函数
   - 结果长度短且固定、抗碰撞性、单向函数、结果和每一个输入bit相关
   - MD5、SHA-1（慢但更安全）
   - 可以防篡改，不能防伪造
3. 报文鉴别码MAC
   - 拼接共享密钥K和报文X，算H(X+K)
   - 可以防伪造

2.2 实体鉴别

在系统接入的全部持续时间对和自己通信的对方实体只鉴别一次

鉴别过程：

1. 共享对称密钥K_{AB}
   - 不能抵抗重放攻击（replay attack）：攻击者直接把加密后的报文发给通信对象
2. 不重数：使用密钥对{A, R_A}加密，R_A是一个不重复的大随机数
3. 公钥体制：使用私钥对不重数加密，使用公钥核实不重数签名
   - 中间人攻击

3 密钥分配

网外：可靠的信使携带密钥分配给互相通信的用户；网内：密钥自动分配

3.1 公钥分配（公钥密码体制）

不能随意公布用户私钥

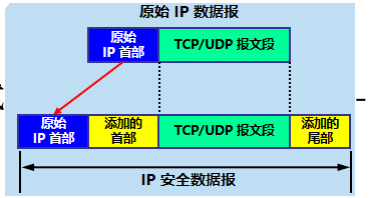
方法：

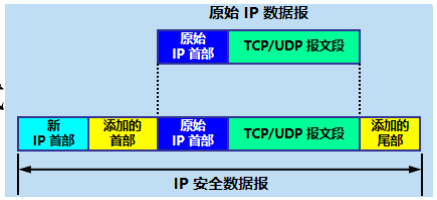
1. 第三方机构
   - 认证中心CA - 负责签发数字证书（digital certificate）
     - 信息：公钥及其拥有者的标识信息、证书签发者CA公钥 + CA使用自己私钥对上述信息的散列运算结果的固定长度散列的数字签名
     - 核实：用CA公钥解密数字签名，对数字证书信息部分散列运算，比较两个结果，一致则证书为真
     - 数字证书公开，不需要加密
     - 证书链：最顶层的根证书是用自己的私钥给自己签名的，允许CA给另一个中间商CA2发证书，再由CA2给用户发证书

4 互联网安全协议

4.1 网络层

1. IPsec协议
   - IP安全，协议族，框架（允许通信双方自行选择算法参数），包括所有协议必须实现的加密算法
   - 支持IPv4和IPv6
   - 组成：
     - IP安全数据包格式 - 使用以下协议的称为IP安全数据报
       - 鉴别首部AH协议 - 源点鉴别和数据完整性，不能保密
       - 封装安全有效载荷ESP协议 - 源点鉴别和数据完整性和保密，包含AH

    - 加密算法 - 3个协议
    - 互联网密钥交换IKE协议
- IP安全数据报的两者工作方式：
    - 运输方式 

- 适用主机到主机
    - 隧道方式 

- 适用虚拟专用网VPN

2. 安全关联
    - 在发送IP安全数据报之前，在源实体和目的实体之间创造一条网络层的逻辑连接安全关联SA，在SA上传送的就是IP安全数据报
    - 把传统互联网无连接的网络层转换为具有逻辑连接的网络层
    - 从源点到终点的**单向连接** - 若n个员工进行**双向**安全通信，一共需要创建(2 + 2n)条安全关联SA
    - 两个局域网之间的主机进行安全通信，SA是在两个局域网的路由器之间建立的

4.2 传输层

1. 安全套接字层SSL
2. 传输层安全TLS
    - 建立在HTTP（使用最多，TLS可以用于任何应用层协议）和运输层之间，为通过TCP传输的应用层数据提供保障
    - 调用TLS加密后网页显示用户且网址栏显示HTTPS，HTTPS端口号443
    - 双向鉴别
        - 单向鉴别一般指客户端浏览器鉴别服务器
        - 前提：CA证书；浏览器有验证服务器安全的手段
        - 阶段：
            1. 握手阶段：使用握手协议 - 验证服务器，生成会话阶段所需的共享密钥

1. 协商加密算法。❶ 浏览器 A 向服务器 B 发送浏览器的 TLS 版本号和一些可选的加密算法。❷ B 从中选定自己所支持的算法（如 RSA），并告知 A，同时把自己的 CA 数字证书发送给 A。

2. 服务器鉴别。❸ 客户 A 用数字证书中 CA 的公钥对数字证书进行验证鉴别。

3. 生成主密钥。❹ 客户 A 按照双方确定的密钥交换算法生成主密钥 MS (Master Secret)。❺ 客户 A 用 B 的公钥 PK_B 对主密钥 MS 加密，得出加密的主密钥 $PK_B(MS)$，发送给服务器 B。

4. 服务器 B 用自己的私钥把主密钥解密出来 ❻：$SK_B(PK_B(MS)) = MS$ 。这样，客户 A 和服务器 B 都有了为后面数据传输使用的共同的主密钥 MS。
5. 生成会话密钥 ❼ 和 ❽。为了使双方的通信更加安全，客户 A 和服务器 B 最好使用不同的密钥。主密钥被分割成 4 个不同的密钥。每一方都拥有这样 4 个密钥（注意：这些都是对称密钥）：
   - 客户 A 发送数据时使用的会话密钥 K_A
   - 客户 A 发送数据时使用的 MAC 密钥 M_A
   - 服务器 B 发送数据时使用的会话密钥 K_B
   - 服务器 B 发送数据时使用的 MAC 密钥 M_B

2. 会话阶段：使用记录协议 - 保证传送数据的机密性和完整性
   - 带关联数据的鉴别加密AEAD：给记录加序号算进散列，但是不写入记录

     对 MAC 密钥 MA 、记录的当前序号和明文记录进行散列运算；使用会话密钥 KA 进行加解密。

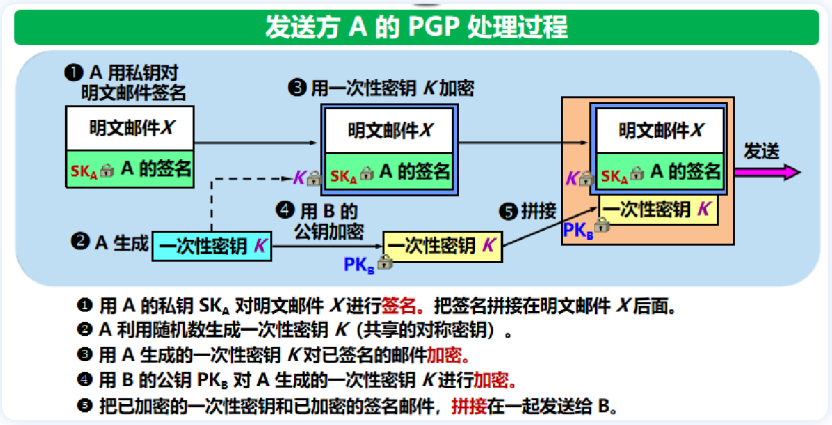
- 类型字段：指明所传送的记录是握手阶段的报文，还是应用程序传送的报文，或最后要关闭 TLS 连接的报文。
- 长度字段：字节数，用于从 TCP 报文中提取 TLS 记录。

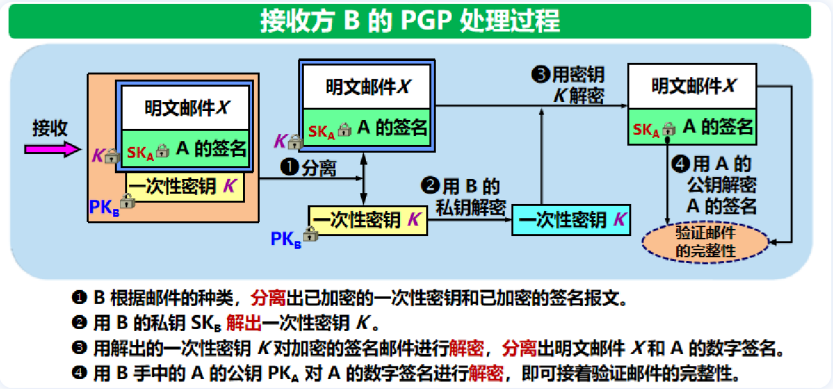
- 补充措施：
  1. 客户 A 和服务器 B相互发送不重数，防止重放攻击。
  2. 生成预主密钥 PMS (Pre-Master Secret)，为下一步生成主密钥使用。
  3. 生成主密钥。客户 A 和服务器 B 各自使用同样的（已商定的）算法，使用预主密钥 PMS 、客户的不重数和服务器的不重数，生成主密钥 MS。（握手阶段）
  4. 客户 A 向服务器 B 发送的全部握手阶段报文的 MAC。
  5. 服务器 B 向客户 A 发送的全部握手阶段报文的 MAC。
  - 关闭的时候要先发送关闭TLS的记录，防止截断攻击（攻击者发送FIN报文段关闭连接）

4.3 应用层

仅讨论电子邮件相关：即时行为，单向报文

电子邮件安全软件包PGP

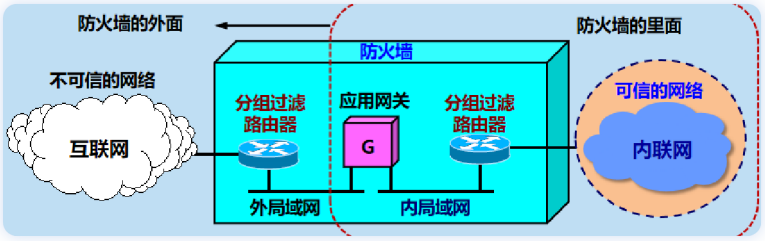




5 系统安全

- 用户入侵：未授权登录、非法获取更高级别权限...
- 软件入侵：病毒、蠕虫、拒绝服务攻击...

5.1 防火墙firewall



控制进出网络边界的分组，禁止任何不必要的通信

一种特殊编程的路由器，安装在一个网点和网络的其余部分之间，目的是实施访问控制策略（由使用防火墙的单位自行决定）

网络划分：

- 防火墙内部网络 - trusted network
- 防火墙外面网络 - untrusted network

防火墙技术：

- 分组过滤路由器 - 根据过滤规则对进出内部网络的分组进行过滤（转发或者丢弃）
  - **过滤规则：基于分组的网络层或运输层首部信息，例如：源/目的IP地址、源/目的端口、协议类型（TCP 或 UDP），等等。**
  - **无状态的：独立地处理每一个分组。**
  - **有状态的：跟踪每个连接或会话的通信状态，根据状态信息决定是否转发分组。**
  - **优点：简单高效，对用户透明。**
  - **缺点：不能对高层数据进行过滤。例如：不能禁止某个用户对某个特定应用进行某个特定的操作，不能支持应用层用户鉴别等。**
- 应用网关 - 也称代理服务器（proxy server）

- 对报文进行中继，实现基于应用层数据的过滤和高层用户鉴别。
- 所有进出网络的应用程序报文都必须通过应用网关。
- 应用网关在应用层打开报文，查看请求是否合法。
  - 如果合法，应用网关以客户进程的身份将请求报文转发给原始服务器。
  - 如果不合法，则丢弃报文。
- 缺点：
  - 每种应用都需要一个不同的应用网关
  - 在应用层转发和处理报文，处理负担较重。
  - 对应用程序不透明，需要在应用程序客户端配置应用网关地址。

5.2 入侵检测系统

深度分析与检测进入的分组，发现疑似入侵行为