# 第十九节 密钥分配、安全协议、防火墙与入侵检测

## 一、课程目标

了解教材 7.4-7.6。

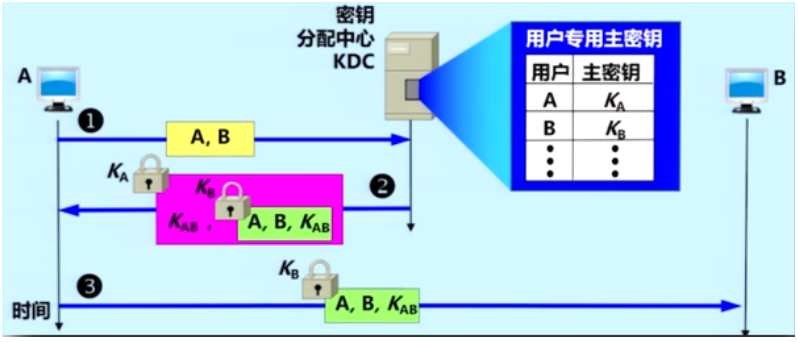
## 二、课程内容

**【密钥分配】（对应对称/非对称两类）**

**对称密钥分配**

1、常用对称密钥分配方案包括预共享密钥分配、密钥分配中心和 DH 算法三种。

2、密钥分配中心 KDC（Key Distribution Center）任务是给所有需要进行秘密通信的用户临时分配一个会话密钥（仅使用一次）。KDC 给报文加入时间戳防止入侵者，定期更换分配给用户的密钥。




**处理过程：**

（1）用户注册：用户 A 和 B 都是 KDC 的注册用户，各自分配了和 KDC 通信的主密钥 $K_A$ 和 $K_B$；

（2）申请密钥：A 向 KDC 发送明文 AB，表明通信双方身份，申请与 B 通信的密钥；

（3）KDC 向 A 回送信息：

- 会话密钥：KDC 用随机数产生一次性会话密钥 $K_{AB}$，该密钥是 AB 会话使用的密钥；
- 票据信息加密：报文中还包含了一个需要 A 转给 B 的信息(票据)，这个信息是使用 B 的密钥 $K_B$ 进行加密的，A 不知道其中的信息；
- 票据信息内容：通信双方信息，以及会话密钥 $K_{AB}$；
- 报文加密：报文中包含会话密钥和票据信息，报文整体使用 A 的主密钥 $K_A$ 进行加密；

- 票据发送：A 向 B 发送票据信息，B 用 $K_B$ 解密就知道了 A 想要和自己通信，并且带来了通信的密钥 $K_{AB}$。

**对称密钥分配优化：**

- 加入时间戳：加入时间戳，可以防止重放攻击；
- 用户密钥有效期：KDC 中分配给用户的主密钥，需要定期更换，降低破译的概率；主密钥都是加密密钥，解密密钥由各自保存；
- 会话密钥有效期：临时会话的密钥 KAB 仅在本次临时会话中有效，会

话结束后失效。

最出名的对称密钥分配协议是 Kerberos v5，包括鉴别服务器和票据授予服务器，只用于客户与服务器之间的鉴别。

公钥分配

3、实现方案：可信任第三方机构（认证中心，CA）给拥有公钥的实体发一个具有数字签名的数字证书（对公钥与其对应的实体进行绑定的证明，因此常称公钥证书），数字证书写有公钥机器拥有者的标识信息，由 CA 使用自己的私钥进行数字签名。由于签发证书机构通过由政府或知名公司建立，因此最终构成的对已签名的证书拥有者 B 的数字证书也认为可信。

**CA 对收到的 B 未签名证书的签名过程：**对 B 未签名的证书进行散列函数运算，再用 CA 私钥对散列值进行 D 运算（即签名），得到 CA 数字签名；把 CA 数字签名和未签名的 B 证书组装，构成已签名的 B 的数字证书。

**A 对 B 的数字证书验证过程：**使用数字证书给出的 CA 的公钥，对数字证书中 CA 的数字签名进行 E 运算，得到第一个数值；再对 B 的数字证书（把 CA 数字签名除外的部分）进行散列运算，得到第二个数值；比较两个数值，若一致，则数字证书为真。

**4、公钥基础结构 PKI**

ITU-T 制定 X.509 协议标准对数字证书格式进行标准化，被称为互联网公钥基础结构，重要字段包括：X.509 版本、数字证书名称及序列号、本数字证书所使用签名算法、数字证书签发者唯一标识符、主体名、公钥等。

**【互联网使用的安全协议】（网络/传输/应用三个典型协议）**

网络层安全协议

**5、网络层安全协议 IPsec 协议组成：**

（1）IPsec 两个协议：鉴别首部 AH 协议和封装安全有效载荷 ESP 协议。

（2）有关加密算法的三个协议。

（3）互联网密钥交换 IKE 协议。


| 安全协议 | ESP | | | | AH | | | |
|---|---|---|---|---|---|---|---|---|
| 加密 | DES | 3DES | AES | SM1/SM4 | | | | |
| 验证 | MD5 | SHA1 | SHA2 | SM3 | MD5 | SHA1 | SHA2 | SM3 |
| 密钥交换 | IKE（ISAKMP，DH） | | | | | | | |

**数据来源验证：**接收方验证发送方身份是否合法。

**数据加密：**发送方对数据进行加密，以密文的形式在Internet上传送，接收方对接收的加密数据进行解密后处理或直接转发。

**数据完整性：**接收方对接收的数据进行验证，以判定报文是否被篡改。

**抗重放：**接收方拒绝旧的或重复的数据包，防止恶意用户通过重复发送捕获到的数据包所进行的攻击。



注意：（1）IPsec 没有规定用户必须使用哪种加密和鉴别算法，但它提供了一套加密算法。（2）AH 协议提供源点鉴别和数据完整性，但不能加密。ESP 协议提供源点鉴别、数据完整性和加密。ESP 比 AH 复杂很多。在 IPv6 中，AH 和 ESP 都是扩展首部的一部分。AH 协议都包含在 ESP 协议内部。（3）使用 AH 或

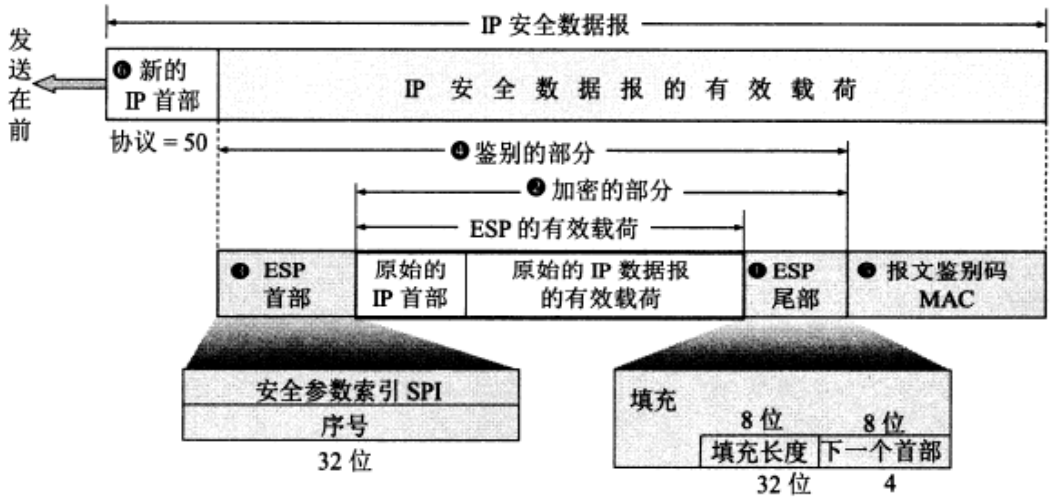
ESP 协议的 IP 数据报叫做 IP 安全数据报（IPsec 数据报）。

6、IPsec 数据包工作方式有两种：

（1）运输方式：在整个运输层报文段的前后分别添加若干控制信息，再加上 IP 首部，构成 IPsec 数据报。

（2）隧道方式（使用最多）：在原始的 IP 数据报的前后分别添加控制信息，再加上新的 IP 首部，构成 IPsec 数据报。

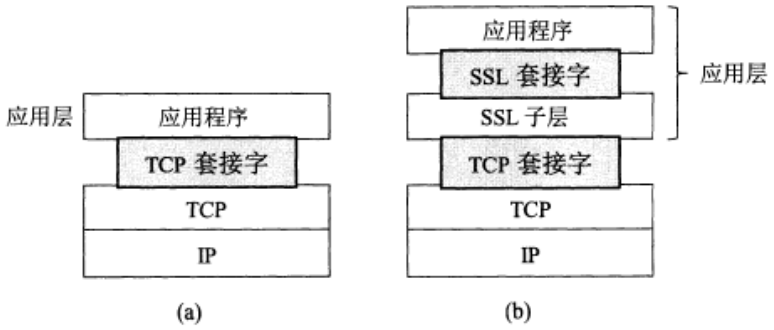
无论哪种方式，IPsec 数据报的首部都是不加密的（这样路由器才能识别首部中的信息），只有数据部分是经过加密的。




## 运输层安全协议

**7、运输层安全协议有安全套接字层 SSL 和运输层安全 TLS。**

**SSL**：SSL 最新版本是 SSL3.0，常用的浏览器和 Web 服务器都支持 SSL，SSL 作用于端系统应用层的 HTTP 和运输层之间，在 TCP 之上建立起一个安全通道，为通过 TCP 传输的应用层提供安全保障。未使用 SSL 时，应用层的数据通过 TCP 套接字与运输层交互，使用 SSL 后，中间又多了一个 SSL 子层。SSL 已废弃。




网址中 https 表示使用了 SSL 协议，TCP 的 https 端口号是 443，http 端口号是 80。

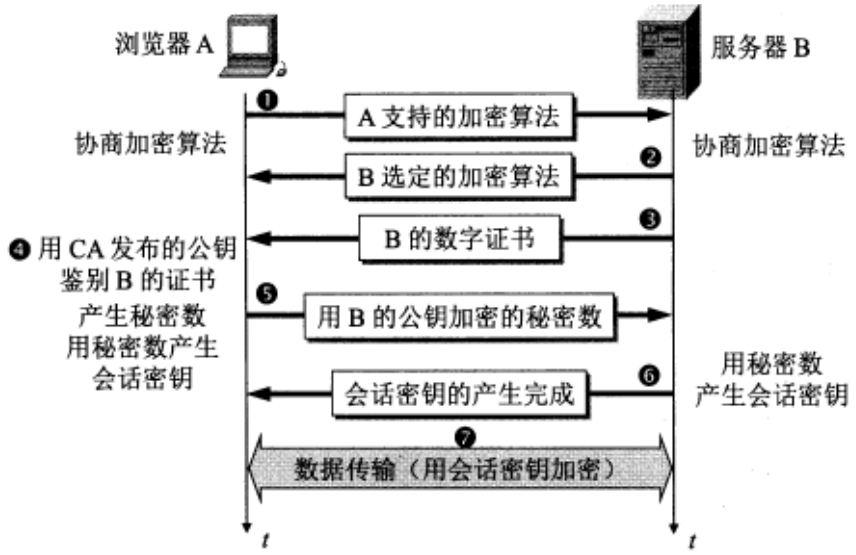
SSL 提供的安全服务可以归纳为三种：

（1）SSL 服务器鉴别，允许用户证实服务器的身份。

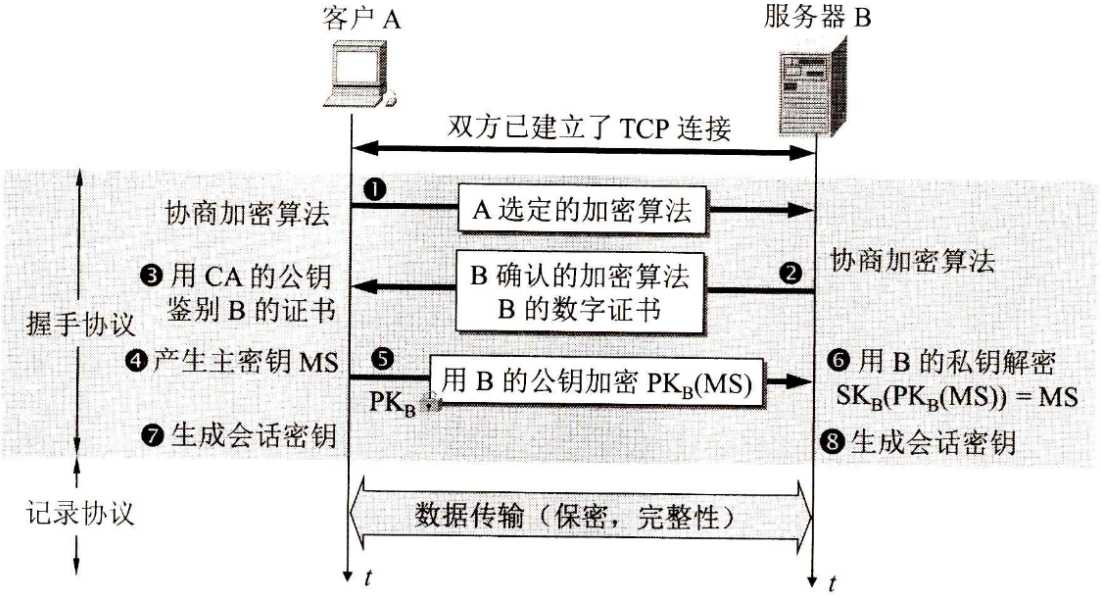
（2）SSL 客户鉴别，允许服务器证实客户的身份。

（3）加密 SSL 会话，对客户和服务器之间发送的所有报文加密，并检测报文是否被篡改。

SSL 工作过程包括：协商加密算法、服务器鉴别、会话密钥计算、安全数据传输。




**TLS**：SSL 是 TLS 的基础（旧说法 SSL/TLS，现统称 TLS）。1999 年，IETF 标准化 SSL3.0 位 TLS 1.0。最新版本位 2018 年 8 月的 TLS 1.3。




客户端 ：Hi，服务端，我这边支持这些算法，这是我本次的随机数。

服务端 ：好的，我看看，我们就选用这个算法套件吧，这是我本次的随机数，这是我的证书，你用这个证书里的公钥来加密预主密钥。

客户端 ：稍等我验下证书，嗯，的确是服务端的证书。这是用证书中公钥加密的预主密钥。（使用两个随机数+预主密钥计算主密钥，然后生成会话密钥。。。）好了，我这边 OK 了。

服务端 ：收到。（用私钥解密出预主密钥，使用两个随机数+预主密钥计算主密钥，然后生成会话密钥。。。）好了，我这边也 OK 了。

客户端 ：这是加密的应用数据。。。

服务端 ：这是加密的应用数据。。。

注意：主密钥通常是非对称加密，会话密钥通常是对称密钥，

## 应用层安全协议

8、电子邮件安全协议 PGP

**工作原理：**假定 A 向 B 发送电子邮件明文 X，使用 PGP 加密。

**A 有三个密钥：**自己的私钥 SKA，B 的公钥 PKB 和自己生成的一次性密钥 K。

**B 有两个密钥：**自己的私钥 SKB 和 A 的公钥 PKA。

**A 加密过程：**

（1）使用私钥 SKA 对明文邮件 X 进行**签名**，把签名拼接在明文邮件 X 后。

（2）利用随机数 A 生成一次性密钥 K（共享的对称密钥）。

（3）用 A 生成的一次性密钥 K 对已签名的邮件**加密**。

（4）用 B 的公钥 PKB 对 A 生成的一次性密钥 K 进行**加密**。

（5）把已加密的一次性密钥和已加密的签名邮件，拼接在一起发送给 B。

注意：三次加密作用不同，第一次是数字签名，证明邮件完整性；第二次是对已签名的邮件加密，保证邮件机密性。第三次是对密钥 K 加密，保证对称密钥 K 的机密性。

密钥 K 是一次性密钥，是对称密钥，加解密过程中各只使用 1 次。

**B 解密过程：**

（1）根据 RFC 4880 对邮件分解，提取一次性密钥 K 和已签名邮件报文。

（2）用私钥 SKB 解密一次性密钥 K 对加密的签名邮件进行解密，分离出明文 X 和 A 的数字签名。

（3）用 A 的公钥 PKA 对 A 的数字签名进行解密，验证完整性。

**【防火墙和入侵检测】**

9、防火墙 FW 是一种访问控制技术，是第一道防线，通过严格控制进出网络边界的分组，禁止不必要的通信，减少潜在入侵发生。

防火墙里面的网络称为可信的网络，防火墙以外的网络称为不可信网络。

10、入侵检测系统 IDS 通过对进入网络的分组进行深度分析和检测发现疑似入侵行为的网络行动。

入侵检测方法一般分为基于特征的入侵检测和基于异常的入侵检测。

## 三、重点习题

P368：全部

## 四、参考资料

https://zhuanlan.zhihu.com/p/575773514

https://www.cnblogs.com/logchen/p/15159382.html

https://www.bilibili.com/video/BV1Eo4y1y7Dh/?spm_id_from=333.337.search-card.all.click&vd_source=ae7c78da643dd0aeb736fa2a6cca9565