哈爾濱工業大學
HARBIN INSTITUTE OF TECHNOLOGY
立足航天，服务国防，面向国民经济主战场

计算机网络之危机四伏

主讲人：李全龙

本讲主题

安全套接字层（SSL）（3）

SSL握手过程（1）

1. 客户发送其支持的算法列表，以及客户一次随机数(nonce)
2. 服务器从算法列表中选择算法，并发回给客户：选择 + 证书 + 服务器一次随机数
3. 客户验证证书，提取服务器公钥，生成预主密钥(pre_master_secret)，并利用服务器的公钥加密预主密钥，发送给服务器
4. 客户与服务器基于预主密钥和一次随机数分别独立计算加密密钥和MAC密钥
5. 客户发送一个针对所有握手消息的MAC
6. 服务器发送一个针对所有握手消息的MAC

SSL握手过程(2)

最后2步的意义：保护握手过程免遭篡改

- 客户提供的算法，安全性有强、有弱
  - 明文传输
- 中间人攻击可以从列表中删除安全性强的算法
- 最后2步可以预防这种情况发生
  - 最后两步传输的消息是加密的

SSL握手过程(3)

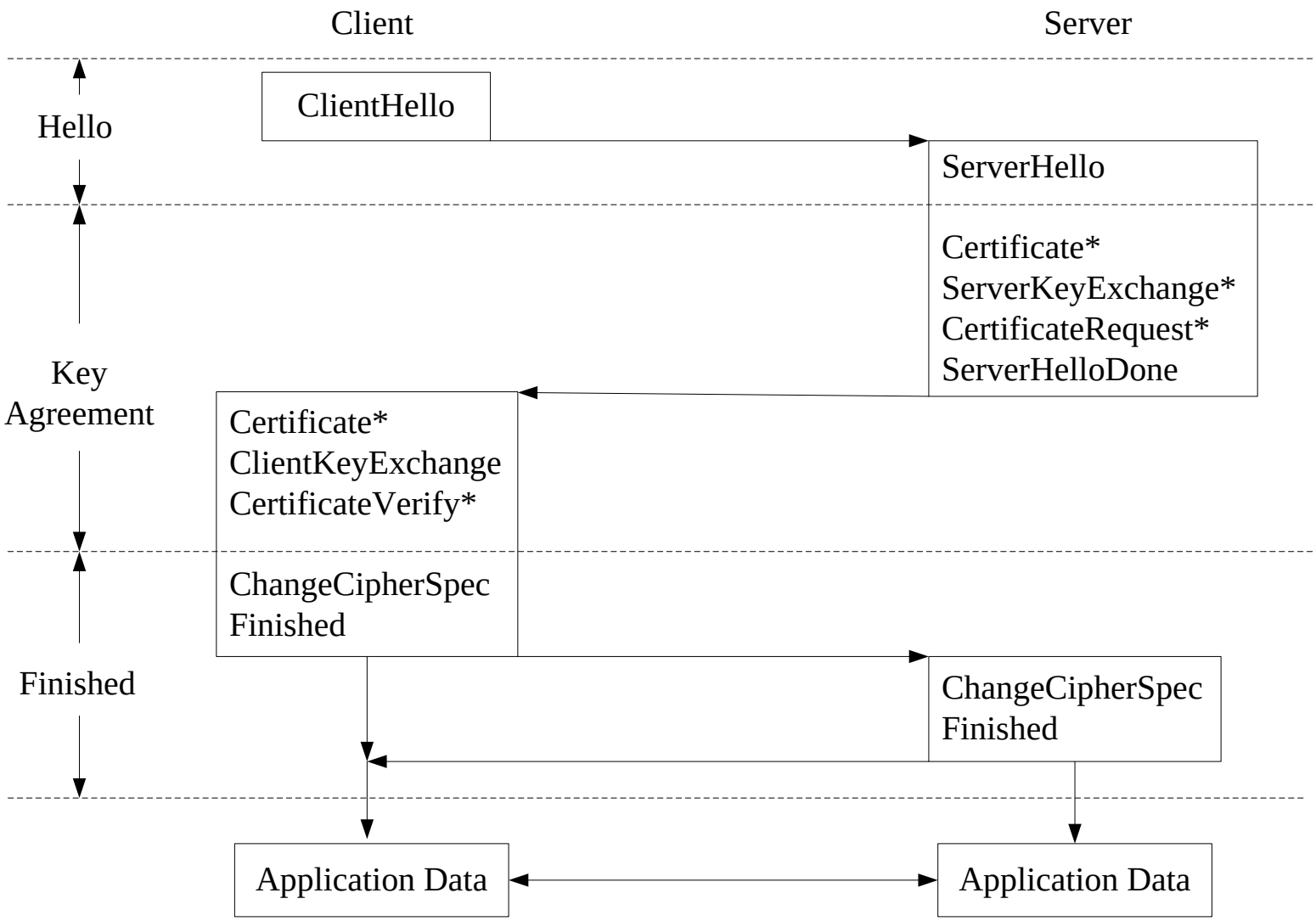
- 为什么使用两个一次随机数？
- 假设Trudy嗅探Alice与Bob之间的所有报文
- 第二天，Trudy与Bob建立TCP连接，发送完全相同的记录序列
  - Bob(如Amazon)认为Alice对同一产品下发两个分离的订单
  - 解决方案: Bob为每次连接发送完全不同的一次随机数
    - 确保两天的加密密钥不同
  - Trudy的报文将无法通过Bob的完整性检验

SSL握手协议

❖SSL握手消息及参数

消息类型	参数
hello_request	Null
client_hello	版本，随机数，会话ID，密码参数，压缩方法
server_hello	
certificate	X.509v3证书
server_key_exchange	参数，签名
certificate_request	类型，CA
server_done	Null
certificate_verify	签名
client_key_exchange	参数，签名
Finished	Hash值

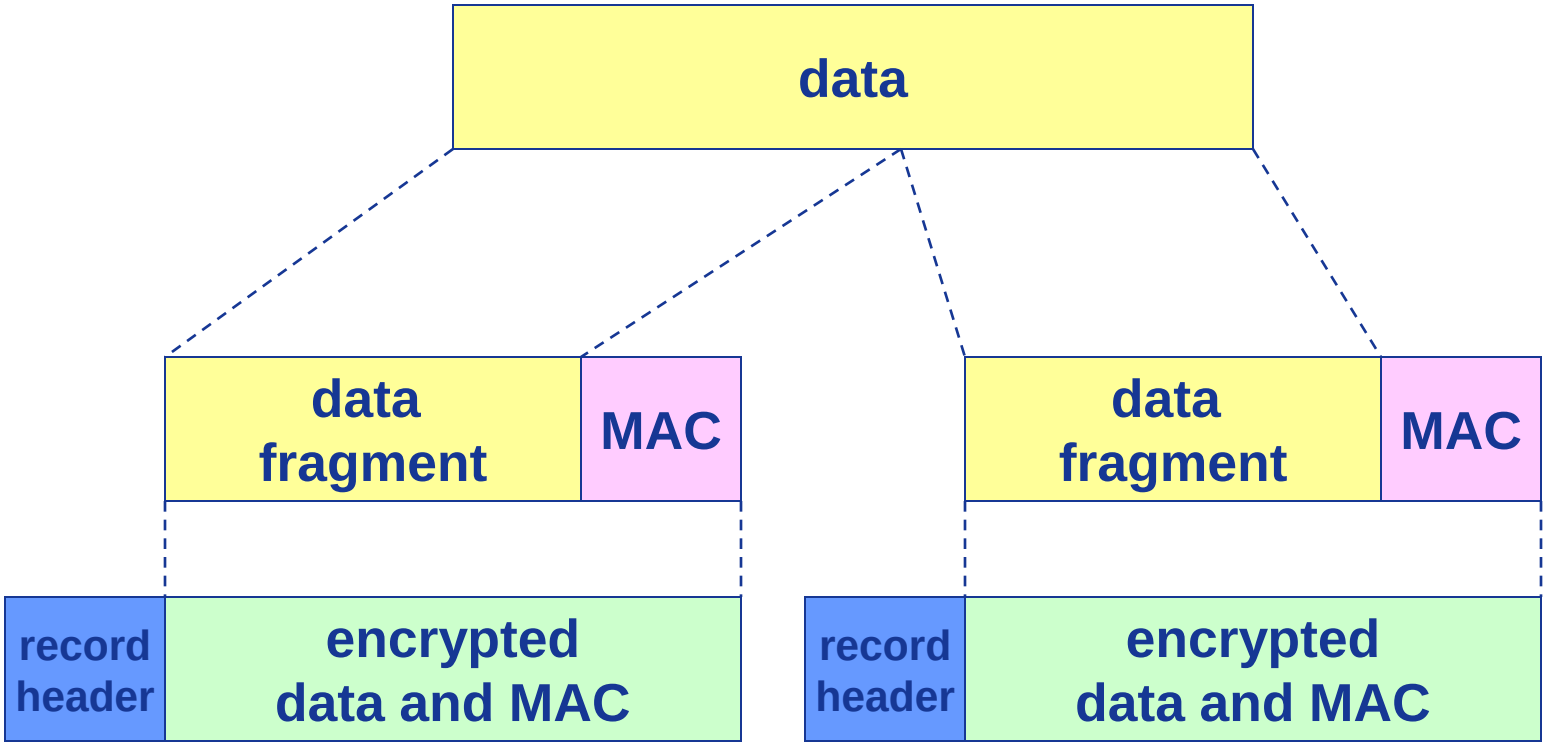
SSL握手协议工作过程



SSL记录协议

- SSL记录协议的操作步骤：
  - 将数据分段成可操作的数据块
  - 对分块数据进行数据压缩
  - 计算MAC值
  - 对压缩数据及MAC值加密
  - 加入SSL记录头
  - 在TCP中传输

SSL记录协议

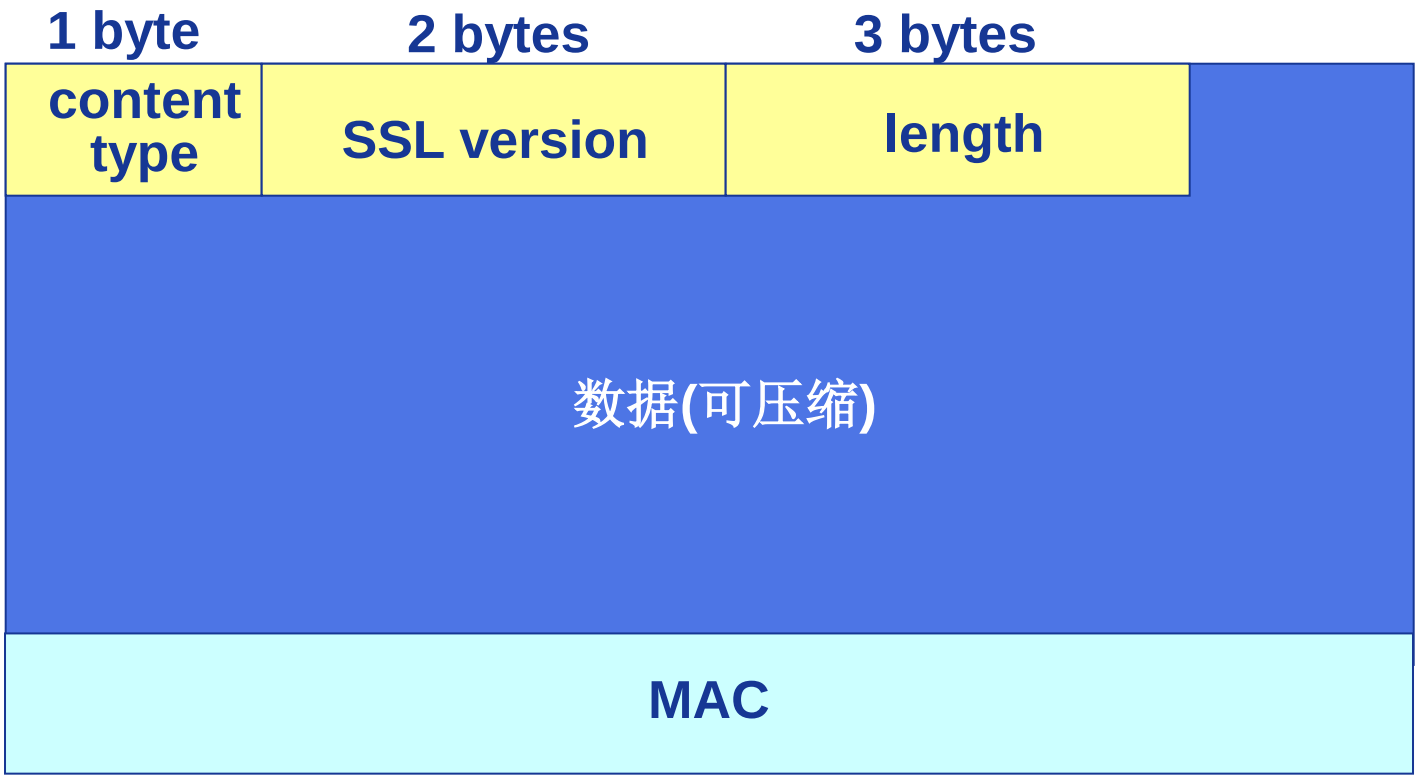


记录头(record header): 内容类型(ContentType); 版本; 长度

MAC: 包括序列号, MAC密钥 M_x

片段(fragment): 每个SSL片段为2^{14}字节 (~16KB)

SSL记录格式



数据和MAC是加密的(对称密钥加密算法)

实际的SSL连接

handshake: ClientHello

handshake: ServerHello

handshake: Certificate

handshake: ServerHelloDone

handshake: ClientKeyExchange

ChangeCipherSpec

handshake: Finished

此后所有内容均加密

ChangeCipherSpec

handshake: Finished

application_data

application_data

Alert: warning, close_notify

接下去是TCP的FIN段

密钥派生

- 客户一次数、服务器一次数和预主密钥输入伪随机数发生器
  - 产生主密钥MS
- 主密钥和新一次随机数输入另一个随机数发生器:“密钥块(key block)”
- 密钥块“切片”:
  - 客户MAC密钥
  - 服务器MAC密钥
  - 客户加密秘钥
  - 服务器加密秘钥
  - 客户初始向量(IV)
  - 服务器初始向量(IV)

哈爾濱工業大學
HARBIN INSTITUTE OF TECHNOLOGY

立足航天，服务国防，面向国民经济主战场

谢 谢！