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

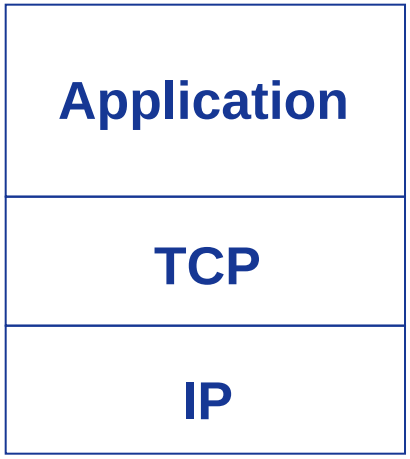
本讲主题

安全套接字层（SSL）（1）

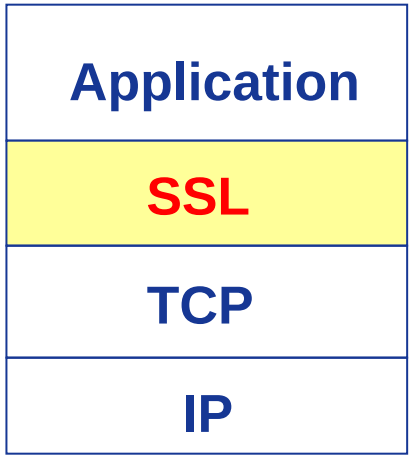
SSL: Secure Sockets Layer

- 广泛部署的安全协议
  - 几乎所有浏览器和Web服务器都支持
  - https
  - 每年通过SSL交易额达数十亿美元
- 实现：Netscape
- 变体：TLS(RFC 2246)
- 提供：
  - 机密性(confidentiality)
  - 完整性(integrity)
  - 认证(authentication)
- 最初目标:
  - Web电子商务交易
  - 加密(尤其信用卡号)
  - Web服务器认证
  - 可选的客户认证
  - 方便与新商户的商务活动(minimum hassle)
- 可用于所有基于TCP的网络应用
  - 安全socket接口

SSL和TCP/IP



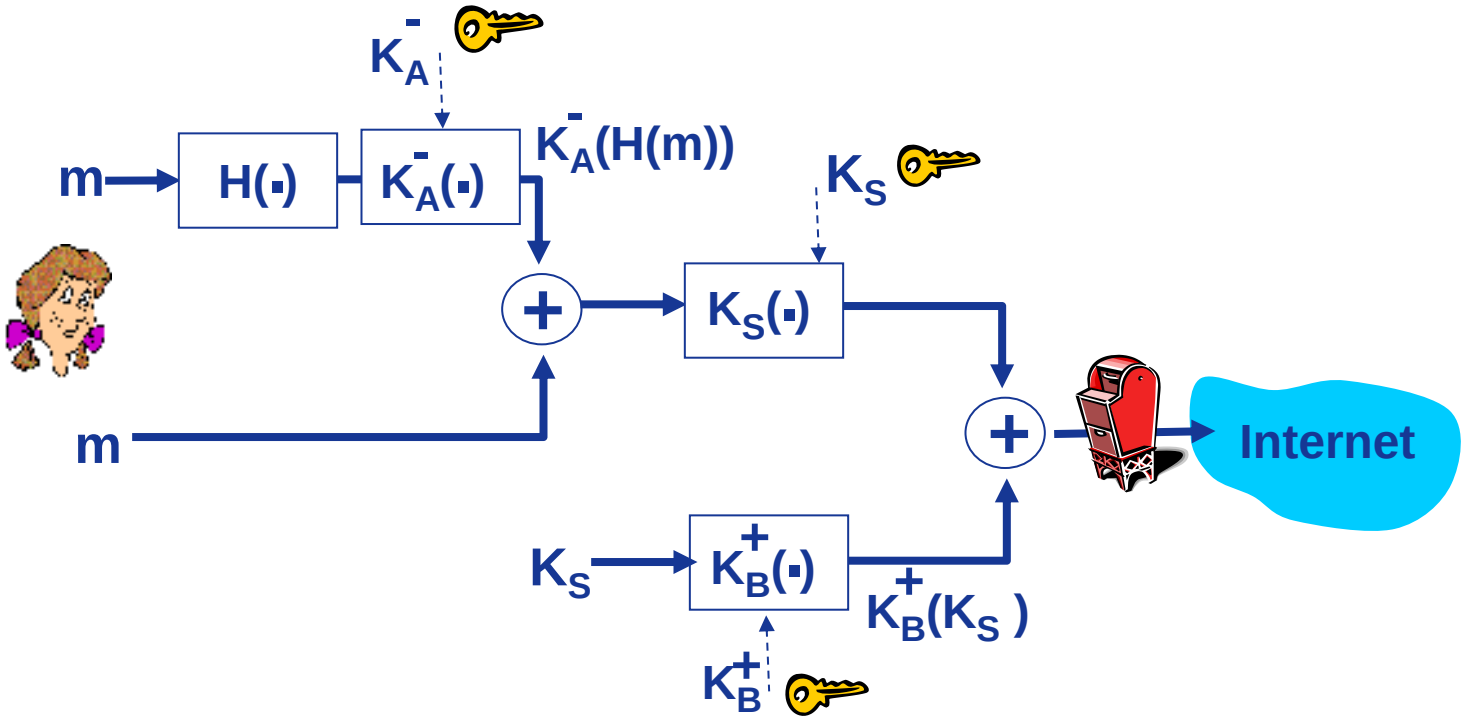
正常应用



采用SSL的应用

- SSL为网络应用提供应用编程接口 (API)
- C语言和Java语言的 SSL库/类可用

可以像PGP那样实现某些安全功能

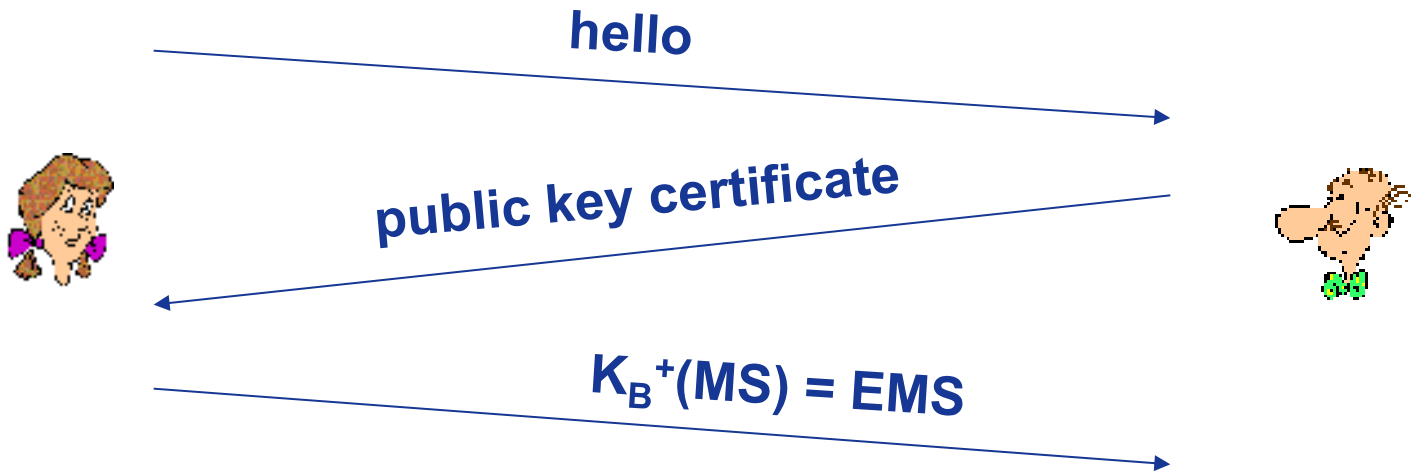


- 但是，需要发送字节流以及交互数据
- 需要一组密钥用于整个连接
- 需要证书交换作为协议的一部分：握手阶段

简化的(Toy)SSL: 一个简单的安全信道

- 握手(handshake): Alice和Bob利用他们的证书、私钥认证（鉴别）彼此，以及交换共享密钥
- 密钥派生(key derivation): Alice和Bob利用共享密钥派生出一组密钥
- 数据传输(data transfer): 待传输数据分割成一系列记录
- 连接关闭(connection closure): 通过发送特殊消息，安全关闭连接

简化的SSL：一个简单的握手过程



MS: 主密钥

EMS: 加密的主密钥

简化的SSL：密钥派生

- 不同加密操作使用不同密钥会更加安全
  - 例如：报文认证码(MAC)密钥和数据加密密钥
- 4个密钥：
  - K_c = 用于加密客户向服务器发送数据的密钥
  - M_c = 用于客户向服务器发送数据的MAC密钥
  - K_s = 用于加密服务器向客户发送数据的密钥
  - M_s =用于服务器向客户发送数据的MAC密钥
- 通过密钥派生函数(KDF)实现密钥派生
  - 提取主密钥和（可能的）一些额外的随机数，生成密钥

简化的SSL：数据记录

- 为什么不直接加密发送给TCP的字节流?
  - MAC放到哪儿?
    - 如果放到最后，则只有全部数据收全才能进行完整性认证。
  - e.g., 对于即时消息应用， 在显示一段消息之前，如何针对发送的所有字节进行完整性检验?
- 方案：将字节流分割为一系列记录
  - 每个记录携带一个MAC
  - 接收方可以对每个记录进行完整性检验
- 问题：对于每个记录， 接收方需要从数据中识别出MAC
  - 需要采用变长记录

简化的SSL：序列号

- 问题: 攻击者可以捕获和重放记录或者重新排序记录
- 解决方案: 在MAC中增加序列号
  - MAC = MAC(M_x, sequence||data)
  - 注意: 记录中没有序列号域

- 问题: 攻击者可以重放所有记录
- 解决方案: 使用一次性随机数(nonce)

简化的SSL：控制信息

- 问题: 截断攻击
  - 攻击者伪造TCP连接的断连段，恶意断开连接
  - 一方或双方认为对方已没有数据发送
- 解决方案: 记录类型, 利用一个类型的记录专门用于断连
  - type 0用于数据记录；type 1用于断连
- MAC = MAC(M_x, sequence||type||data)

简化的SSL：总结

bob.com

hello

certificate, nonce

$K_B^+(MS) = EMS$

type 0, seq 1, data

type 0, seq 2, data

type 0, seq 1, data

type 0, seq 3, data

type 1, seq 4, close

type 1, seq 2, close

加密的

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！