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）（2）

简化的SSL不完整

- 每个域多长？
- 采用哪种加密协议？
- 需要协商吗？
  - 允许客户与服务器支持不同加密算法
  - 允许客户与服务器在数据传输之前共同选择特定的算法

SSL协议栈

- 介于HTTP与TCP之间的一个可选层
  - 绝大多数应用层协议可直接建立在SSL之上
- SSL不是一个单独的协议，而是两层协议

SSL密码组(cipher suite)

- 密码组(cipher suite)
  - 公开密钥算法(public-key algorithm)
  - 对称加密算法(symmetric encryption algorithm)
  - MAC算法
- SSL支持多个密码组
- 协商(negotiation): 客户与服务器商定密码组
  - 客户提供选项(choice)
  - 服务器挑选其一

常见的SSL对称密码：

- **DES –分组密码**
- **3DES –分组密码**
- **RC2 – Rivest Cipher 2 分组密码**
- **RC4 – Rivest Cipher 4 流密码**

SSL公开密钥加密：

- **RSA**

SSL更改密码规格协议

- 更改密码规格协议(Change Cipher Spec Protocol)
  - 更新当前连接的密钥组
    - 标志着加密策略的改变
  - 位于SSL记录协议之上
  - ContentType=20
  - 协议只包含一条消息（一个值为1的字节）

SSL警告协议

- 警告协议(Alert Protocol)
  - Alert消息：
    - 当握手过程或数据加密等出错或发生异常时，为对等实体传递SSL警告或终止当前连接
  - 位于SSL记录协议之上
  - ContentType=21
  - 协议包含两个字节：警告级别和警告代码

SSL握手协议

- 握手协议(Handshake Protocol)
  - 协商结果是SSL记录协议的基础，ContentType=22
  - SSL v3.0的握手过程用到三个协议：握手协议、更改密码规格协议和警告协议
- 目的：
  - 服务器认证/鉴别
  - 协商: 商定加密算法
  - 建立密钥
  - 客户认证/鉴别(可选)

SSL记录协议

- 记录协议(Record Protocol)
  - 描述SSL信息交换过程中的记录格式
  - 所有数据（含SSL握手信息）都被封装在记录中
  - 一个记录由两部分组成：记录头和数据

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！