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

Web应用安全

Web安全威胁

- 攻击与破坏事件层出不穷，需要安全Web服务
  - Web应用广泛、服务器底层软件复杂，可能隐藏安全漏洞
- Web安全威胁的分类：
  - 主动攻击：篡改C/S之间信息或篡改Web站点信息（难防易检）
  - 被动攻击：监听数据流获取信息或进行信息量分析（难检易防）
- 机密性
  - 网络监听、窃取数据
- 完整性
  - 修改用户数据、修改传输的信息
- 拒绝服务
  - 伪造请求淹没服务器
- 身份认证
  - 冒充合法用户、伪造数据

Web安全威胁

- Web服务器的安全威胁
  - Web服务越强大，包含安全漏洞概率就越高
  - HTTP服务可在不同权限下运行
- Web浏览器的安全威胁
  - 活动Web页可能隐藏恶意程序
- 通信信道的安全威胁
  - 监听程序会威胁通信信道中所传输信息的机密性
  - 伪造、篡改、重放会威胁所传输信息的完整性
  - 缺乏身份认证使得冒充他人身份进行中间人攻击
  - 缺乏数字签名机制使得通信双方能相互攻击
  - 拒绝服务攻击使得通信信道不能保证可用性

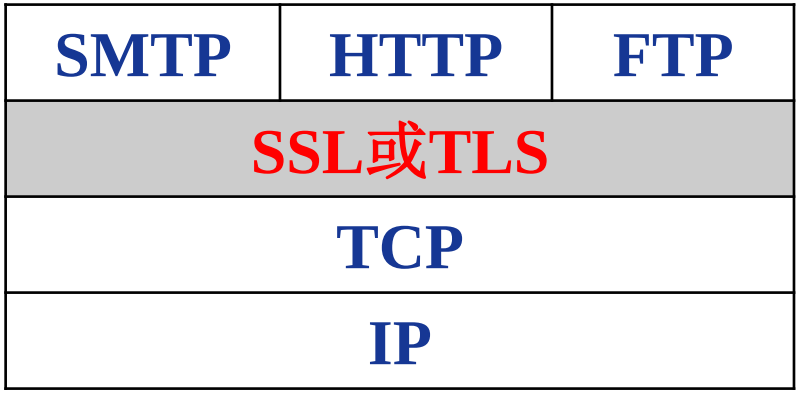
基于应用层实现Web安全

- 为特定应用定制特定安全服务，将安全服务直接嵌入在应用程序中

<table>
<tr><td rowspan="3">Kerberos</td><td>S/MIME</td><td>PGP</td><td>SET</td><td></td></tr>
<tr><td colspan="2">SMTP</td><td>HTTP</td><td>FTP</td></tr>
<tr><td colspan="4">SSH</td></tr>
<tr><td>UDP</td><td colspan="4">TCP</td></tr>
<tr><td colspan="5">IP</td></tr>
</table>

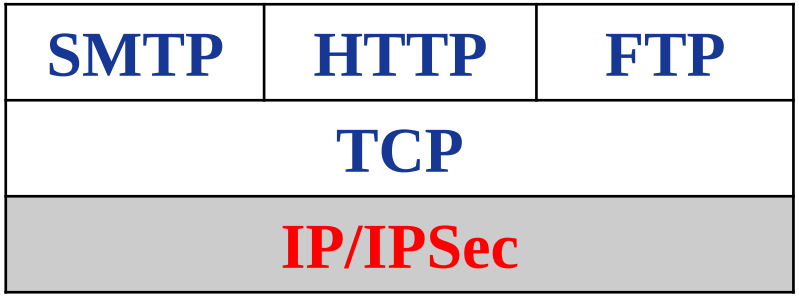
基于传输层实现Web安全

- SSL或TLS可作为基础协议栈的组成部分，对应用透明
  - 也可直接嵌入到浏览器中使用
- 使用SSL或TLS后，传送的应用层数据会被加密
  - 保证通信的安全



基于网络层实现Web安全

- IPSec提供端到端（主机到主机）的安全机制
  - 通用解决方案
- 各种应用程序均可利用IPSec提供的安全机制
  - 减少了安全漏洞的产生



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！