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

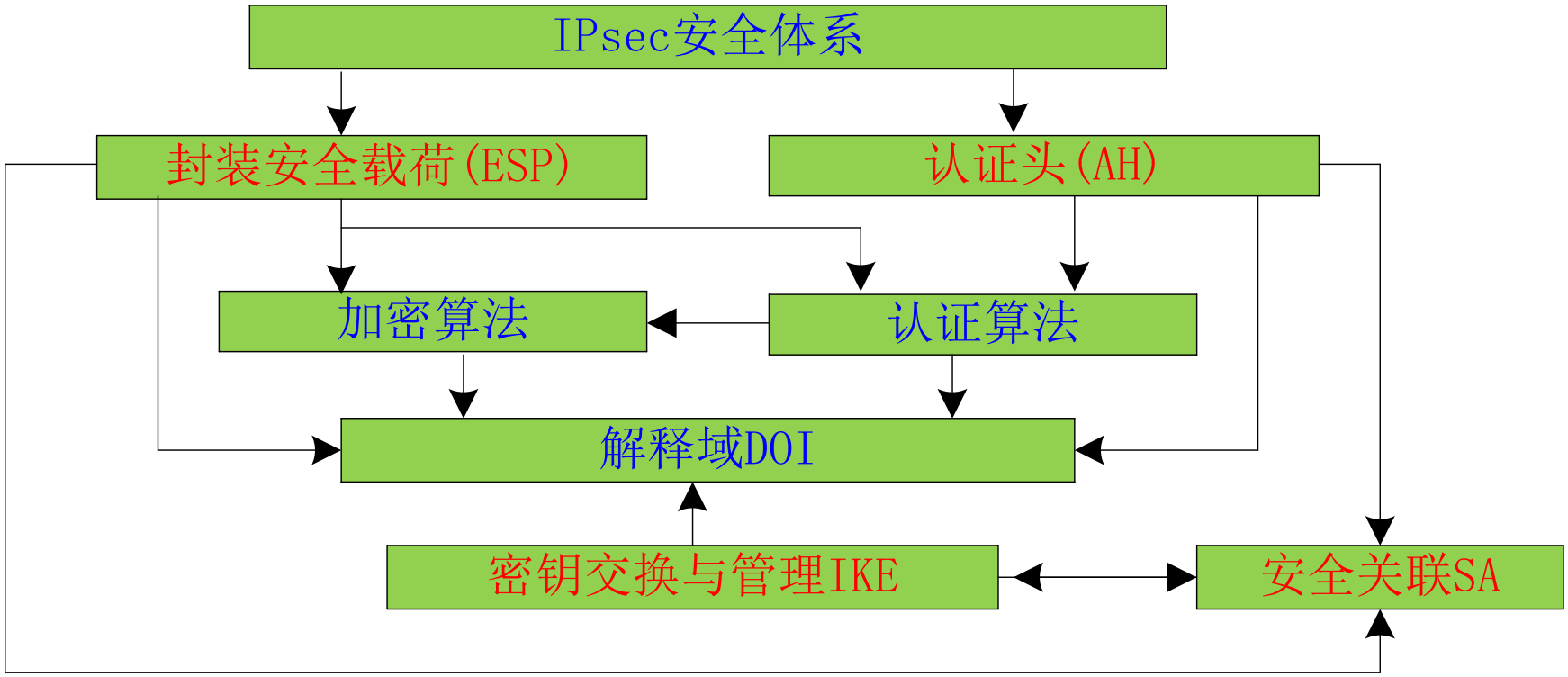
计算机网络之危机四伏

主讲人：李全龙

本讲主题

IP安全（IPsec）（1）

IPsec体系结构

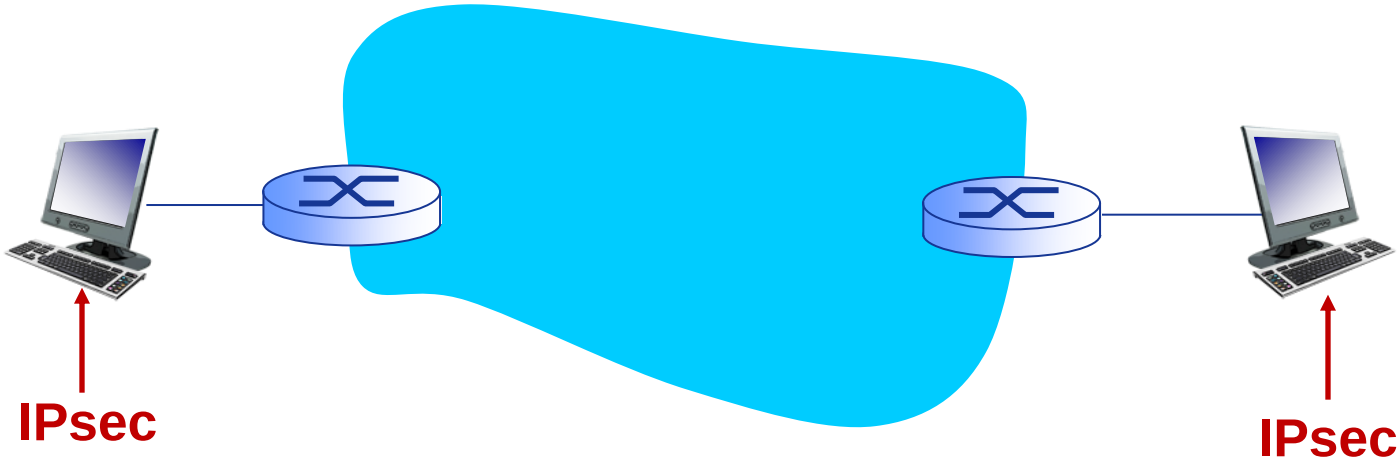

IPsec安全体系
封装安全载荷(ESP)
认证头(AH)
加密算法
认证算法
解释域DOI
密钥交换与管理IKE
安全关联SA

IPsec服务

- 机密性(confidentiality)
- 数据完整性(data integrity)
- 源认证/鉴别(origin authentication)
- 重放攻击预防(replay attack prevention)

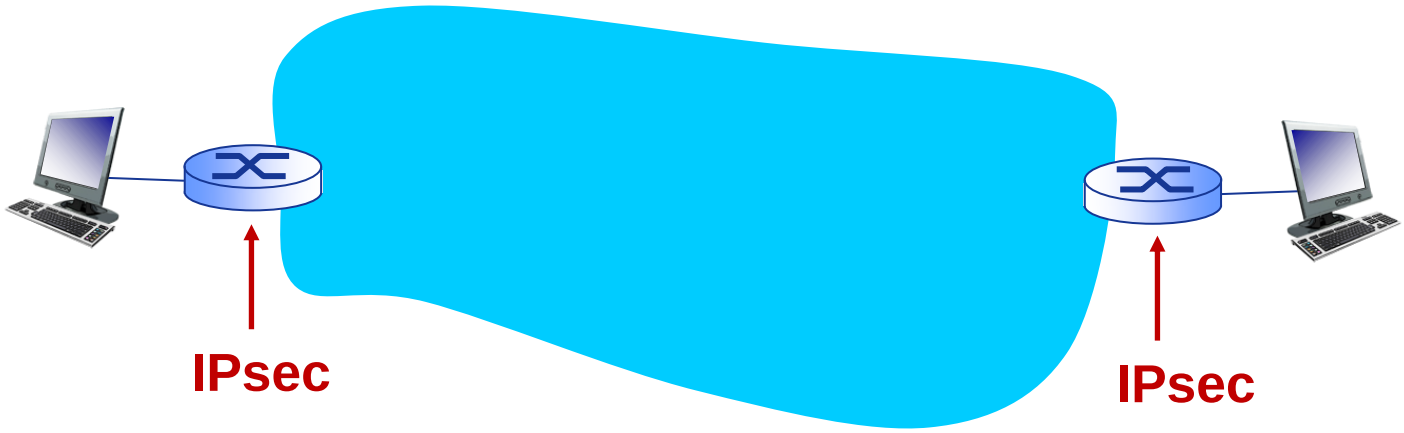
- 提供不同服务模型的两个协议:
  - AH
  - ESP

IPsec的传输(transport)模式



- IPsec数据报的发送与接收均由端系统完成
- 主机是IPsec感知的(IPsec-ware)

IPsec的隧道(tunneling)模式



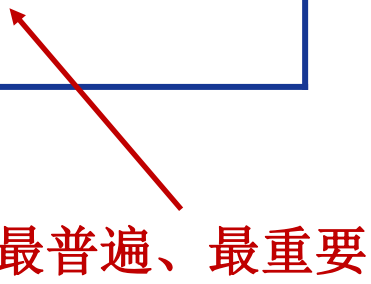
- 边缘路由器是IPsec感知的(IPsec-ware)

两个IPsec协议

- 提供IPsec服务的两个协议:
  - AH：在IP数据报文头中的协议号为51
  - ESP：在IP数据报文头中的协议号为50
- 认证头协议AH(Authentication Header)
  - 提供源认证/鉴别和数据完整性检验，但不提供机密性
- 封装安全协议ESP(Encapsulation Security Protocol)
  - 提供源认证/鉴别、数据完整性检验以及机密性
  - 比AH应用更广泛

IPsec模式与协议的4种组合!

传输模式AH	传输模式ESP
隧道模式AH	隧道模式ESP



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！