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

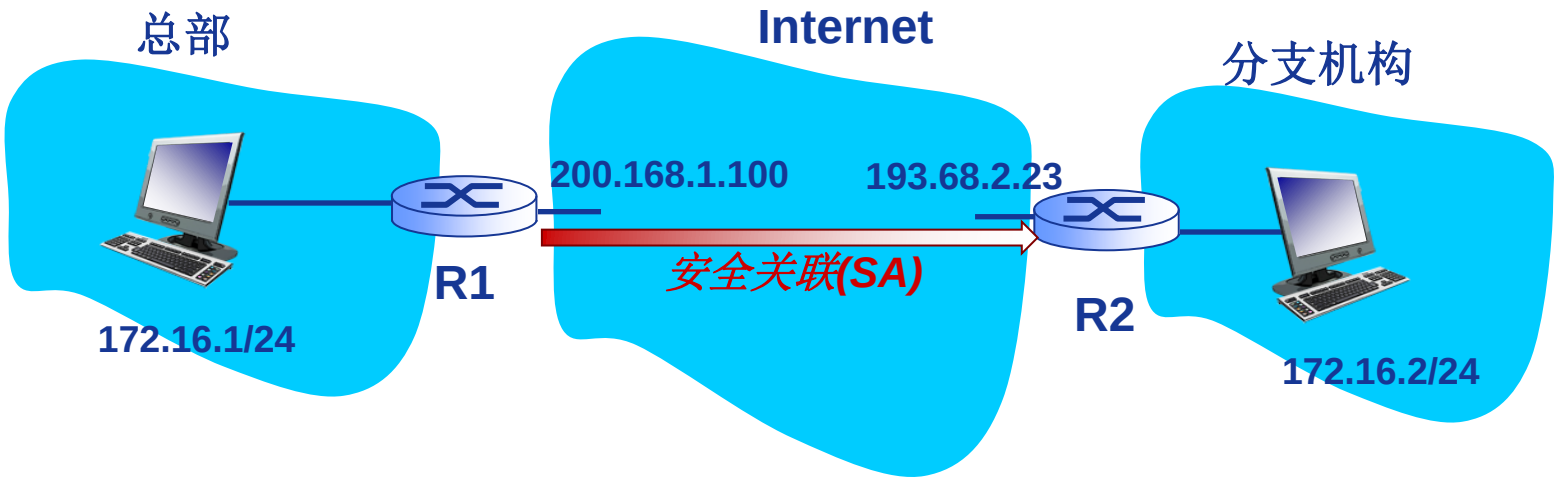
计算机网络之危机四伏

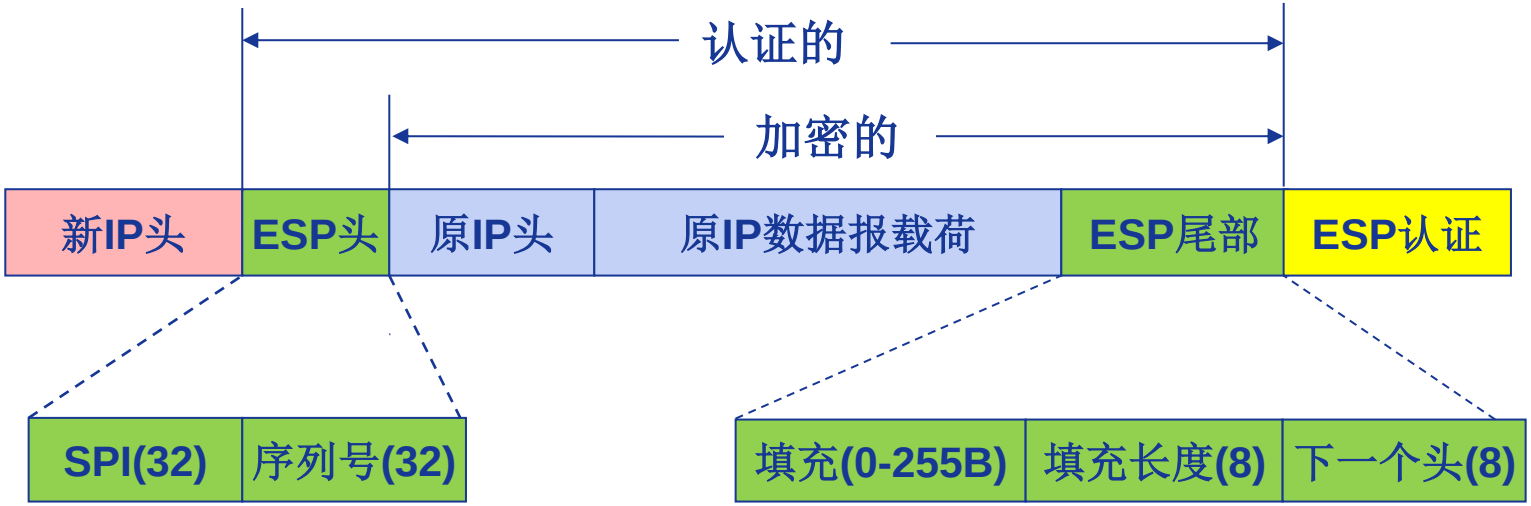
主讲人：李全龙

本讲主题

IP安全（IPsec）（4）

数据报处理过程


总部
Internet
分支机构
200.168.1.100
193.68.2.23
R1
安全关联(SA)
R2
172.16.1/24
172.16.2/24


认证的
加密的
新IP头
ESP头
原IP头
原IP数据报载荷
ESP尾部
ESP认证
SPI(32)
序列号(32)
填充(0-255B)
填充长度(8)
下一个头(8)

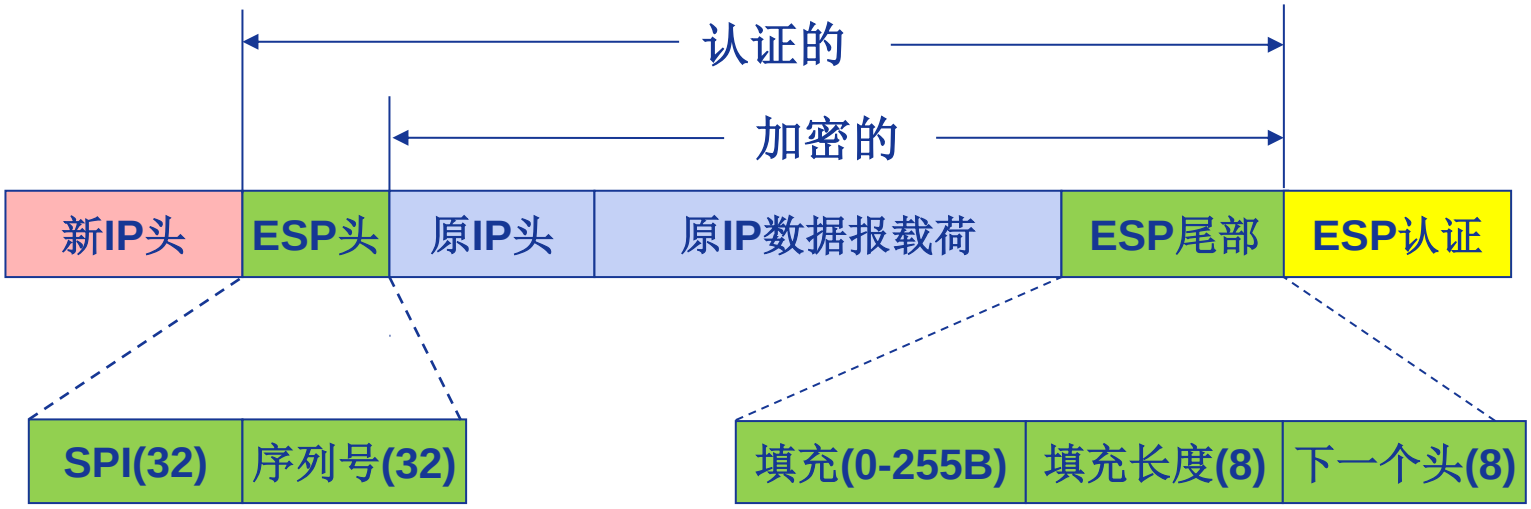
R1: 将原IP数据报转换为IPsec数据报

- 检索SPD，确定处理策略
- 检索SAD，确定SA
- 在原IP数据报(包括原IP首部域！)后面附加“ESP尾部”.
- 利用SA定义的算法与密钥，加密上述结果.
- 在加密结果前面附加“ESP头”，创建“enchilada”.
- 针对整个enchilada，利用SA定义的算法与密钥，创建报文认证码MAC;
- 在enchilada后面附加MAC，构成载荷(新IP数据报载荷);
- 构造全新的IP头，包含所有经典的IPv4首部字段;
- 将新IP头附加在载荷的前面

R2: 解封IPsec数据报

- 从原始IP数据报中提取选择符，并搜索SPD，确定处理策略
  - 丢弃或转入系统IP协议栈进行后继处理
- 判断是否为IPsec数据报
- 从头部提取<SPI>，并检索SAD
  - 若找不到SA，则触发IKE或丢弃包；
  - 若找到，则根据SA解封数据报，得到原始IP数据报

在enchilada内部:



- ESP尾部：填充以便应用分组密码
- ESP首部：
  - SPI，接收实体基于此知道该做什么
  - 序列号，抵抗重放攻击
- ESP的MAC认证字段，基于共享的秘密密钥

IPsec序列号

- 对于新SA，发送方初始化序列号为0
- 每次通过SA发送数据报:
  - 发送方增加序列号计数器（加1）
  - 将计数器值置于序列号字段
- 目的：
  - 预防嗅探与回放分组攻击
  - 接收重复的、已认证的IP分组，会破坏正常服务
- 方法：
  - 接收方检验分组重复
  - 无需记录所有已接收分组；而是利用一个窗口

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！