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）（5）

SA的建立和密钥管理

IPsec支持两种方式的SA建立和密钥管理：

- 手工方式
  - 所有的信息需要手工配置
  - SA永远存在
  - 适用于结构简单的网络
- 自动方式
  - SA可以通过协商方式产生
  - SA过期以后重新协商，提高了安全性
  - 适用于较复杂拓扑和较高安全性的网络

Internet密钥交换(IKE)

- 前面的例子：在IPsec端点，手工建立IPsec SA

  Example SA

  SPI: 12345

  Source IP: 200.168.1.100

  Dest IP: 193.68.2.23

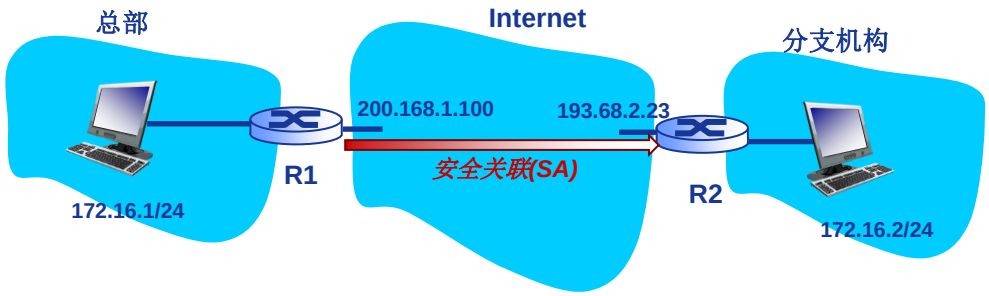
  Protocol: ESP

  Encryption algorithm: 3DES-cbc

  HMAC algorithm: MD5

  Encryption key: 0x7aeaca…

  HMAC key:0xc0291f…



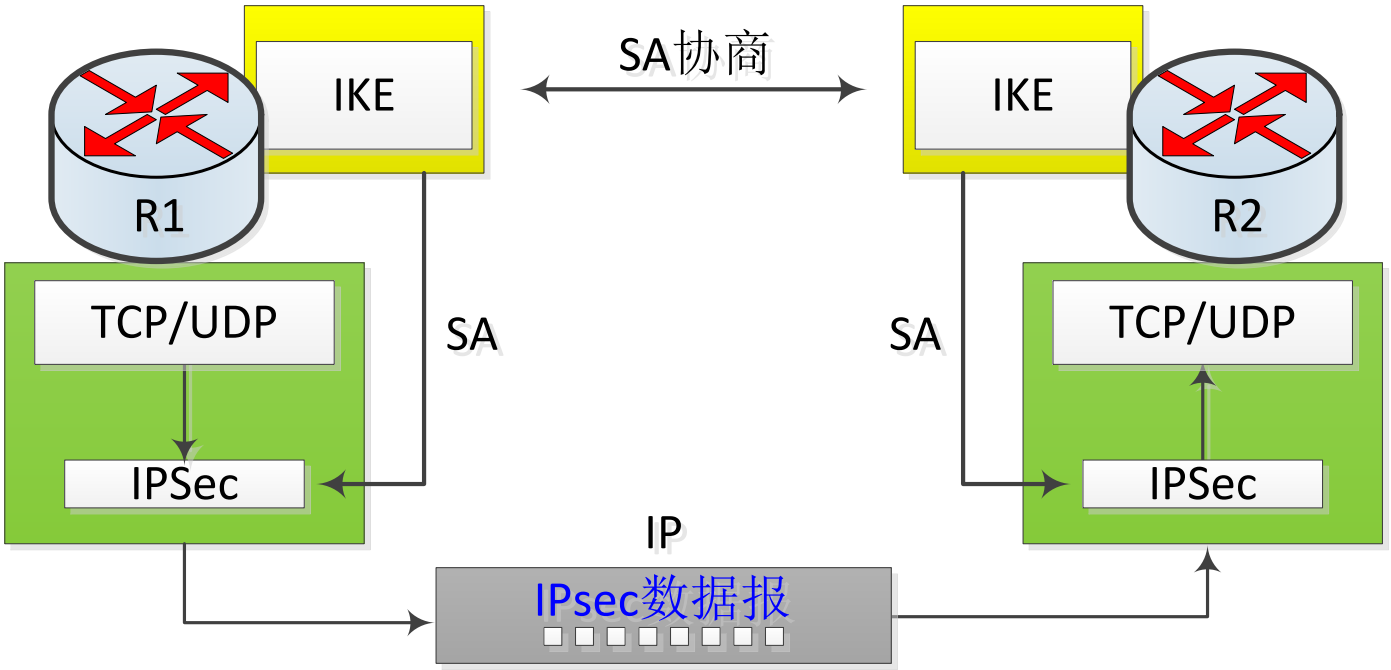
- 对于几百个端点规模的VPN，手工设置密钥是不可行的
- 替代方案：IPsec IKE (Internet Key Exchange)

Internet密钥交换(IKE)

- IKE协议可自动管理SA的建立、协商、修改和删除，是IPSec唯一的密钥管理协议
- IKE：
  - ISAKMP(Internet Security Association and Key Management Protocol)的通用框架
    - 定义了协商、建立、修改和删除SA过程的通用框架
  - OAKLEY的密钥交换模式
    - 一个密钥交换协议，允许认证过的双方通过不安全的网络交换密钥参数
  - SKEME的共享和密钥更新技术
    - 提供了IKE交换密钥的算法

IKE和IPSec

- IKE为IPSec提供服务：
  - 密钥交换与管理
  - 身份认证：通信对等体的认证
  - IPSec SA的协商与管理



IKE: PSK与PKI

- 认证可以通过：
  - 预共享密钥 (PSK)，或者
  - 公钥基础设施PKI (公开/私有密钥对以及证书).
- PSK：基于共享的秘密密钥
  - 运行IKE认证彼此，并建立IPsec SAs (每个方向一个)
  - 包括加密秘钥和认证密钥
- PKI：基于公开/私有密钥对以及证书
  - 运行IKE认证彼此，并建立IPsec SAs (每个方向一个)
  - 类似于SSL的握手过程

IKE的阶段

IKE包括两个阶段：

- 阶段1：建立双向IKE SA(也称为ISAKMP安全关联)
  - 为双方进一步的IKE通信提供机密性、数据完整性以及数据源认证服务
  - 注意：IKE SA不同于IPsec SA
  - 两种模式：
    - 野蛮模式(aggressive mode)
      - 3个消息交互，使用较少的消息
    - 主模式(main mode)
      - 6个消息交互
      - 主模式提供身份保护(identity protection)，并且更灵活
- 阶段2：基于ISAKMP协议，进行IPsec SA的安全协商

IPsec总结

- IKE用于交换算法、秘密密钥、SPI
- 采用AH协议或者ESP协议 (或者两者)
  - AH提供完整性、源认证服务
  - ESP提供完整性、源认证以及机密性服务
- IPsec对等端可以是：
  - 两个端系统
  - 两个路由器/防火墙
  - 一个路由器/防火墙与一个端系统

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！