Instituto de Informática - UFRGS

Redes de Computadores

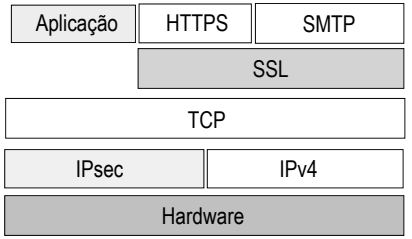
IPsec

Virtual Private Network (VPN)

Aula 29

Introdução

- Os protocolos Internet (TCP/IP) não seguros
  - Necessidade de inserir garantias para segurança da informação
- Duas "correntes" ideológicas
  - "fim a fim": a segurança é uma questão dos processos que se comunicam (camada de aplicação ou camada de transporte)
  - "infraestrutura de rede":autentica e/ou cifra os datagramas sem envolver as aplicações
- IP *security*



IP Security (IPsec)

- IP*sec* é especificação de um conjunto de serviços
  - Nem todos querem "pagar" o preço computacional necessário a criptografia
  - Fornece uma estrutura e um mecanismo deixando a escolha do usuário o tipo de cifragem, autenticação e métodos de *hashing*
  - Descrito nas RFCs 2401, 2402 e 2406
- Benefícios de IP*sec*
  - Transparente para as aplicações (abaixo do nível de transporte (TCP, UDP))
  - Oferece seguranca para usuários individuais
- Principais serviços:
  - Confidencialidade, integridade e autencidade
  - Proteção contra ataques de reprodução (*reply*)

Características do IPsec

- É um protocolo orientado a conexão ("à la TCP")
  - *Security Association* (SA) na terminologia IPsec
  - Objetivo é "amortizar" os custos de configuração da segurança
- SA é uma conexão é unidirecional (*simplex*)
  - Possui um identificador associado a ela
  - Comunicação bidirecional necessita duas SAs
- Dois modos de operação:
  - Transporte e túnel
- Dois protocolos de segurança:
  - *Authentication Header* (AH) e *Encapsulating Security* (ESP)

Security Association (SA)

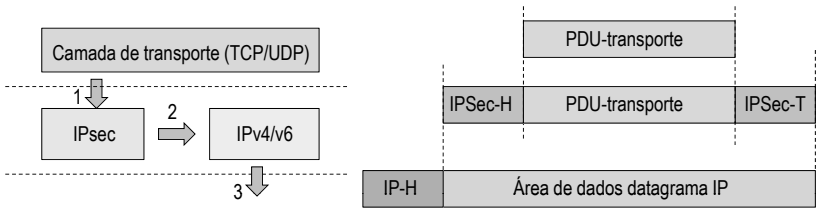
- Estabelecido através de um protocolo de sinalização
- Define uma conexão entre dois pontos
- Identificada por:
  - Um SPI (*Security Parameter Index*) que age como um identificador de circuito virtual ou par de endpoints (*sockets*)
  - Tipo do protocolo usado para a segurança (AH ou ESP)
  - O endereço IP de destino

Gerenciamento de Chaves

- Relacionado com a determinação e a distribuição de chaves
- Dois tipos:
  - Manual: configurado pelo administrador da rede
  - Automática: gerado sob demanda
    - *Oakley Key Determination Protocol (Internet Key Excahnge – iKE)*
      - Baseado em Diffie-Hellman
    - *Internet Security Association and Key Management Protocol (ISAKMP)*
      - Define formatos de pacotes

Modo de transporte

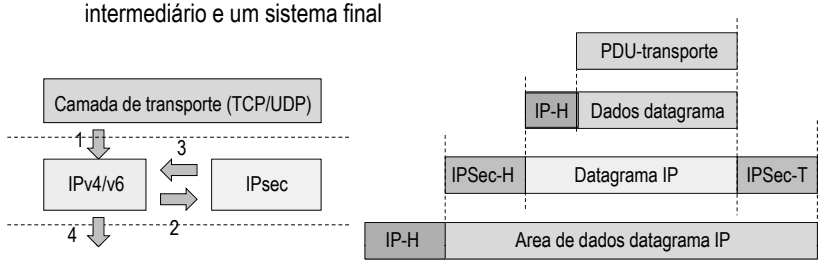
- Protege apenas a carga útil de um datagrama IP
  - Corresponde a T-PDU (cabeçalho TCP/UDP + dados)
- Emprego típico
  - Proteção de dados fim-a-fim
  - Emissor autentica e/ou cifra os dados e receptor verifica integridade e/ou decifra



H = Header; T = Tail

Modo de túnel

- Protege o datagrama IP inteiro
  - Cria um novo datagrama IP com um cabeçalho com informações diferentes do datagrama IP original
- Emprego típico
  - Usado entre dois sistemas intermediários (roteador) ou entre um sistema intermediário e um sistema final

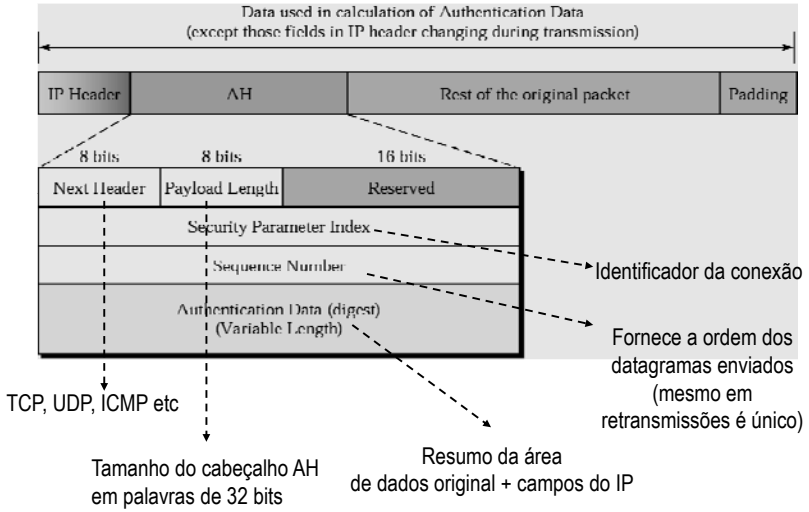


H = Header; T = Tail

Protocolo *Authentication Header* (AH)

- Objetivos:
  - Autenticar a origem e assegurar a integridade da mensagem
  - Não oferece confidencialidade
- Procedimento:
  - Calcula uma função de resumo com o corpo da mensagem usando uma função de *hashing* e uma chave simétrica
    - Chave é negociada antes de se instalar a SA
  - Insere o resumo no cabeçalho AH antes da área de dados (*payload*)
  - O cabeçalho IP é adicionado indicando 51 como tipo de protocolo

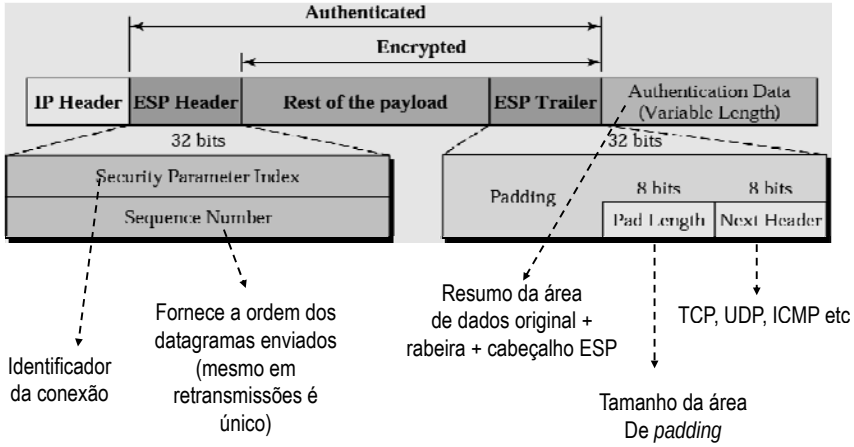
Descrição dos campos do protocolo AH



Protocolo *Encapsulating Security Payload* (ESP)

- Objetivo:
  - Fornecer autenticação da origem, integridade e confidencialidade
- Procedimento:
  - Uma "rabeira" ESP é adicionada a área de dados do datagrama
  - A área de dados e a rabeira são cifrados, formando uma nova área de dados
  - Um cabeçalho ESP é adicionado a nova área de dados →novo datagrama
  - Gera informação de autenticação (resumo) do novo datagrama
  - Agrega autenticação no final da rabeira
  - Insere cabeçalho IP indicando 50 como tipo de protocolo

Descrição dos campos do protocolo ESP

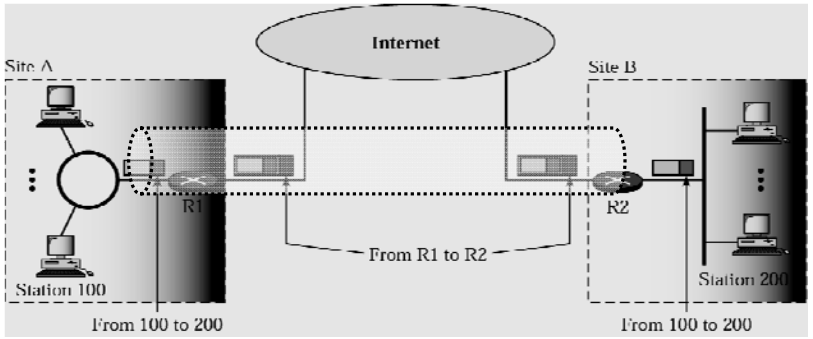


Virtual Private Networks (VPNs)

- Rede privadas são usadas dentro de uma organização fornecendo privacidade e acesso a recursos compartilhados
- Emprega o protocolo ESP em modo túnel
- Ideia da extranet
  - É uma intranet coorporativa exceto pelo fato que alguns recursos podem ser acessados por usuários externos a rede da organização
    - (intranet = rede privativa que usa o modelo Internet, i.é., roda aplicativos baseados em TCP/IP limitando o acesso a seus usuários internos)
- Endereçamento é baseado em IP
  - Normalmente utiliza os endereços privativos ou não roteáveis
    - 10.0.0.0/8 ; 172.16.0.0/12 e 192.168.0.0/16

Princípio de funcionamento

Emprega IPsec no modo túnel



Os datagramas de comunicação entre as máquinas 100 e 200 são tunelados sobre um datagrama IP enviado, no caso, pelos roteadores responsáveis por implementar a VPN.

Leituras complementares

- Tanenbaum, A. *Redes de Computadores* (4ª edição), Campus 2003.
  - Capítulo 8 (seção 8.6)