Engenharia de Segurança

IPsec

Profa. Dra. Kalinka Regina Lucas Jaquie Castelo Branco
kalinka@icmc.usp.br

Segurança da Comunicação

Tópicos

- IPSec
- Firewalls
- Redes Privadas Virtuais
- Segurança sem fio
  - Segurança de redes 802.11
  - Segurança do Bluetooth
  - Segurança do WAP 2.0

Segurança da Comunicação

- Atualmente o *Internet Protocol* (IP) possui diversas vulnerabilidades ainda muito exploradas, permitindo por exemplo,
  - a monitoração não autorizada de pacotes de dados trocados entre dois hosts,
  - a exploração de aplicações cuja autenticação é feita baseada no endereço IP.
- **Solução**: **IPSec**

Segurança da Comunicação

IPSec (IP Security)

- A segurança na camada de rede engloba duas áreas funcionais:
  - **autenticação** e
  - **privacidade**.
- **Autenticação** - garante que um pacote recebido foi de fato transmitido pelo nó identificado como origem no cabeçalho do pacote. Além disso, esse mecanismo também assegura que o pacote não foi alterado enquanto transitava pela rede.
- **Privacidade** - permite que sejam criptografadas mensagens de modo a evitar que essas possam ser interceptadas e lidas por terceiros.

Segurança da Comunicação

IPSec (IP Security)

- Estrutura de padrões abertos para assegurar na rede de IP uma comunicação privada segura.
- **Assegura**: confidencialidade, integridade e autenticidade para a comunicação de dados em uma rede pública de IP.
- Pacote criptografado de IPSec – similar ao pacote comum de IP (redução de custos de implementação e de gerenciamento).

Vantagem: Transparente para o usuário (utiliza a camada de rede).

Segurança da Comunicação

IPSec (IP Security)

- Estrutura para **vários serviços**, **algoritmos** e **granularidades**.
- **Principais serviços**:
  - Sigilo
  - Integridade de dados
  - Proteção contra ataques de reprodução
- Serviços baseados em **criptografia de chave simétrica** – alto desempenho é importante.

Segurança da Comunicação

IPSec (IP Security)

- **Vários algoritmos** ? torná-lo independente do tipo de algoritmo utilizado (menos susceptível à violação, a flexibilidade permite que sejam utilizadas as normas mais recentes disponíveis, incrementando a segurança).
- **Várias granularidades** ? tornar possível a proteção de uma única conexão TCP,
  - de todo o tráfego entre um par de hosts ou
  - de todo o tráfego entre um par de roteadores seguros, etc.

Segurança da Comunicação

IPSec (IP Security)

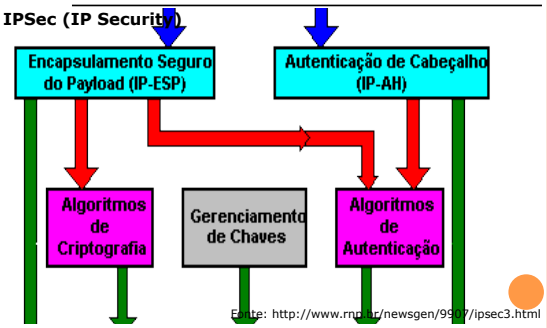
- Embora esteja na camada de IP é orientado à conexão
- **Denominação da conexão** - SA (*Security Association*)
  - Conexão simplex entre dois pontos extremos e tem um identificador de segurança associado a mesma.
  - Se houver necessidade de tráfego seguro em ambos os sentidos – serão exigidas duas associações de segurança.
  - Identificadores de segurança – transportados em pacotes, percorrem as conexões seguras e são usados para pesquisar chaves e outras informações relevantes ao chegar um pacote seguro.

SEGURANÇA DA COMUNICAÇÃO

IPSec (IP Security)

- Uma entidade deseja estabelecer uma associação de segurança - utiliza um SPI (*Security Parameter Index*) e um endereço de destino (da entidade na qual se deseja fazer a comunicação segura) e envia essas informações à entidade com que se quer estabelecer o canal seguro.
- Para cada sessão de comunicação autenticada serão necessários dois SPIs, ou seja, um para cada sentido, devido ao fato de que a associação de segurança ser **unidirecional**.

SEGURANÇA DA COMUNICAÇÃO



Fonte: http://www.rnp.br/newsgen/9907/ipsec3.html

SEGURANÇA DA COMUNICAÇÃO

IPSec (IP Security)

- Mecanismos de segurança inclusos no IPSec (definidos pelas especificações do IPv6)
  - autenticação de cabeçalho (AH - *authentication header*)
  - segurança do encapsulamento IP (ESP - *encrypted security payload*).
- Os cabeçalhos de extensão se seguem ao cabeçalho IP principal.
  - Cabeçalho de autenticação - AH
  - Cabeçalho para privacidade - ESP.
- O IPSec no IPv6 encripta os dados em todo o seu percurso enquanto no IPv4 os dados apenas podiam se encriptados entre roteadores da camada de distribuição.

SEGURANÇA DA COMUNICAÇÃO

IPSec (IP Security)

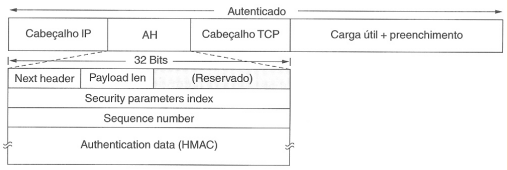
Autenticação de cabeçalho

- assegura ao destinatário que os dados IP são realmente do remetente indicado no endereço de origem, e que o conteúdo foi entregue sem modificações.
- Exemplo de algoritmo de autenticação utilizado: **MD5**.

Segurança do encapsulamento IP

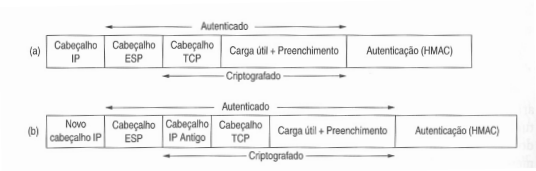
- permite confidencialidade, autenticação da origem e integridade dos dados encapsulados no pacote IP.
- Exemplo de algoritmo de criptografia: **DES/3DES**

SEGURANÇA DA COMUNICAÇÃO



Cabeçalho de autenticação do IPSec.

SEGURANÇA DA COMUNICAÇÃO



(a) ESP em modo de transporte **b) ESP em modo de túnel**

SEGURANÇA DA COMUNICAÇÃO

IPSec (IP Security)

- Os algoritmos de autenticação e criptografia utilizam o conceito de associação de segurança entre o transmissor e o receptor.
  - o transmissor e o receptor devem concordar com uma chave secreta e com outros parâmetros relacionados à segurança, conhecidos apenas pelos membros da associação.
  - Para gerar as chaves provavelmente será utilizado o IKMP (*Internet Key Management Protocol*).
- Uma empresa pode usar uma rede TCP/IP privada segura eliminando os links com instalações não-confiáveis, cifrando os pacotes que deixam as suas instalações físicas e autenticando os pacotes que entram nas suas instalações físicas.

Engenharia de Segurança

IPsec

Profa. Dra. Kalinka Regina Lucas Jaquie Castelo Branco

kalinka@icmc.usp.br