Criptografia Aplicada

IPSec e SSH

Sumário

- Contextualização
- IPSec
- SSH

Contextualização

- Protocolos de segurança são fundamentais para estabelecer confiança em comunicações via redes de computadores
- Definem um conjunto de procedimentos para assegurar que os dados transmitidos sejam seguros
  - confidencialidade, integridade, autenticidade, etc.
- Através deles, podemos:
  - negociar algoritmos a serem utilizados;
  - autenticar os participantes da comunicação;
  - fazer um acordo seguro de chaves (de sessão, de cifragem, etc.);
  - estabelecer uma comunicação segura;
  - entre outros.
- Exemplos:
  - SSL/TLS, IPsec, SSH, Kerberos.

Contextualização

- Tanto o TLS quando o IPSec são utilizados para proteger dados trafegados entre dispositivos e proteger tráfego de rede
- A diferença entre eles é a camada no qual operam
  - TLS fica entre a camada de transporte (TPC) e a de serviços
  - IPSec opera na camada de rede
- Já o SSH é um protocolo utilizado para administrar dispositivos remotos de forma segura

Sumário

- Contextualização
- **IPSec**
- SSH

IPSec

- Criado na década de 90 pelo *Internet Engineering Task Force*
- IPSec é uma extensão do protocolo IP
- O protocolo IP é o principal protocolo de roteamento de pacotes na internet
  - se preocupa com conexão e entrega de pacotes
  - não utiliza criptografia por *default*
- IPSec adiciona criptografia ao protocolo IP
  - garantia de integridade, autenticidade e confidencialidade dos pacotes
- Normalmente utiliza a porta 500
- Mais detalhes: RFC6071

IPSec - protocolos

O IPSec consiste de uma série de protocolos. Listamos alguns abaixo

- Authentication Header (AH):
  - adiciona um cabeçalho que contém dados para a autenticação do remetente
  - protege o conteúdo do pacote contra modificações por partes não autorizadas.
- Encapsulating Security Protocol (ESP)
  - Dependendo do modo selecionado, criptografa todo o pacote IP ou apenas o conteúdo
  - adiciona um cabeçalho e um rodapé ao pacote de dados após a encriptação.
- Security Association (SA)
  - se refere a uma série de protocolos usados para negociação de chaves e algoritmos
  - o protocolo SA mais utilizado é o Internet Key Exchange (IKE)

Como funciona o IPSec?

Visão geral:

- Emissor inicia uma transmissão para o destinatário utilizando IPSec
- Emissor e destinatário negociam os requisitos para o estabelecimento de uma conexão segura
  - Algoritmos, chaves, e outros parâmetros do protocolo SA
- Pacotes são enviados e recebidos de forma criptografada
  - decifragem, verificação de integridade e autenticidade são feitas
- Conexão IPSec é encerrada

Como funciona o IPSec?

As conexões IPSec incluem os seguintes passos:

- **Troca de chaves**: dispositivos conectados fazem um acordo de chaves para poder cifrar e decifrar mensagens entre eles
- **Autenticação**: cada pacote é autenticado para garantir sua origem
- **Cifragem**: pacotes são cifrados e decifrados com criptografia simétrica
- **Transmissão**: pacotes cifrados são transmitidos através de uma ou mais redes de computadores usando um protocolo de transporte
- **Pacotes e cabeçalhos**: todos os dados enviados são divididos em pedaços menores chamados de pacotes, que contém o conteúdo e um cabeçalho. O cabeçalho contém informações importantes sobre o pacote, como informações de autenticação e criptografia

Modo de transporte x modo de tunelamento

- IPSec opera em dois modos diferentes
- Modo de transporte:
  - somente o conteúdo do pacote (payload) é cifrado
  - o cabeçalho (header) do IP permanece intacto, permitindo que roteadores identifiquem o endereço do destino
- Modo de túnel
  - tanto o conteúdo do pacote quando o cabeçalho são cifrados
  - um novo cabeçalho IP é adicionado para auxiliar roteadores intermediários
  - mais adequado para a transferência de dados em redes públicas

VPN IPSec

- Uma Virtual Private Network (VPN) é uma aplicação que permite fazer uma conexão cifrada entre dois ou mais computadores
- Permitem o acesso e troca segura de dados confidenciais
- Muitas VPNs utilizam o protocolo IPSec
- Também é possível utilizar o protocolo TLS

Segurança

- Replay attacks:
  - interceptação e retransmissão de pacotes capturados
  - obter acesso não autorizado
  - proteção contra o ataque no ESP e no AH usando um Sequence Number
- Man-in-the-Middle:
  - atancante consegue interceptar e manipular a troca de chaves no IKEv1
  - IKEv2 trouxe melhorias nesse problema
- Ataques no DH
  - existem alguns grupos padronizados para o uso de DH em diversos protocolos (primos de 512 bits)
  - pré-cálculo de operações nesses grupos e armazenamento de resultados em cluster podem permitir ataques no logaritmo discreto de maneira eficiente para esses grupos
  - permitindo derivação de chaves acordada no IKE
  - alternativa: aumentar o tamanho dos primos, utilizar outros métodos para troca de chaves

Sumário

- Contextualização
- IPSec
- **SSH**

SSH

- O *Secure Shell* (SSH) é um protocolo que permite o acesso e gerenciamento de dispositivos remotos de maneira segura
- Foi criado em 1995 Tatu Ylönen para resolver problemas de segurança em uma universidade finlandesa
- Normalmente baseado em uma arquitetura cliente/servidor
- Normalmente utiliza a porta 22

Como funciona o SSH?

Visão geral:

- Um cliente inicia uma conexão SSH em um servidor
- Cliente e servidor negociam algoritmos e estabelecem uma chave de sessão
- Uma autenticação do servidor é feita
- Cliente envia suas credenciais (login/senha) para autenticação no servidor
- A partir daqui, a conexão SSH é estabelecida e está pronta para uso

SSH - Protocolos

O SSH consiste em três protocolos geralmente acima da camada TCP:

- Transport Layer Protocol
- User Authentication Protocol
- Connection Protocol

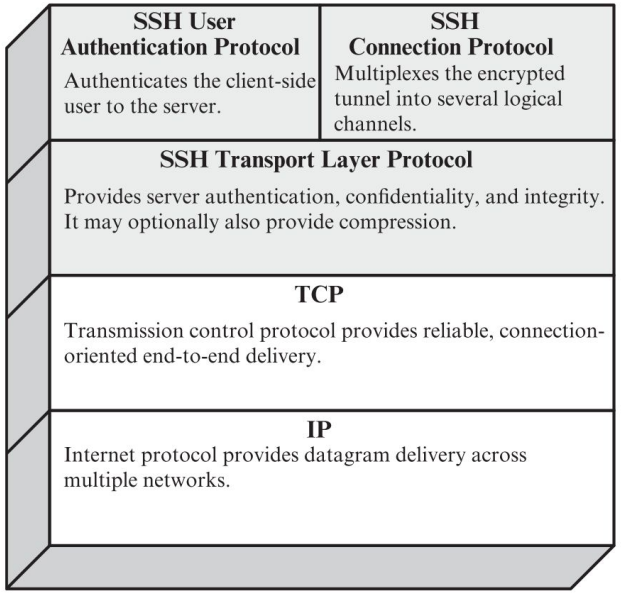

Figure 17.8 SSH Protocol Stack

Imagem: W. Stallings. *Cryptography and network security*. Cap 17.4

SSH - Protocolos

O SSH consiste em três protocolos geralmente acima da camada TCP:

- **Transport Layer Protocol:**
  - provê autenticação do servidor, confidencialidade e integridade dos dados
  - pode opcionalmente prover compressão
- User Authentication Protocol
- Connection Protocol

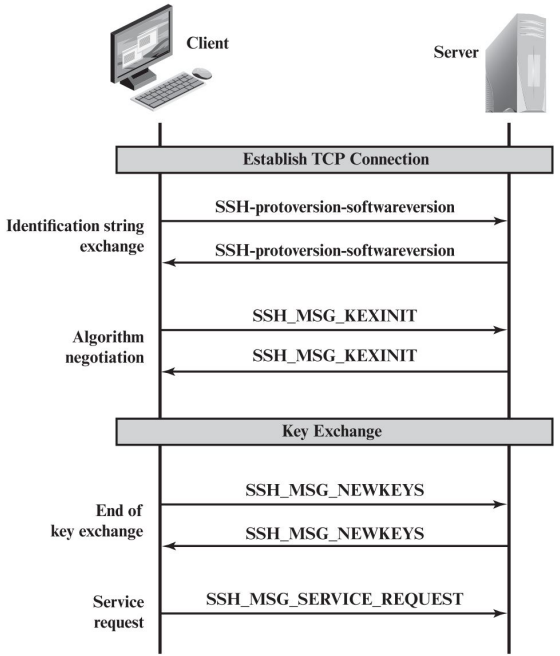

Figure 17.9 SSH Transport Layer Protocol Packet Exchanges

Imagem: W. Stallings. *Cryptography and network security*. Cap 17.4

SSH - Protocolos

O SSH consiste em três protocolos geralmente acima da camada TCP:

- Transport Layer Protocol:
  - provê autenticação do servidor, confidencialidade e integridade dos dados
  - pode opcionalmente prover compressão
- **User Authentication Protocol:**
  - autentica o usuário para o servidor
  - diversos métodos são possíveis
    - criptografia de chave pública, login/senha, etc.
- Connection Protocol

byte	`SSH_MSG_USERAUTH_REQUEST (50)`
string	user name
string	service name
string	method name
. . .	method specific fields

Imagem: W. Stallings. *Cryptography and network security*. Cap 17.4

SSH - Protocolos

O SSH consiste em três protocolos geralmente acima da camada TCP:

- Transport Layer Protocol:
  - provê autenticação do servidor, confidencialidade e integridade dos dados
  - pode opcionalmente prover compressão
- User Authentication Protocol:
  - autentica o usuário para o servidor
  - diversos métodos são possíveis
    - criptografia de chave pública, login/senha, etc.
- **Connection Protocol:**
  - combina vários canais de comunicação lógica em uma única conexão SSH
  - assume que uma conexão segura (túnel) foi estabelecida

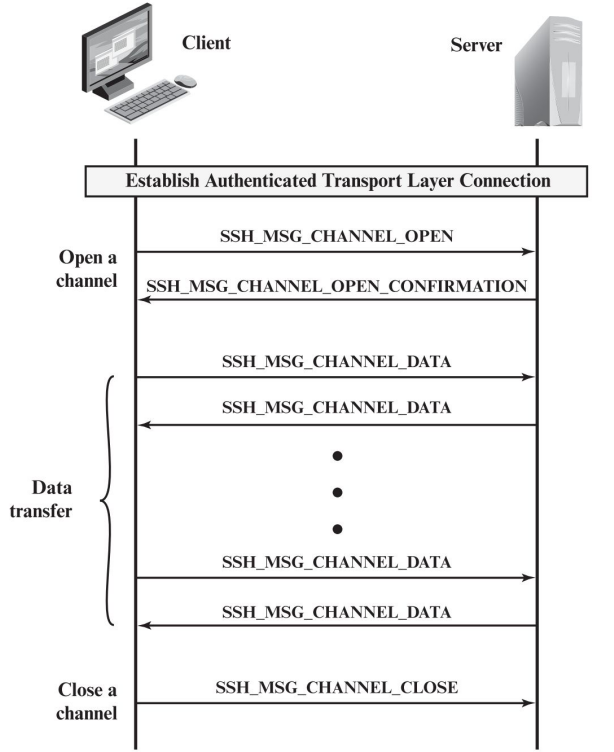

Figure 17.11 Example of SSH Connection Protocol Message Exchange

Imagem: W. Stallings. *Cryptography and network security*. Cap 17.4

LabSEC
Laboratório de Segurança em Computação

cpqd

SSH - Aplicações

- Acesso remoto seguro
- Transferência segura de arquivos
- Gerenciamento de servidores
- Execução de comandos remotos

SSH, VPN e TLS

- SSH vs VPN
  - SSH geralmente é utilizado para proteger a comunicação entre um cliente e um servidor específico
  - enquanto VPN garante um túnel criptografado para toda a rede do usuário, como se ele estivesse fisicamente conectado à rede privada
- SSH vs TLS
  - TLS é geralmente utilizado para proteger transações via web (HTTPS)
  - SSH é geralmente utilizado para gerenciamento remoto e transferência de arquivos

SSH - Segurança

- Brute Force: força bruta nas combinações de login/senha do usuário
  - ferramentas automatizadas podem testar milhares de combinações em segundos
  - segurança: limitar o número de tentativas falhas, exigir senhas fortes, etc.
- Terrapin Attack (2024): ataque no handshake permite remover uma quantidade arbitrária de mensagens e passar despercebido
  - permite downgrade dos algoritmos criptográficos
  - consequentemente permite uma autenticação menos segura
  - SSH é vulnerável quando usa ChaCha20-Poly1305 ou CBC with Encrypt-then-MAC
- entre outros
- Atualizações de segurança geralmente são feitas rapidamente para corrigir os problemas.

Referências

- W. Stallings. *Cryptography and network security*. 7a edição. Capítulos 17.4.
- AWS. *O que é IPSec?*
- Cloudfare. What is IPsec? | How IPsec VPNs work
- RD Station. Descubra o que é o protocolo Secure Shell (SSH)
- RFC6071: IP Security (IPsec) and Internet Key Exchange (IKE) Document Roadmap
- RFC2409: The Internet Key Exchange (IKE)
- RFC4302: IP Authentication Header
- NISTIR 7966: Security of Interactive and Automated Access Management Using Secure Shell (SSH)
- RFC4253: The Secure Shell (SSH) Transport Layer Protocol