Shell Segura (SSH)

Jaime Cohen

2018

Sumário

Secure Shell (SSH)

Secure Shell (SSH)

- Login Remoto Seguro
- Protocolo de comunicação segura
  - autenticação
  - sigilo
  - integridade de dados
- Protocolo de Autenticação
- Protocolo de Conexão: túneis seguros
- RFC 4251 (complementada por outras)

Usos

- login remoto seguro (substitui telnet e rlogin)
- execução de comandos em host remoto (substitui rsh)
- transferência de arquivos segura
- usado em aplicações de backup e espelhamento (rsync,unison)
- tunelamento e encaminhamento
- navegar na web via proxy criptografada (SOCKS)
- implementação de VPN
- redirecionamento gráfico (X)
- montar diretório remoto no computar local (sshfs)

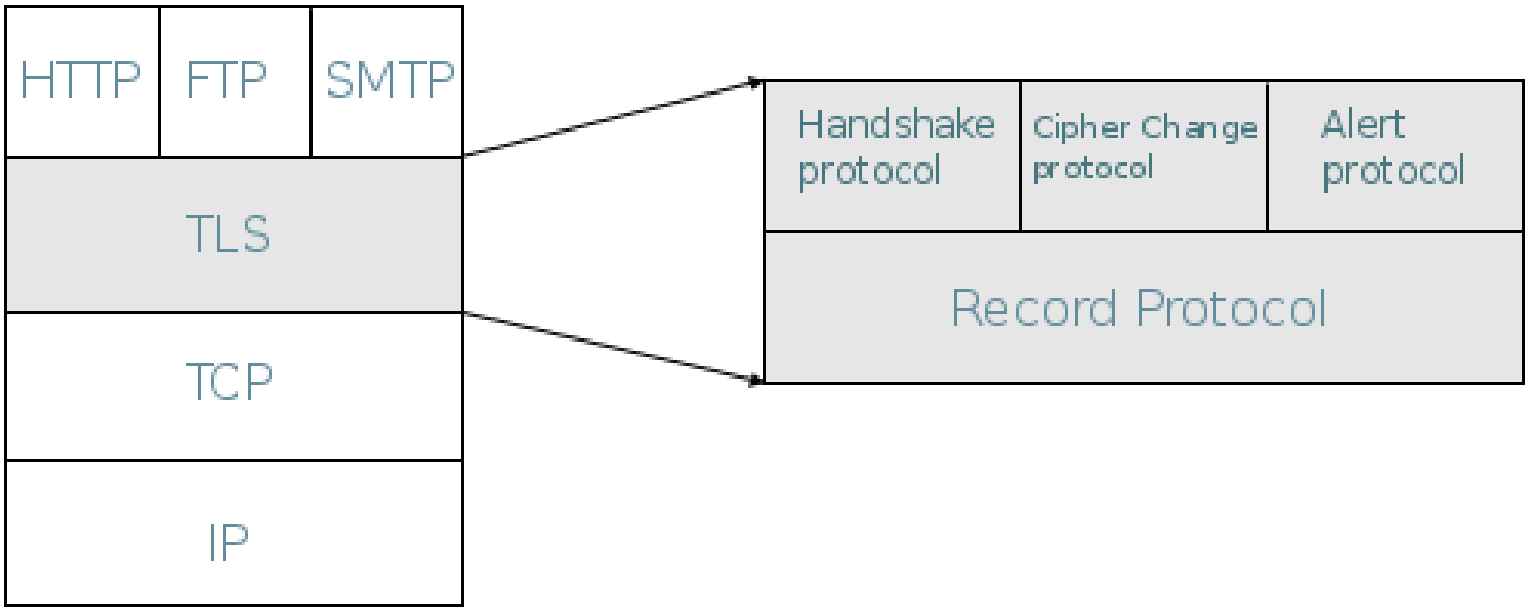
Propriedades

- Sigilo
- Integridade de dados
- Autenticação
- Detecção de ataques

Secure Socket Layer - SSL

- TLS - Transport Layer Security
- SSL - Secure Socket Layer

Secure Socket Layer - SSL



Secure Socket Layer - SSL

- Autenticação por chave pública (certificado digital)
- Comunicação usando criptografia simétrica (e.g. AES-CBC)
- Código de autenticação de mensagens (MAC) e numeração das mensagens
- *Forward secrecy* - protege comunicação anteriores
- Configuração e negociação dos algortimos

Secure Socket Layer - SSL

tipos de mensagens SSL

- Handshake
- Mudança de algoritmos
- Aplicação
- Alerta
- Heartbeat

Alertas

- MAC incorreto
- Problemas no certificado
- outros

Login Remoto

Certificados digitais

- Geração local das chaves: par de arquivos (chave privada, chave pública)
- ssh-keygen
  - parâmetros: tipo, tamanho, nome do arquivo
- permite login automático
- mais seguro contra ataque de força bruta do que login/senha

Chave Pública

Tipos suportados pelo ssh-keygen

- rsa
- dsa
- ecdsa
- ed25519

Chaves Autorizadas

- Pasta `.ssh`
- Arquivo `authorized_keys`
- Anexa a chave pública no arquivo `authorized_keys`

Chave Pública

Comando que gera o par de chaves (chave pública, chave privada).

```
ssh-keygen -t rsa -b 4096 -f filename
```

- os arquivos com as chaves devem estar no diretório .ssh local

Chaves Autorizadas

Copia a chave pública para a máquina remota

```
ssh-copy-id -i ~/.ssh/nome-da-chave user@host
```

Automatização

- ssh-agent
- Arquivo `config`

Automatização com config

```
Host *
AddressFamily inet
ServerAliveInterval 100
ServerAliveCountMax 3

Host home
    # PubkeyAuthentication=no
    IdentityFile ~/.ssh/nome-da-arquivo
    HostName example.com # ou End. IP
    User apollo
    Port 4567
```

Configuração de Tunel no Config

```
Host server-name
PubkeyAuthentication=no
ProxyCommand ssh hostname nc via-this-host 22
User jaime
```

Usos do SSH

Comandos remotos: `ssh user@host commando`

Login: `ssh user@host`

Aplicações gráficas no linux: `ssh -X`

Usos do SSH - Túneis

```
ssh -L porta_local:host_dest:porta user@host
```

Usos do SSH - Túneis

```
$ ssh -f -N -L3310:localhost:3306 servidor
$ mysqldump -P 3310 -h 127.0.0.1 \
  <opções do comando mysqldump>
```

SOCKS - navegando por proxy

```
ssh -D porta user@servidor
```

outras opções:

```
ssh -C -N -f -o ServerAliveInterval=100 \
    -o  ServerAliveCountMax=3 -D 5003 \
    user@servidor
```