Comunicação segura

Nuno Neves
Departamento de Informática
Faculdade de Ciências da Universidade de Lisboa

Comunicação segura

- Propriedades
- Concretização genérica
- Comunicação segura nas várias camadas
- SSL/TLS
- IPSec
- SSH

Comunicação segura

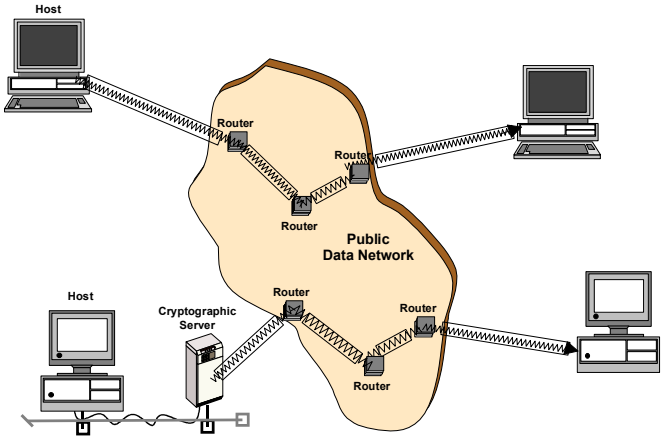
- Propriedades
  - Confidencialidade
    - Chaves de sessão
  - Autenticidade
  - Integridade
- Concretização genérica
  - Criptografia simétrica
  - Criptografia assimétrica

Comunicação segura nas várias camadas

- Aplicação - S/MIME, OpenPGP, SSH
- Transporte - SSL/TLS
- Rede - IPSec
- Ligação de dados - IEEE 802.11, Bluetooth
- Físico - Circuito Físico Seguro

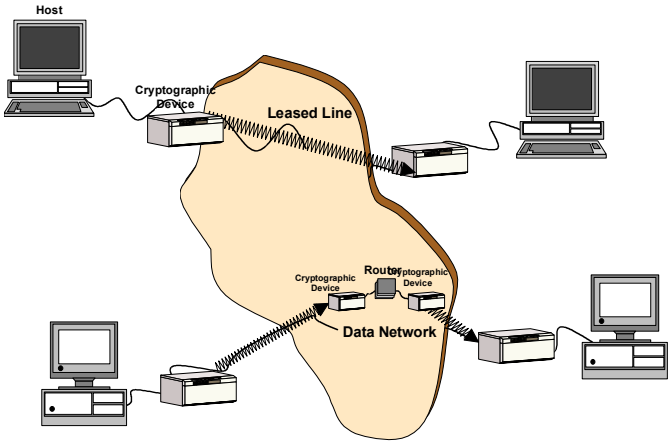
- Comunicação segura entre extremos
  - Aplicação, transporte, rede
- Comunicação em troços
  - Ligação de dados (MAC), físico

Comunicação segura entre extremos



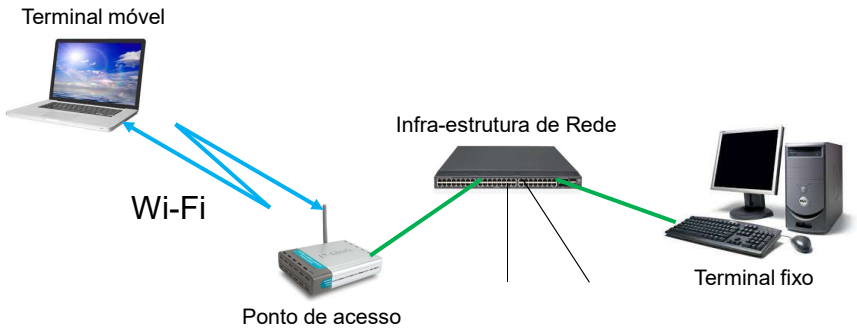
 5

Comunicação segura em troços



 6

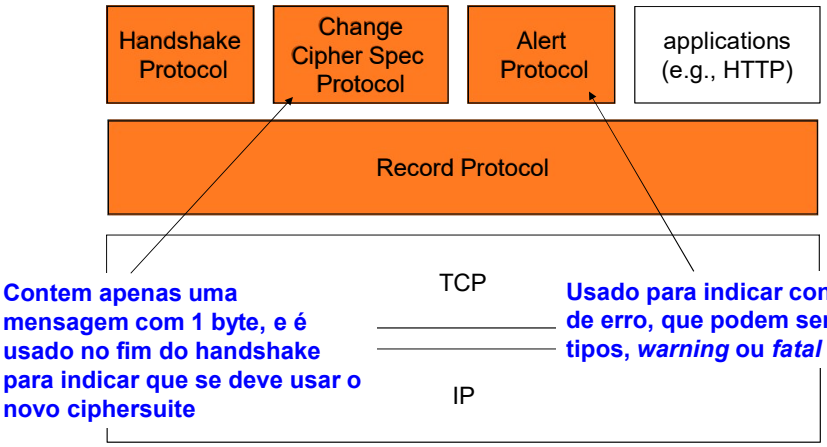
Comunicação segura em troços / extremos



SSL - Secure Sockets Layer & TLS – Transport Layer Security

- Breve histórico:
  - SSL v2 criado pela Netscape em 1994
  - Versão 3.0 surgiu em 1996 corrigindo uma série de falhas da v2
  - Evolução normalizada e aberta: TLS (RFC 4346)
  - Inicialmente concebido para ser usado com HTTP
- Características
  - Comunicação segura sobre o nível transporte com ligação
    - Exemplo: TCP
    - Transporte seguro sobre um protocolo de transporte inseguro
      - confidencialidade
      - autenticação
      - integridade
      - e ainda compressão de dados

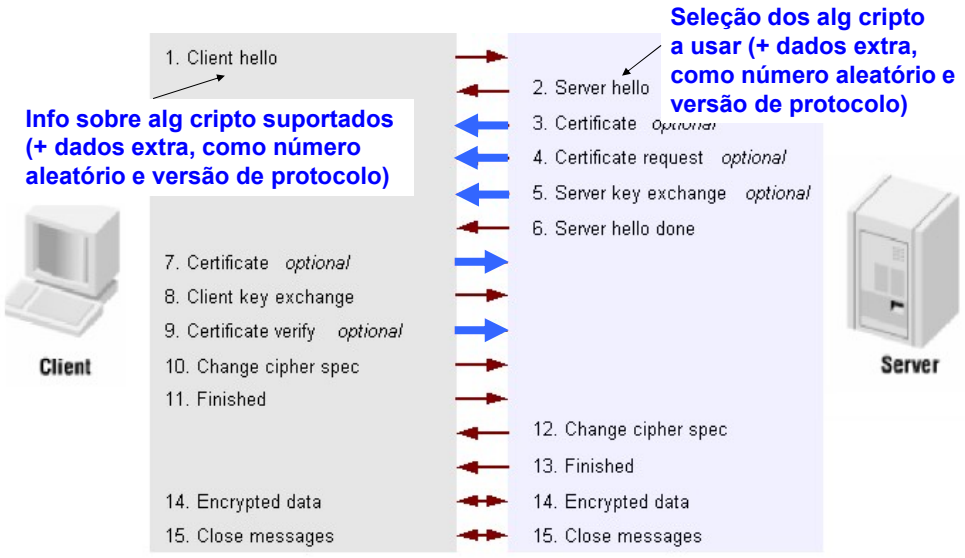
Arquitectura do SSL/TLS



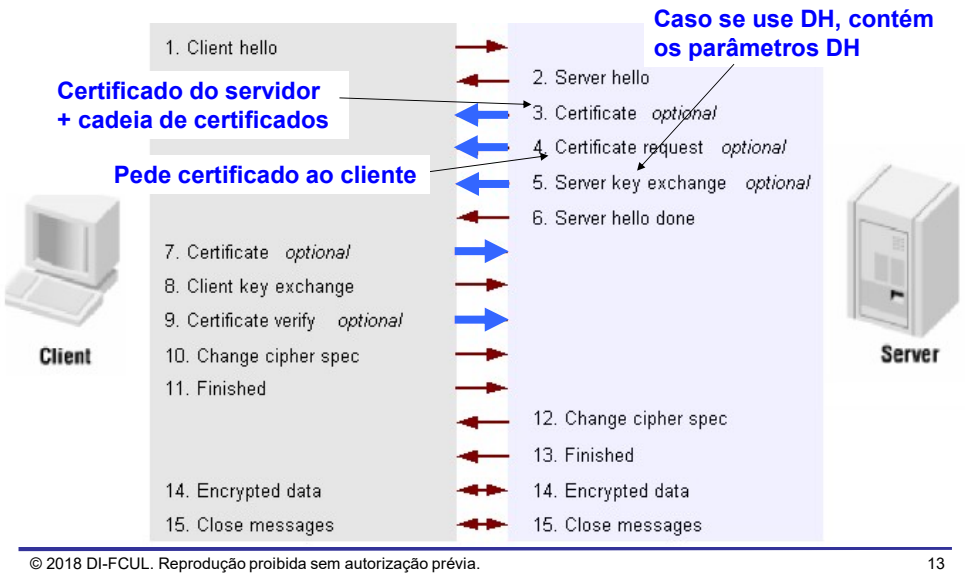
Autenticação: suporte para vários métodos

- Nenhuma (interações anónimas)
  - Chave de sessão gerada através de Diffie-Hellman
- Autenticação do servidor
  - Certificado X.509
  - Chave de sessão
    - Gerada pelo cliente e enviada para o servidor cifrada com a sua chave pública **ou**
    - Diffie-Hellman
- Autenticação mútua
  - Certificado X.509
  - Chave de sessão
    - Gerada pelo cliente e enviada para o servidor cifrada com a sua chave pública **ou**
    - Diffie-Hellman

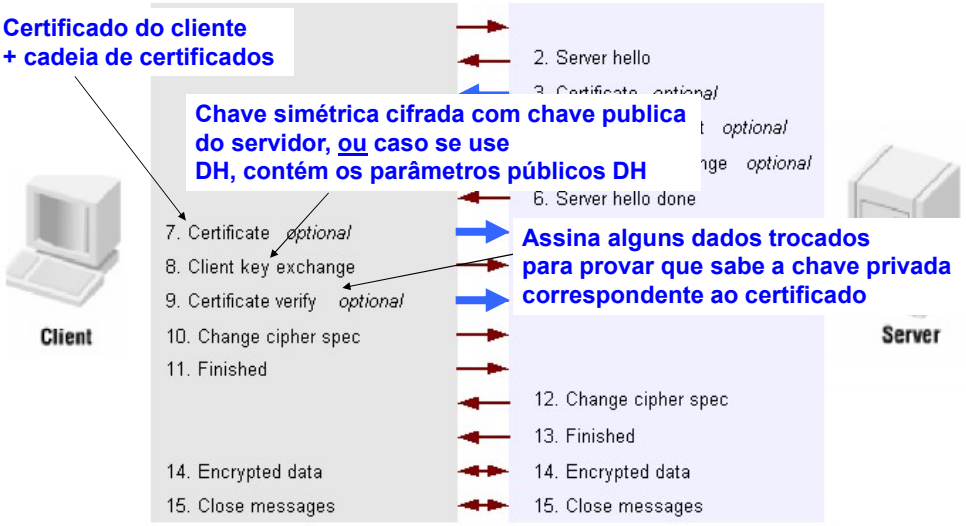
Handshake Protocol



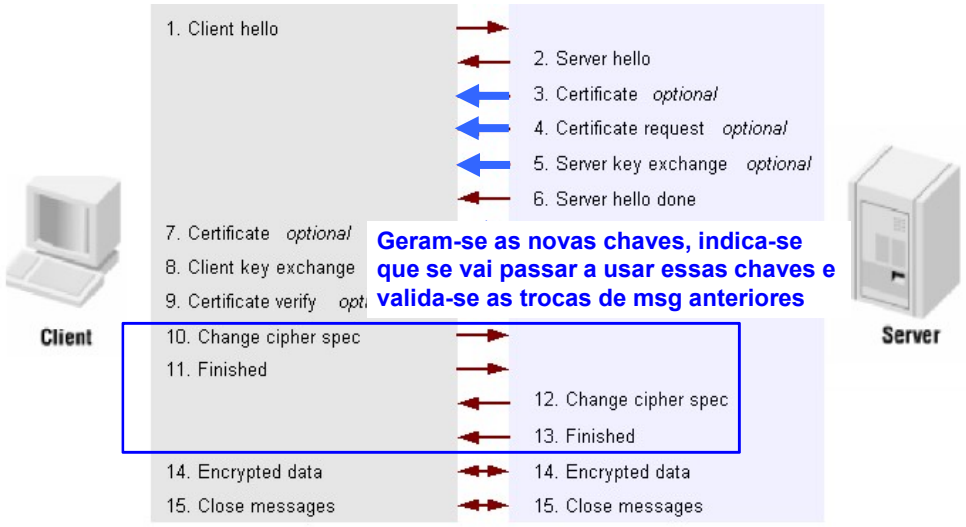
Handshake Protocol



Handshake Protocol



Handshake Protocol



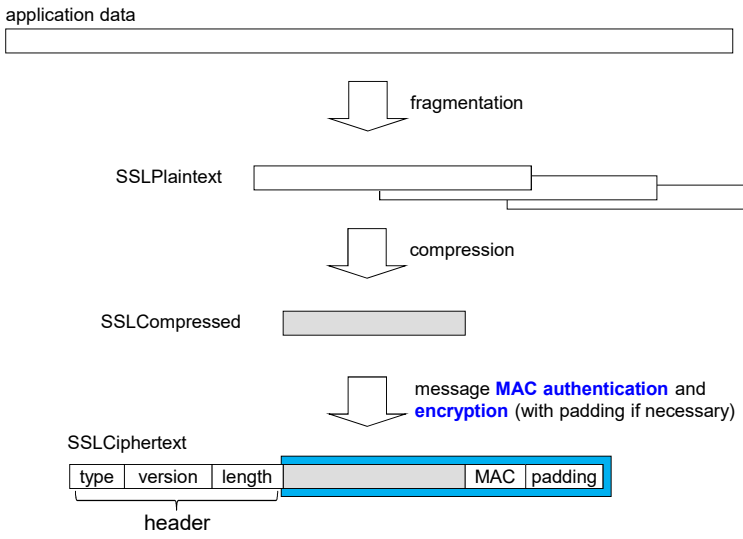
Parâmetros

- Cliente e servidor criam um *pre-master-secret*
- Valores calculados a partir de *pre-master-secret* e de nonces trocados entre cliente e servidor
  - Duas Chaves secretas para MACs
    - Servidor -> cliente
    - Cliente -> Servidor
  - Duas chaves de cifra
    - Servidor -> cliente
    - Cliente -> Servidor
  - Vectores de inicialização se modo de cifra CBC
- Estes valores são calculados com funções de síntese

Protocolo Record

- Responsável pela comunicação segura
- Faz fragmentação, compressão e cifra
- Garante autenticação e integridade das mensagens
- Encapsula protocolos de nível superior como HTTP, Telnet, FTP, etc.
- Corre sobre TCP/IP ou outros protocolos de transporte

Protocolo *Record* – Criação de uma mensagem



Algoritmos

- MACs
  - MD5 ou SHA-1
- Cifra simétrica
  - IDEA, DES, 3DES, AES (128, 256), ...
- Padding
  - ISO10126

Exemplos de utilização do SSL

- O HTTP quando corre sobre SSL é chamado **HTTPS**
  - URLs do tipo `https://.../index.html`
  - O servidor tem o certificado gerado por uma CA fiável contendo a sua chave pública
  - Cliente quer ter certeza que está a aceder ao servidor correto, e portanto o servidor deve provar a sua identidade
  - A autenticação dos clientes é geralmente feita através de *login* e senha na aplicação Web (como nos bancos)
- Outros exemplos
  - SMTPS porto 465
  - LDAPS porto 663
  - IMAPS porto 993