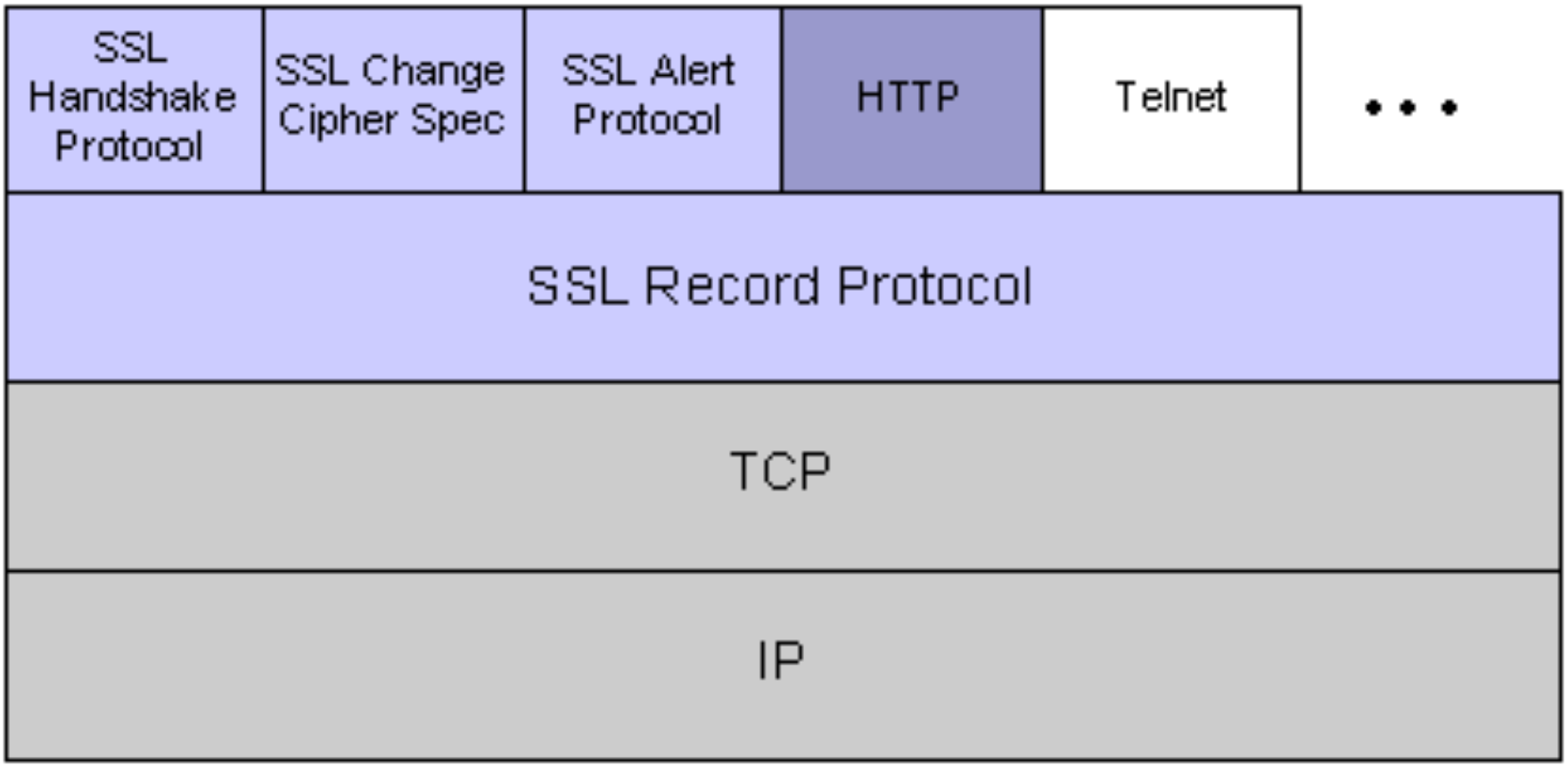
HTTPS
Hypertext Transfer Protocol Secure

Prof. Plinio Marcos Mendes Carneiro

HTTPS – Introdução

- Trata-se do uso do protocolo HTTP "encima" de uma sub-camada SSL, intermediária entre o TCP e o HTTP, que prove autenticação e confidencialidade.
- O SSL – Secure Sockets Layer foi concebido para operar com muitos protocolos, sendo o HTTP somente mais um.
- O HTTPS também pode fazer uso do TLS, padrão que teve origem a partir do SSL da Netscape.
- O HTTPS utiliza a porta TCP 443.

SSL


SSL Handshake Protocol
SSL Change Cipher Spec
SSL Alert Protocol
HTTP
Telnet
• • •
SSL Record Protocol
TCP
IP

SSL

- Os dados que vem e voltam entre o cliente e o servidor são criptografados utilizando um algoritmo simétrico, como DES ou RC4.
- Um algoritmo de chave pública (normalmente RSA) é utilizado para trocar as chaves simétricas (de forma segura) e para as assinaturas digitais.
- Com o certificado digital do servidor, o cliente pode verificar a identidade do servidor e obter sua chave pública para uso no algoritmo.

SSL

- As versões 1 e 2 do protocolo SSL fornecem somente autenticação de servidor.
- A versão 3 inclui autenticação de cliente, utilizando os certificados digitais do servidor e do cliente.
- TLS v1 = SSL v3.
- Veremos uma série de conceitos essenciais para entender como o SSL funciona.

Algoritmos de chave simétrica

- Os algoritmos de chave simétrica (criptografia de chave única, ou criptografia de chave secreta) são uma classe de algoritmos que usam chaves criptográficas relacionadas (mesma ou derivadas) para a operações de cifragem ou decifragem.
- As chaves, na prática, representam um segredo, partilhado entre duas ou mais partes, que podem ser usadas para manter um canal confidencial de informação.
- Obtêm-se a confidencialidade

Criptografia de chave pública

- A criptografia de chave pública ou criptografia assimétrica é um método de criptografia que utiliza um par de chaves: uma chave pública e uma chave privada.
- A chave pública é distribuída livremente para todos os correspondentes, enquanto a chave privada deve ser conhecida apenas pelo seu dono.
- Num algoritmo de criptografia assimétrica, uma mensagem cifrada com uma chaves pode somente ser decifrada somente pela outra chave, par dessa.
- Os algoritmos de chave pública podem ser utilizados para autenticidade e confidencialidade.

Criptografia de chave pública

- Para **confidencialidade**, a chave pública é usada para cifrar mensagens, com isso apenas o dono da chave privada pode decifrá-la.
- Para **autenticidade**, a chave privada é usada para cifrar mensagens, com isso garante-se que apenas o dono da chave privada poderia ter cifrado a mensagem que foi decifrada com a 'chave pública'.

Troca de chaves

- A troca de **chaves simétricas** entre usuários para comunicação segura tornou-se impraticável, a criptografia de chaves públicas provê um meio de solucionar este problema.
- Uma **chave simétrica** pode ser enviada a um destinatário fazendo uso da **chave privada** deste.
- Cria-se assim um canal seguro.

Hash

- É um resumo da mensagem através de algoritmos complexos (Exemplos: MD5, SHA-1, SHA-256) que reduzem qualquer mensagem sempre a um resumo de mesmo tamanho.
- Uma função de *hash* deve apresentar necessariamente as seguintes características:
  - Deve ser impossível encontrar a mensagem original a partir do *hash* da mensagem.
  - O *hash* deve parecer aleatório, mesmo que o algoritmo seja conhecido. Uma função de *hash* é dita forte se a mudança de um bit na mensagem original resulta em um novo *hash* totalmente diferente.
  - Deve ser impossível encontrar duas mensagens diferentes que levam a um mesmo *hash.*

Assinatura Digital

- De maneira resumida uma assinatura digital típica envolve dois processos criptográficos: o *hash* (resumo) e a encriptação deste *hash*.
- Encripta-se o *hash* de uma mensagem e em seguida o criptografa com uma chave privada, esse *hash* criptografado é enviado ao destinatário juntamente com a mensagem original.
- No destinatário, com a chave pública do emissor é possível abrir o *hash* recebido que pode ser comparado com um *hash* calculado do destinatário.
- Se os *hashes* forem iguais a mensagem foi autenticada com sucesso.

Certificado digital

- Um **certificado digital** é um arquivo de computador que contém um conjunto de informações referentes a entidade para o qual o certificado foi emitido (seja uma empresa, pessoa física ou computador) mais a chave pública deste.
- Esse arquivo ele é Assinado Digitalmente com a chave privada de alguém confiável (Infraestrutura de Chaves Públicas - PKI).
- Não Repudio, ICP-Brasil, Padrão X.509.

SSL Handshake - 2 way