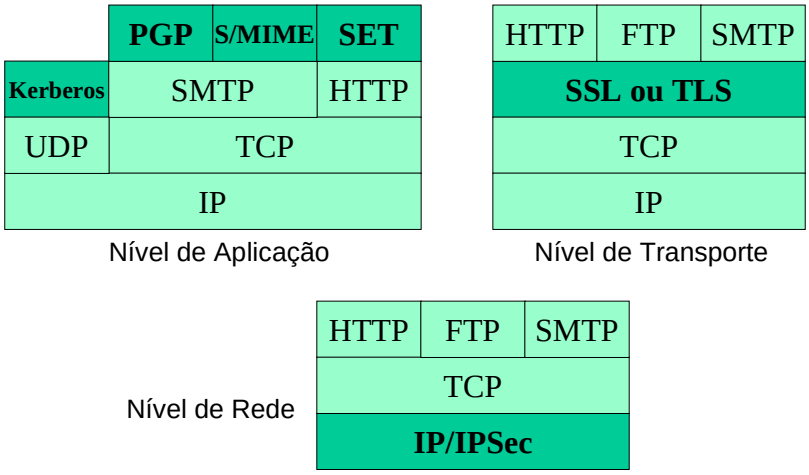
Segurança na Internet

- Muito do sucesso e popularidade da Internet é por ela ser uma rede global aberta
- Por outro lado, isto faz da Internet um meio não muito seguro
- É difícil identificar com segurança entidades, em um meio sem presença física, face ou voz
- Sendo rede global, a Internet não reconhece limites físicos e jurisdições legais das nações
- Certas situações demandam segurança no tráfego pela Internet

Segurança na Internet

- Várias abordagens são possíveis para prover segurança no tráfego de dados da Internet
- As opções atualmente existentes provêm serviços e recursos similares, mas variam em escopo e localização na pilha TCP/IP
- Localização relativa dos mecanismos de segurança na pilha do protocolo TCP/IP:
  - Nível de Aplicação: Kerberos, PGP, S/MIME, SET
  - Nível de Transporte: SSL e TLS
  - Nível de Rede: IPSec

Segurança na Internet



Os Riscos do Cartão de Crédito

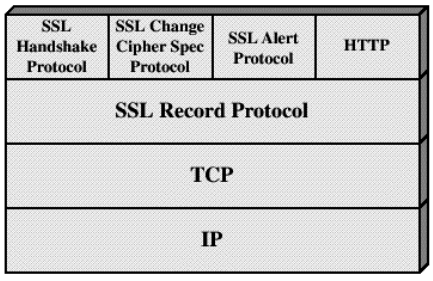
- Um paradoxo de segurança na Web:
  - Hoje pessoas fazem questão de segurança ao informar dados de cartão de crédito pela Web, mas não se preocupam, por exemplo, ao deixar seu cartão c/ um garçom que nunca viram antes
- O risco do número do cartão de crédito ou outra informação sigilosa ser roubada durante a transmissão pela Internet é pequeno
- Há risco maior quando dados sigilosos são armazenados em sistemas, sujeitos a invasão

SSL – Secure Sockets Layer

- SSL - Secure Sockets Layer (Camada de Soquetes Segura)
  - SSL: Protocolo desenvolvido pela Netscape, para prover segurança na transmissão pela Internet
  - Visava principalmente necessidade de segurança no envio de informações via Web (ex: e-comércio)
  - SSL versão 3 (SSLv3) atual foi projetado sob revisão pública da indústria e publicado na Internet como uma proposta de padrão
  - SSL usa TCP para prover serviço fim-a-fim confiável e seguro

Arquitetura do SSL

- O protocolo SSL também pode ser visto em duas camadas
- O Protocolo de Registro SSL provê serviços básicos de segurança para os módulos acima



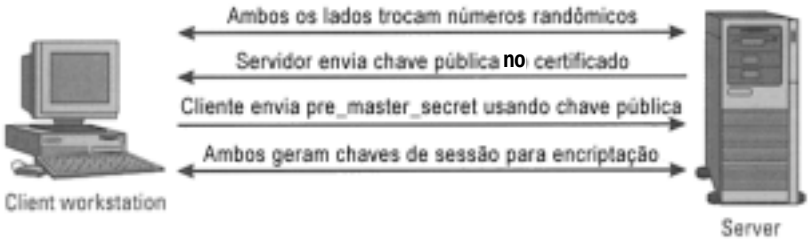
SSL & Segurança na Web

- Conceitos importantes de SSL:
  - Sessão: associação entre servidor e cliente
  - Conexão: transporte de terminado tipo de serviço, sempre associada a uma sessão SSL
- Um servidor e um cliente Web podem realizar várias conexões HTTP em uma sessão SSL
- Web: HTTP sobre SSL – HTTPS
  - Usada pelos browsers e servidores Web
  - Identificado no endereço como https://
  - Simbologia típica no browser: cadeado fechado

Funcionamento do SSL

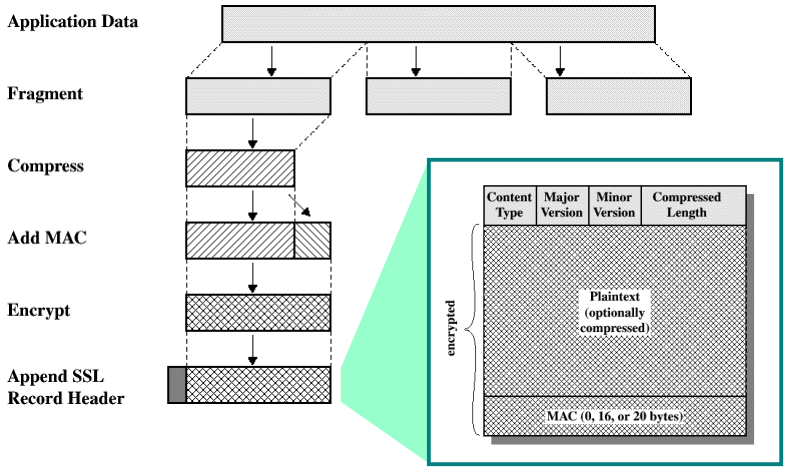
- Tipicamente, o SSL usa criptografia de chave-pública e criptografia simétrica
- Inicialização - Estabelecimento de sessão:
  - Cliente e servidor trocam nºs randômicos
  - Servidor envia chave-pública (certificado X.509)
  - Certificado também valida domínio, nome etc.
  - Cliente gera um valor secreto (pre_master_secret) e envia ao servidor, protegido pela KU do servidor
  - Os dois lados usam os nºs aleatórios e o valor secreto para definir valor secreto e chave de sessão que serão usados na criptografia

Funcionamento do SSL

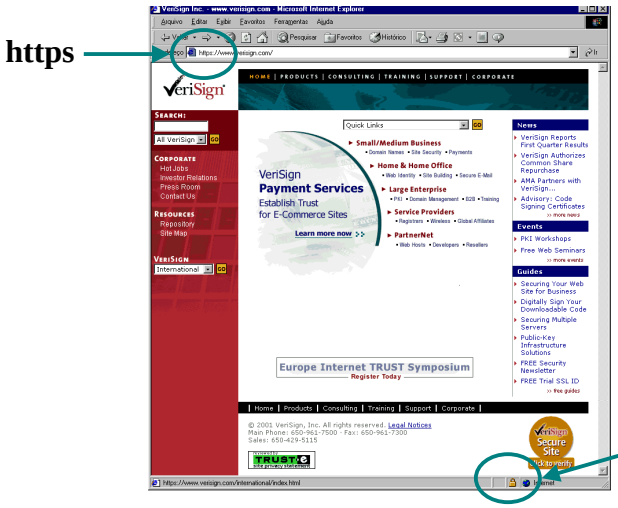


- Operações na conexão SSL
  - Integridade: o valor secreto é usado em MAC
  - Confidencialidade: a chave de sessão é usada para criptografar o pacote SSL
- Criptografia simétrica é usada por ser mais rápida

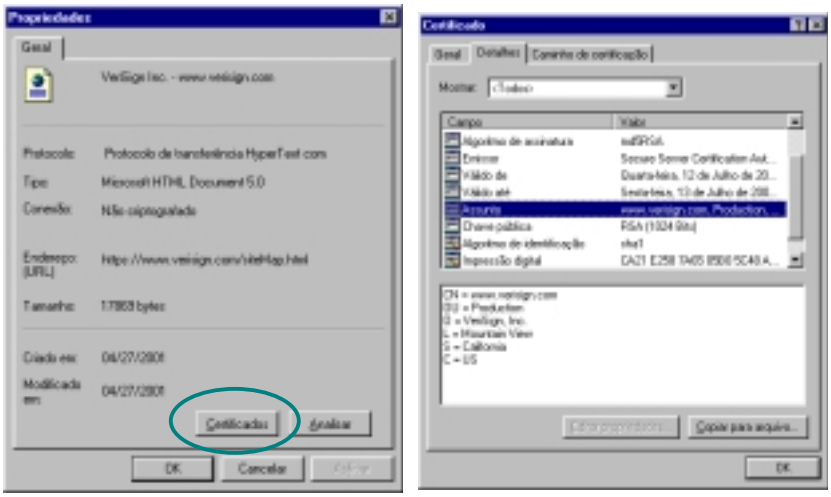
Operações de Registro SSL



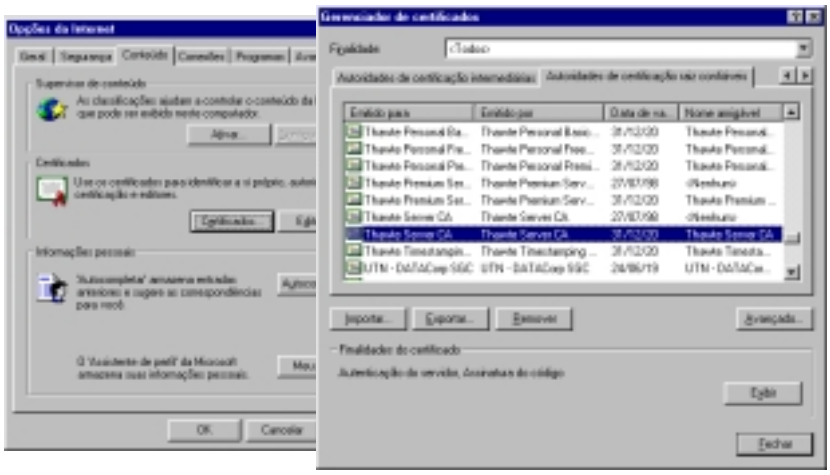
Internet Explorer: HTTPS



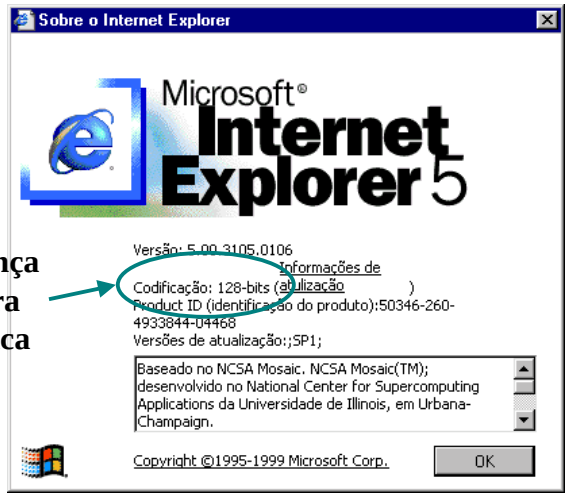
Internet Explorer: Certificado



Internet Explorer: CAs



Internet Explorer: Criptografia



Segurança da cifra simétrica