Instituto de Informática - UFRGS

Redes de Computadores

Aspectos de segurança em TCP/IP

Secure Socket Layer (SSL)

Aula 28

Introdução

Instituto de Informática - UFRGS
A. Carissimi -25-nov.-13

"Na Internet, ninguém sabe que você é um cachorro."

Peter Steiner, *The New Yorker*, julho 1993

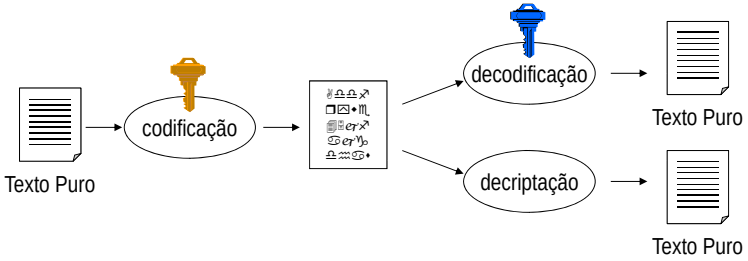
Introdução

- Em segurança da informação é importante garantir três aspectos:
  - Confidencialidade
  - Integridade
  - Disponibilidade
- Porém há outras duas correlacionadas: autenticidade e não repúdio
- Uso de criptografia auxilia na obtenção dessas propriedades
  - Criptografia simétrica
  - Criptografia assimétrica

Instituto de Informática - UFRGS
A. Carissimi -25-nov.-13

Criptografia

- Arte de codificar e decodificar mensagens de forma que a decriptação seja impossível



Instituto de Informática - UFRGS
A. Carissimi -25-nov.-13

Princípio Básico de Funcionamento

- Codificação (cifrar):
  - Determinar uma função *f* que a partir de um texto puro (P) se obtém um texto cifrado (C) com ajuda de uma chave K_c

$$f(K_c, P): P \mapsto C$$

- Decodificação (decifrar):
  - Permitir a operação inversa a partir de uma chave K_d

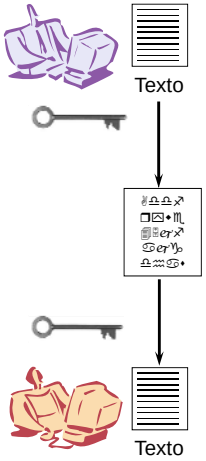
$$f'(K_d, C) = P \quad \text{ou} \quad f'(K_d, f(K_c, P)) = P$$

$$K_c = K_d \rightarrow \text{simétrica}$$

$$K_c \neq K_d \rightarrow \text{assimétrica}$$

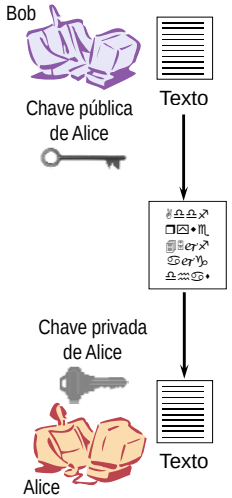
Chaves Simétricas

- Uma única chave empregada pelo remetente e pelo destinatário
  - Utilizada para codificar e decodificar os dados
- Caracaterísticas
  - Cifragem e decifração são computacionalmente rápidas
  - Usuários são responsáveis pela "proteção" da chave
    - Problema de gerenciamento e distribuição das chaves
- Algoritmo popular:
  - AES (Advanced Encryption Standard)
  - Empregado desde 2001
  - Chaves de 128, 192 e 256 bits



Chaves Assimétricas

- Duas chaves distintas:
  - Pública e Privada
  - O que é cifrado com a chave pública só pode ser decifrado com a chave privativa (e vice-versa)
- Características
  - Cifragem e decifração exigem poder computacional maior que com chaves simétricas
  - Facilita gerenciamento e distribuição das chaves, já que a chave pública é conhecida de todos e a privada é mantida secreta por seu proprietário
- Algoritmo popular:
  - RSA (Rivest-Shamir-Adleman)
  - Chaves de no mínimo 2048 bits



Gerenciamento de Chaves

- Chaves simétricas
  - O segredo é compartilhado entre duas pessoas
  - Número de chaves necessárias é dado por *n*(n-1)/2*
  - Armazenamento local (arquivos, pendrive, post-it, agenda,...)
    - Problema é vulnerabilidade
- Chaves assimétricas
  - O segredo (chave privativa) é pessoal, não é compartilhado
    - Armazenamento disco local (arquivos) ou dispositivo (smartcard, ...)
  - A chave pública é... pública ☺: armazenada em qualquer lugar público!
  - O número de chaves necessárias é 2**n* (por usuário, 1 pública e 1 privada)

Questão adicional: Como distribuir ou divulgar as chaves?

Distribuição de Chaves

- Chave simétrica
  - Com servidor: centro distribuição de chaves (*Key Distribution Center-KDC*)
    - Uma chave entre usuário e o KDC
    - KDC gera uma chave temporária (chave de sessão) para usuários
  - Sem servidor: acordo de chave simétrica (protocolo *Diffie-Hellman*)
    - Geração de uma chave de sessão diretamente entre os usuários
- Chave pública (chaves assimétrica)
  - Anúncio público (página *web*)
    - Problema: sujeito a falsificação (quem garante que é a chave pública é de fato de quem diz ser?)
  - Via certificados digitais emitidos por autoridade certificadora

Autoridade Certificadora (AC)

- Entidade pública ou privada responsável por emitir, distribuir, renovar, revogar e gerenciar certificados digitais
  - Cria e assina digitalmente os certificados que emite
  - Emite lista de certificados revogados (LCR)
  - Garante que o titular do certificado possui a chave privada que corresponde a chave pública fornecida
  - Mantém o registro de suas operações
- AC Raiz
  - Primeira autoridade da cadeia de certificação
  - emite, expede, distribui, revoga e gerencia os certificados das autoridades certificadoras de nível imediatamente subsequente ao seu
    - Cadeia de autoridades certificadoras

Autoridade de Registro (AR)

- É a interface entre o usuário e a autoridade certificadora
  - Responsável pelo processo final na cadeia de certificação digital, realizando a identificação presencial dos interessados em adquirir certificados
  - recebimento, validação, encaminhamento de solicitações de emissão ou revogação de certificados digitais
- Vinculada a uma autoridade certificadora

Public Key Infraestructure (PKI)

- Infraestrutura para a criação, armazenamento e distribuição de certificados digitais
- Composta por:
  - Autoridade certificadora (AC)
  - Autoridade de registro (AR)
  - Repositório seguro onde são armazenadas as chaves
  - Um sistema de gerenciamento de certificados
  - Uma política de certificação (Declaração de Praticas de Certificação)
- Infraestrutura de chave públicas do Brasil (IC-Brasil)
  - http://www.iti.gov.br/icp-brasil
  - AC-Raiz vínculada a Casa Civil da Presidência da República

Certificado Digital

- Identidade virtual que permite a identificação segura e inequívoca de autores de mensagens ou transações na Internet
- Documento eletrônico contendo:
  - Chave pública do proprietário
  - Nome, endereço de e-mail
  - Validade e número de série
  - Nome da autoridade certificadora emissora
  - Assinatura digital da autoridade certificadora
- Formato segue X.509 (ITU-T)
- Certificados digitais autoassinados
  - Aqueles assinados por uma autoridade certificadora não reconhecida podendo ser o próprio "gerador" do certificado

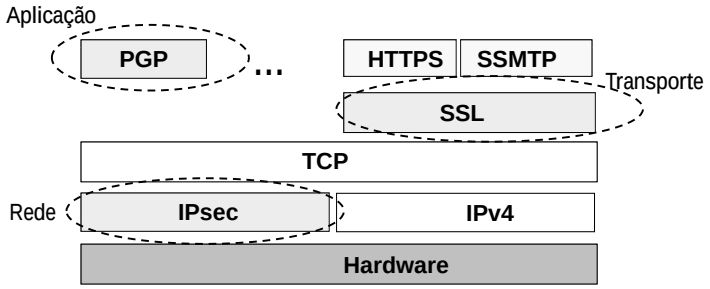
PKI: Algumas Empresas

Empresa	Site
Baltimore	www.baltimore.com
CertCo	www.certco.com
Certisign	www.certisign.com.br
CyberSafe Corp.	www.cybersafe.com
Digital Signature Trust Co.	www.didsigtrust.com
Entrust Technologies Inc.	www.entrust.com
GTE CyberTrust	www.cybertrust.com
IBM Corp.	www.ibm.com
Microsoft Corp.	www.microsoft.com
Network Associates Inc.	www.nai.com
Rainbow Technologies Inc.	www.rainbow.com
Security Dynamics Technologies Inc.	www.securitydynamics.com
VeriSign Inc.	www.verisign.com
Xcert Int'l. Inc.	www.xcert.com

Segurança e Protocolos TCP/IP

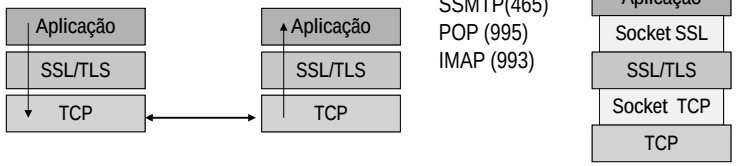
- Constatação: os protocolos Internet (TCP/IP) não seguros!
  - Necessidade de inserir garantias para segurança da informação
  - Duas "correntes" ideológicas: *fim a fim* versus infraestrutura de rede
- Corrente "fim a fim":
  - Camada de aplicação: processo origem cifra e/ou protege integridade dos dados e os envia para o destino que executa a decifração e/ou verificação
    - Desvantagem: aplicação necessita "estar ciente"
  - Camada de transporte (ou imediatamente acima – nova, sessão e/ou apresentação): tornar a segurança transparente para a aplicação (ex. SSL)
- Corrente "infra-estrutura de rede":
  - Camada de rede: autentica e/ou cifra os datagramas sem envolver as aplicações (ex. IPsec)

Protocolos Orientados a Segurança



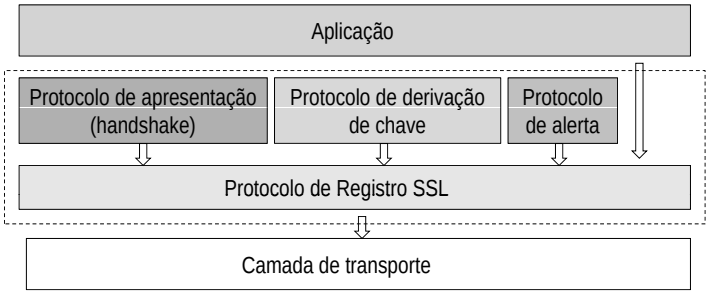
Secure Socket Layer (SSL)

- Desenvolvido originalmente pela Netscape.
- Versão 3.0 foi publicada como *draft* da Internet
  - Base para a definição do Transport Layer Security (TLS)
  - TLS é compatível com SSL versão 3.0
- Projetado para fornecer cifragem de dados entre um cliente e um servidor web
  - Não é limitado a web



HTTPS (443)
SSMTP(465)
POP (995)
IMAP (993)

Arquitetura do SSL



- Organizado em duas camadas de protocolos:
  - Protocolos específicos empregado no gerenciamento do SSL
    - Usado no estabelecimento
  - *SSL Record Protocol*
    - Empregado na utilização de uma conexão segura

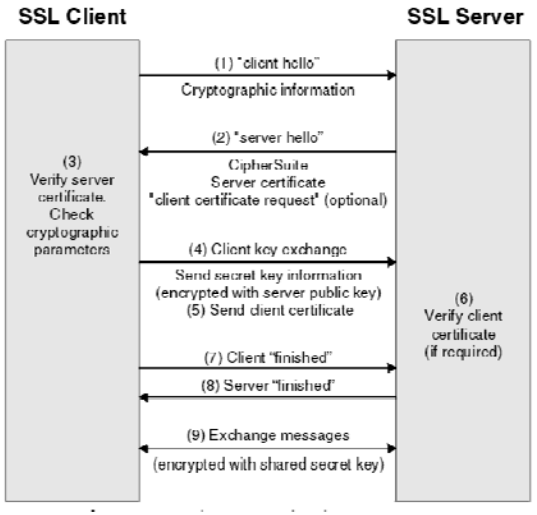
Protocolo de Apresentação (*handshake*)

- Empregado antes de qualquer dado ser transmitido
  - Objetivo: negociar os algoritmos criptográficos e de compactação a serem usados, autenticar o servidor e o cliente
- Composto de quatro fases
  - Fase I: estabelecimento das capacidades de segurança
    - Versão SSL, algoritmos de criptografia e compreensão, números aleatórios para geração de uma chave mestre (simétrica)
  - Fase II: autenticação do servidor e troca de chaves
    - Cliente recebe certificado digital do servidor (chave pública)
  - Fase III (opcional): autenticação do cliente e troca de chaves
    - Servidor recebe certificado digital do cliente (chave pública)
  - Fase IV: Finalização e encerramento

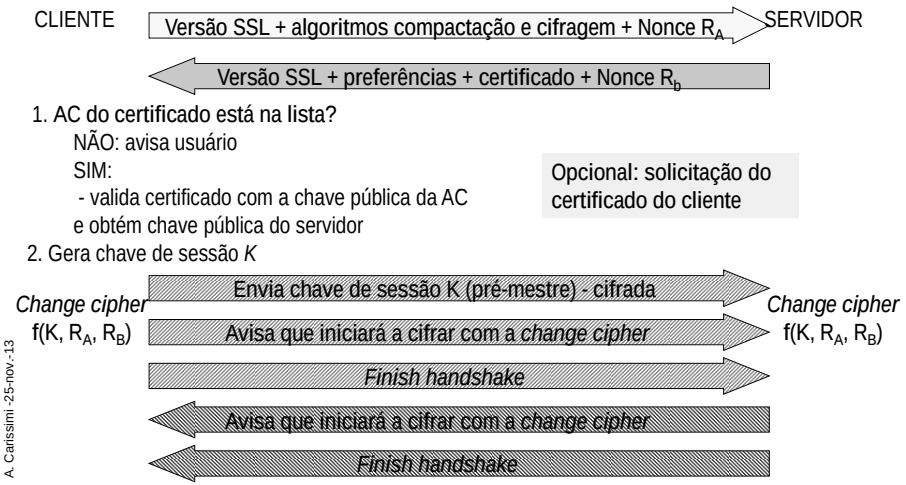
Protocolo de Derivação de Chaves (*change cipher*)

- Objetivo:
  - Gerar chaves para serem usadas na cifragem de dados e verificação de integridade durante a troca de dados
- Existem quatro chaves de sessão geradas por uma combinação de uma chave pré-mestre e os números aleatórios
  - Cifragem de dados enviados do cliente ao servidor
  - Cifragem de dados enviados do servidor ao cliente
  - Verificação de integridade de dados do cliente ao servidor
  - Verificação de integridade de dados do servidor ao cliente
- Cada lado avisa o outro que passará a usar as chaves de sessão
  - Mensagens “finished”

Funcionamento do SSL (*handshake e cipher change*)



Funcionamento SSL (*handshake* e *change cipher*)

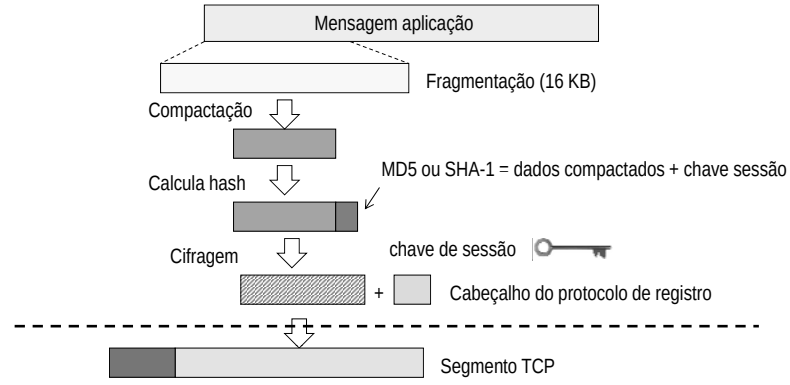


Protocolo de Alerta

- Objetivo:
  - Relatar erros e condições consideradas anormais durante uma sessão SSL
- Mensagem que descreve:
  - O problema
  - Grau de gravidade (*warning* ou *fatal*)

Protocolo de Registro SSL

- Recebe dados da camada superior e os prepara para transmissão
  - O resultado é a geração da área de dados (*payload*) para o TCP



Leituras complementares

- Tanenbaum, A. *Redes de Computadores* (4ª edição), Campus 2003.
  - Capítulo 8
- Carissimi, A.; Rochol, J; Granville, L.Z; *Redes de Computadores*. Série Livros Didáticos. Bookman 2009.
  - Capítulo 8, seções 8.1 (8.1.1 a 8.1.3), 8.3