Material de Apoio

Ameaças e Mecanismos de Proteção

(Aula 02)

Parte 01: Ameaças

Sumário

- **Malware**
  - Definição de Malware
  - Descrição de Códigos Maliciosos
- **Engenharia Social**
- **Referências**

Malware

- **Definição de *Malware***
  - O termo Malware se refere a programas especificamente desenvolvidos para executar ações danosas em um computador (códigos maliciosos). Exemplos:
    - vírus
    - cavalos de tróia
    - *backdoors*
    - *spywares*
    - *keylogger*
    - *worms*
    - *rootkits*
    - *spam*

Malware

- **Descrição de Códigos Maliciosos**
  - Vírus de Computador
    - É um programa ou parte de um programa de computador, normalmente malicioso, que se propaga infectando, isto é, inserindo cópias de si mesmo e se tornando parte de outros programas e arquivos de um computador. O **vírus depende da execução do programa** ou arquivo **hospedeiro** para que possa se **tornar ativo** e dar continuidade ao processo de infecção.

Malware

- **Descrição de Códigos Maliciosos**
  - Cavalos de Tróia
    - É um programa, normalmente recebido como um **"presente"** (por exemplo, cartão virtual, álbum de fotos, protetor de tela, jogo, etc), que além de executar funções para as quais foi aparentemente projetado, também **executa outras funções** normalmente **danosas** e sem o conhecimento do usuário.
    - Algumas das funções maliciosas que podem ser executadas por um cavalo de tróia são:
      - instalação de *keyloggers* ou *screenloggers*;
      - **furto de senhas** e outras informações sensíveis, como **números de cartões de crédito**;
      - inclusão de *backdoors*, para permitir que um atacante tenha total controle sobre o computador;

Malware

- **Descrição de Códigos Maliciosos**
  - Backdoors
    - Normalmente um atacante procura garantir uma forma de retornar a um computador comprometido, sem precisar recorrer aos métodos utilizados na realização da invasão. Na maioria dos casos, também é intenção do atacante poder retornar ao computador comprometido sem ser notado. A esses **programas que permitem o retorno de um invasor a um computador comprometido**, utilizando serviços criados ou modificados para este fim, dá-se o nome de *backdoor*.

Malware

- **Descrição de Códigos Maliciosos**
  - Spyware
    - Refere-se a uma categoria de software que tem o objetivo de **monitorar atividades de um sistema e enviar as informações coletadas** para terceiros. Atividades realizadas por esse tipo de malware:
      - monitoramento de URLs acessadas enquanto o usuário navega na Internet;
      - varredura dos arquivos armazenados no disco rígido do computador;
      - monitoramento e captura de informações inseridas em outros programas, como IRC ou processadores de texto;
      - cavalo de tróia -> spyware -> keyloggers ou screenloggers

Malware

- **Descrição de Códigos Maliciosos**
  - Keylogger
    - É um **programa capaz de capturar e armazenar as teclas digitadas pelo usuário**. Dentre as informações capturadas podem estar o texto de um *e-mail*, dados digitados na declaração de Imposto de Renda e outras informações sensíveis, como senhas bancárias e números de cartões de crédito.

Malware

- **Descrição de Códigos Maliciosos**
  - Worm
    - Código capaz de **propagar-se automaticamente** através de redes, enviando cópias de si mesmo de computador para computador. Diferente do vírus, o *worm* não embute cópias de si mesmo em outros programas ou arquivos e **não necessita ser explicitamente executado** para se propagar. Sua **propagação se dá através da exploração de vulnerabilidades** existentes ou falhas na configuração de *softwares* instalados em computadores.
    - *Worms* são notadamente responsáveis por **consumir muitos recursos**.
    - Detectar a presença de um *worm* em um computador não é uma tarefa fácil. Muitas vezes os *worms* realizam uma série de atividades, incluindo sua propagação, sem que o usuário tenha conhecimento.

Malware

- **Descrição de Códigos Maliciosos**
  - Rootkits
    - Um invasor, ao realizar uma invasão, pode utilizar **mecanismos para esconder e assegurar a sua presença** no computador comprometido. O conjunto de programas que fornece estes mecanismos são conhecidos como *rootkit*.
    - Um *rootkit* pode fornecer programas com as mais diversas funcionalidades. Dentre eles, podem ser citados:
      - programas para esconder atividades e informações deixadas pelo invasor, tais como arquivos, diretórios, processos, conexões de rede;
      - programas para remoção de evidências em arquivos de *logs*;
      - *sniffers*, *backdoors e scanners*,outros tipos de *malware*, como cavalos de tróia, *keyloggers*, ferramentas de ataque de negação de serviço, etc.

Malware

- **Descrição de Códigos Maliciosos**
  - Spam
    - Spam é o termo usado para referir-se aos e-mails não solicitados, que geralmente são enviados para um grande número de pessoas. Quando o conteúdo é exclusivamente comercial, esse tipo de mensagem é chamada de UCE (do inglês *Unsolicited Commercial* E-mail).
    - Spam zombies são computadores de usuários finais que foram comprometidos por códigos maliciosos em geral, como worms, bots, vírus e cavalos de tróia. Estes códigos maliciosos, uma vez instalados, permitem que spammers utilizem a máquina para o envio de spam, sem o conhecimento do usuário. Enquanto utilizam máquinas comprometidas para executar suas atividades, dificultam a identificação da origem do spam e dos autores também.

Engenharia Social

- **Definição**
  - Conjunto de técnicas usadas para **obter informações sigilosas** através da interação (presencial ou virtual) com colaboradores.
  - Esse tipo de ameaça explora diversas **vulnerabilidades**, por exemplo, falta de treinamento e capacitação de colaboradores, ausência de controles (política de segurança e mecanismos de controle de acesso e monitoramento)
    - O ser humano possui traços comportamentais que o torna vulnerável a ataques de engenharia social.
  - A engenharia social permite ao invasor reunir uma série de informações sobre a vítima (rotina, telefone, dados pessoais, dados da empresa, etc.)

Engenharia Social

- **Anatomia**
  - Obter Informações gerais sobre o alvo
  - Desenvolve o relacionamento
  - Explora esse relacionamento
  - Ações para atingir o objetivo

Parte 02: Mecanismos de Proteção

Sumário

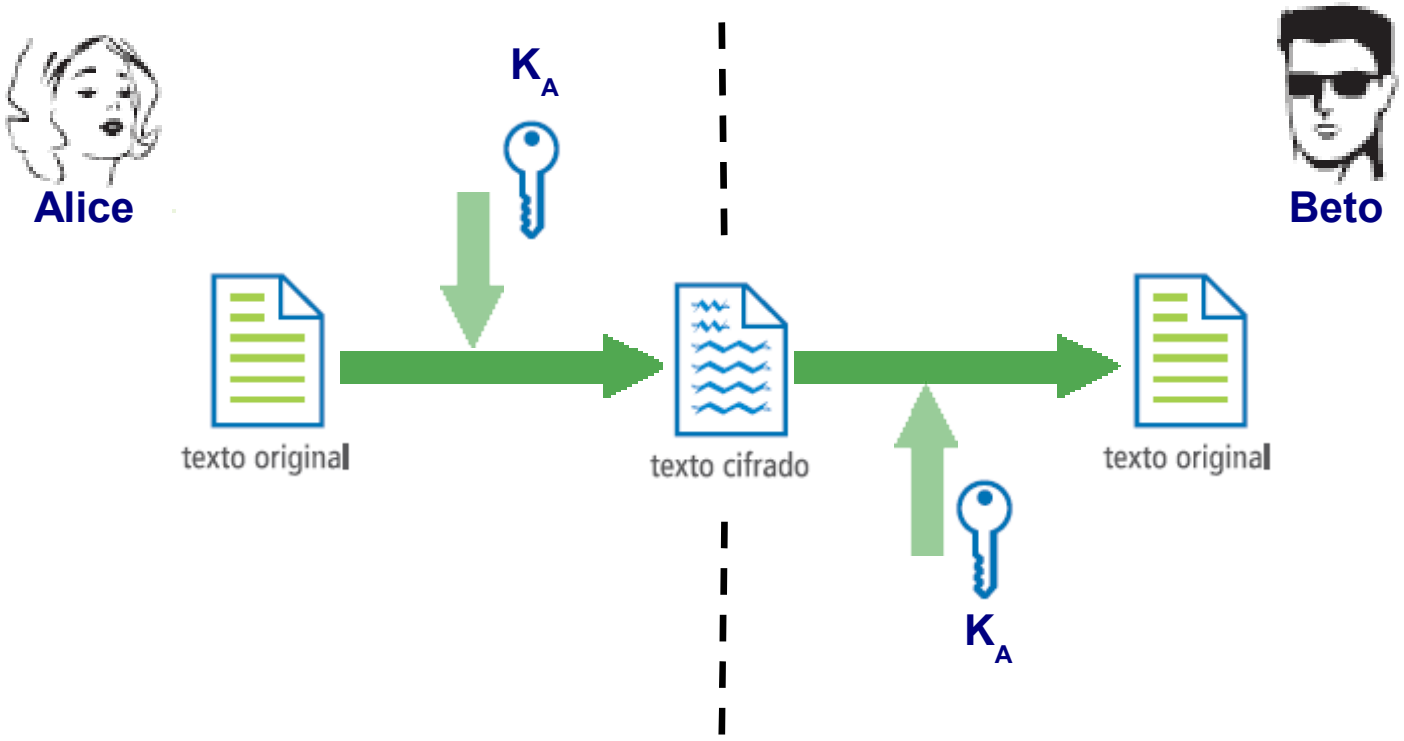
- Conceito de Controle
- Criptografia
- Firewalls
- Detecção e Prevenção de Intrusão
- Redes Virutais Privadas
- Outros Controles
- Considerações Finais
- Referências

Conceito de Controle

- **Controle**
  - Forma de Gerenciar o risco, incluindo políticas procedimentos, diretrizes, práticas ou estruturas organizacionais, que podem ser de natureza administrativa, **técnica**, de gestão ou legal [ISO/IEC 17799:2005].
  - Controle também é utilizado como sinônimo para proteção ou contramedida, medidas de segurança.
  - Os controles podem ser classificados como: preventivas e corretivas.
  - Um Plano de Continuidade de Negócios pode ser considerado tanto um controle preventivo (quando da sua criação) quanto uma ação corretiva (quando da sua aplicação).

Criptografia

- **Criptografia Simétrica (1)**
  - Baseia-se na simetria das chaves, isto é: a mesma chave é utilizada tanto para cifrar quanto para decifrar uma mensagem.



Criptografia

- **Criptografia Simétrica (2)**
  - **Algoritmos Simétricos.**

Algoritmo	Descrição
DES	Data Encryption Standard, possui um alfabeto de 256 simbolos, foi quebrado em 1997.
Triple DES	Evolução do DES, possui "48 rodadas" para cifrar uma informação. Utiliza chaves de 112 bits.
Blowfish	Esse algoritmo pode utilizar chaves de até 448 bits. Não possui patentes de software e é mais rápido que o DES e o IDEA.
IDEA	Baseado no DES, possui uma chave de 128 bits, utilizado pelo PGP.
RC4, 5, 6	"Concorrente" do AES o RC 5, or exemplo, pode trabalhar com chaves de até 2048 bits.
AES	É o algoritmo simétrico indicado pelo NIST como o mais seguro no momento.

Criptografia

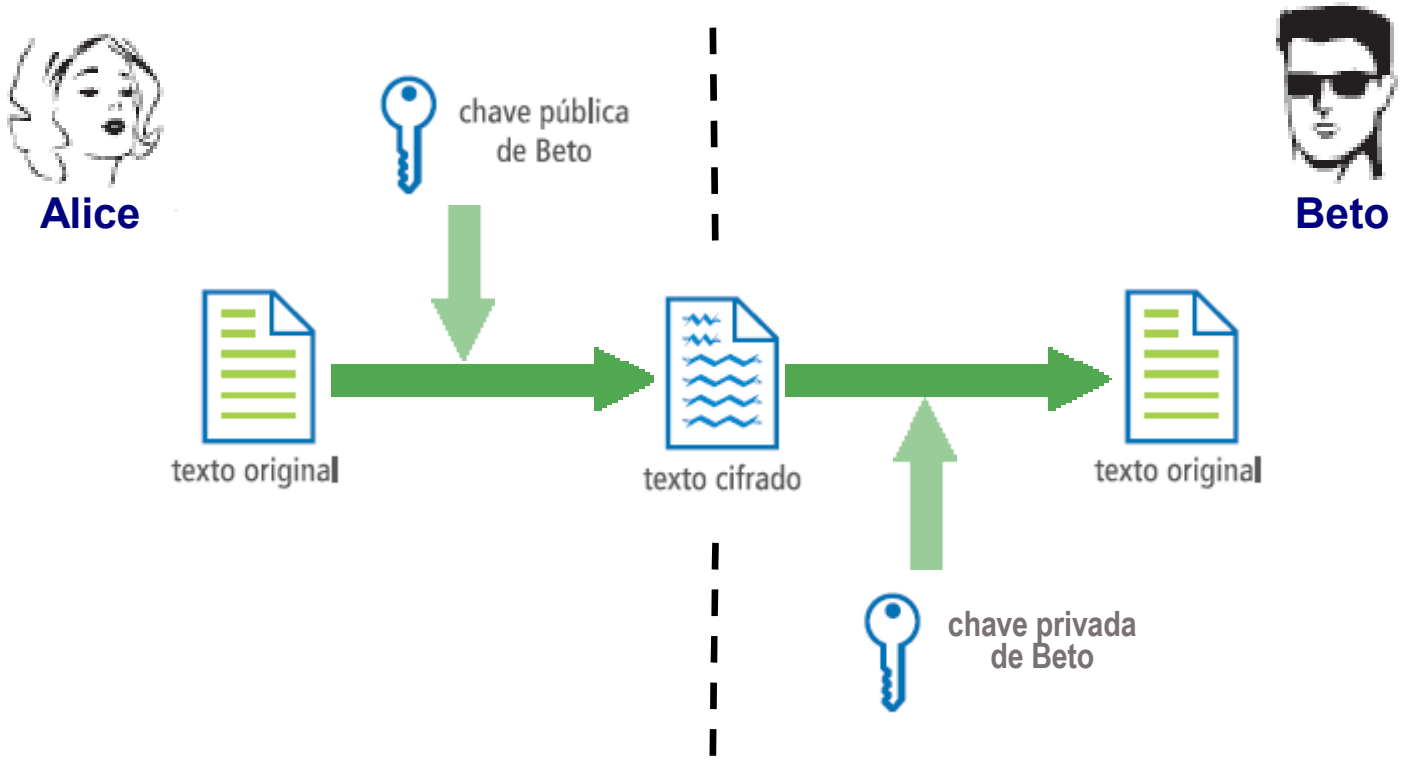
- **Criptografia Simétrica (3)**
  - **Aspectos Positivos**
    - Bom desempenho nos processos de criptografia e descriptografia;
    - Garantia de confidencialidade;
  - **Limitações**
    - Necessita de um canal seguro para a realização da troca de chaves;
    - Não garante autenticidade e não-repúdio;
    - Cada par (receptor - emissor) necessita de um $\frac{(n)(n-1)}{2}$ para se comunicar de forma segura. Sendo assim temos como o número total de chaves necessárias.

Criptografia

- **Criptografia Assimétrica (1)**
  - As chaves são sempre geradas aos pares: uma para cifrar e a sua correspondente para decifrar.
    - As duas chaves são relacionadas através de um processo matemático, usando funções unidirecionais para a codificação da informação.
  - Uma das chaves é mantida em segredo e ganha o nome de chave privada, enquanto a outra é livremente divulgada pela rede e recebe o nome de chave pública
  - A chave pública cifra e a chave privada decifra

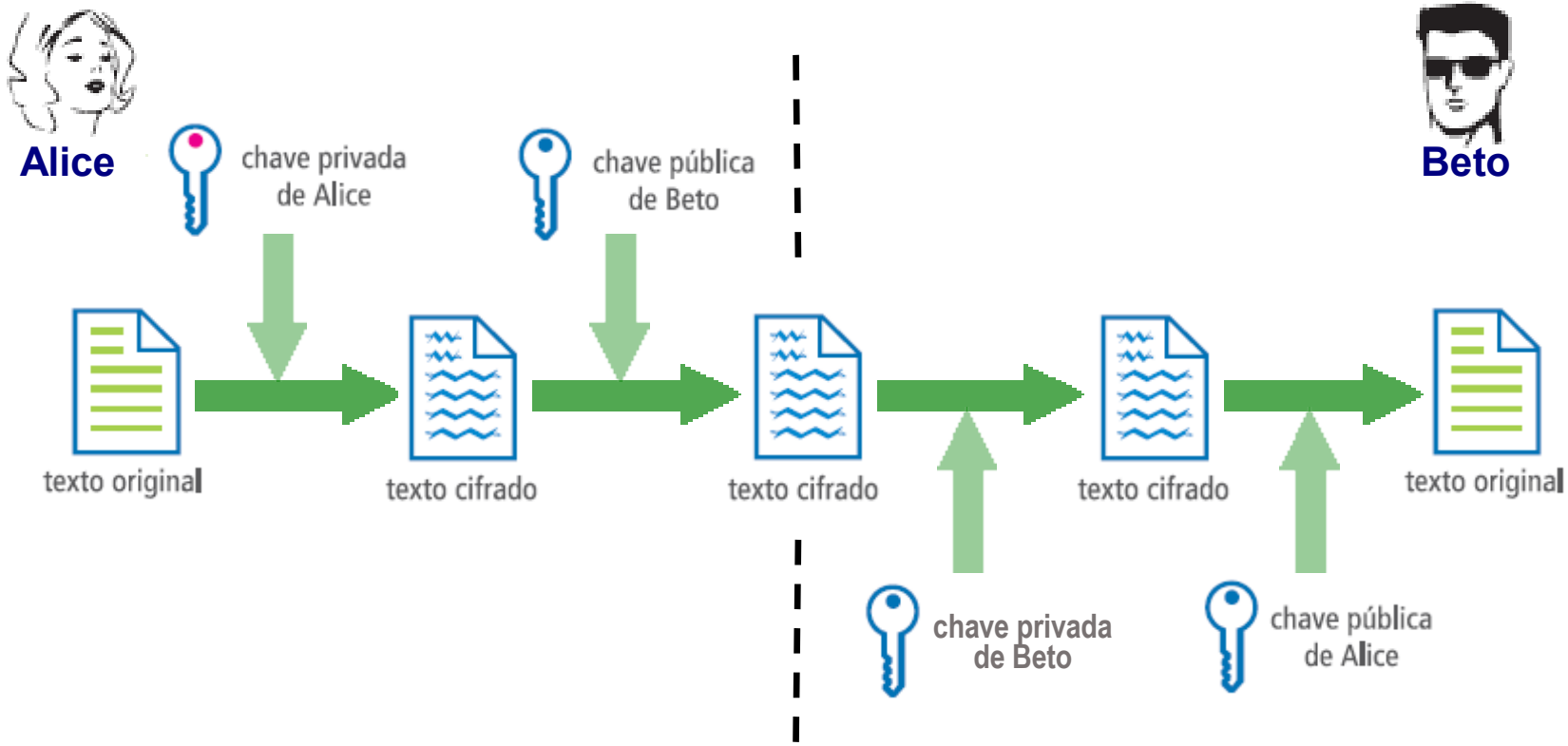
Criptografia

- **Criptografia Assimétrica (2)**



Criptografia

- **Criptografia Assimétrica (3)**



Criptografia

- **Criptografia Assimétrica (4)**
  - **Algoritmos Assimétricos**

Algoritmo	Descrição
RSA	Um dos algoritmos de chave pública mais poderosos atualmente (é fácil multiplicar dois nros primos, o dificial é obter esses dois nros a partir do resultado dessa multiplicação).
Diffie-Hellman	É o criptosistema de chave pública mais antigo ainda em uso.
El Gama	Baseado na dificuldade de fatorar grandes nros (problema do logaritmo discreto).

Criptografia

- **Criptografia Assimétrica (5)**
  - **Aspectos Positivos**
    - Mais segura do que a criptografia simétrica, por não precisar comunicar ao receptor a chave necessária para descriptografar a mensagem.
    - Qualquer usuário pode enviar uma mensagem secreta, utilizando apenas a chave pública de quem irá recebê-la. Como a chave pública está amplamente disponível, não há necessidade do envio de chaves como no modelo simétrico.
    - Garante confidencialidade, autenticidade e não-repúdio
    - O número de chaves por participantes é 2n
  - **Limitações**
    - Baixo desempenho quando comparado com a criptografia simétrica

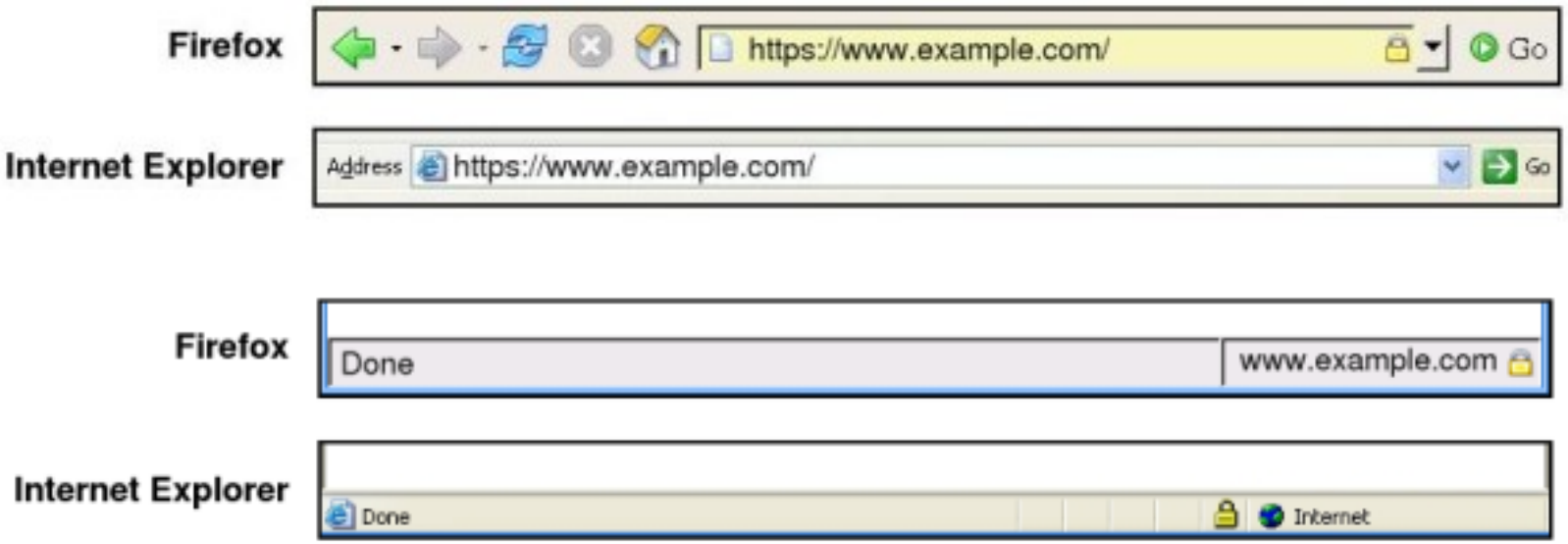
Criptografia

- **Protocolos Seguros (1)**
  - **SSL (*Secure Socket Layer*)**
    - O protocolo SSL, originalmente desenvolvido pela Netscape, atua na camada de transporte e, geralmente, é utilizado para garantir que a comunicação entre um servidor web e um cliente (*browser*) seja segura.

    - Serviços oferecidos pelo SSL
      - Confidencialidade
      - Autenticação
      - Integridade

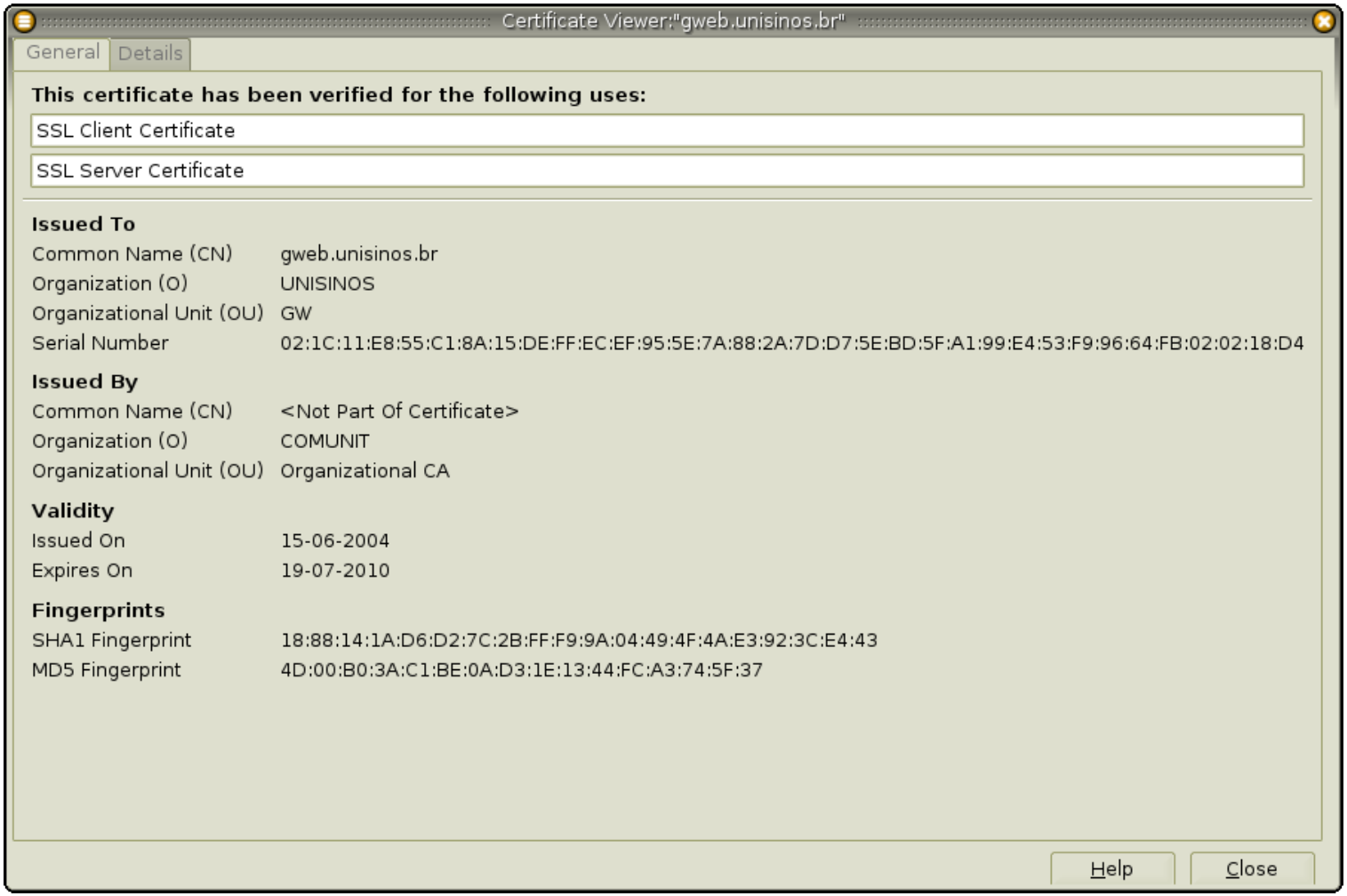
Criptografia

- **Protocolos Seguros (2)**
  - **SSL (*Secure Socket Layer*)**
    - Como idenificar sites Seguros (https)



Criptografia

- **Protocolos Seguros (3)**
  - **SSL (*Secure Socket Layer*)**

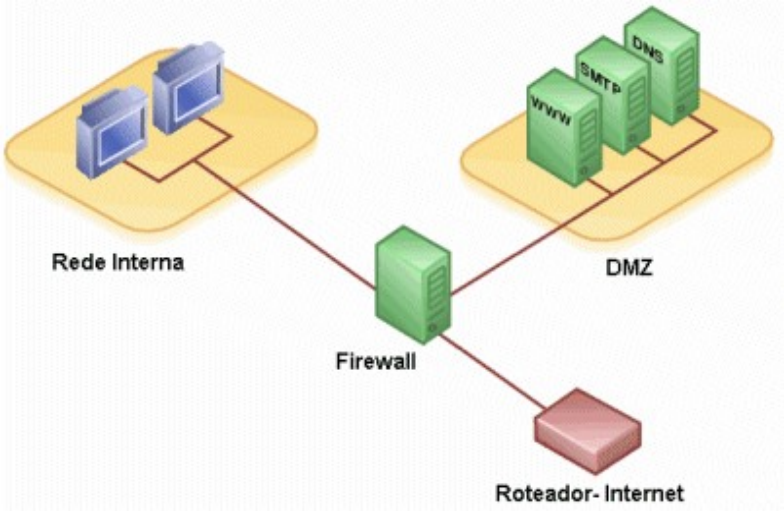


Criptografia

- **Protocolos Seguros (4)**
  - **IPSEC (*Internet Protocol Security*)**
    - Conjunto de protocolos que visa oferecer autenticidade e confidencialidade na camada de rede.
      - Autenticidade -> identificar o endereço IP de origem
      - Confidencialidade -> criptografar o campo de dados do datagrama
    - Através desse protocolo são oferecidos serviços de segurança de forma transparente as demais camadas superiores.
      - Não é necessário implementar segurança, por exemplo, na camada de aplicação
    - Permite criar múltiplos canais seguros entre dois *hosts*
    - Recurso nativo no IPv6.

Firewalls

- **Conceito**
  - Mecanismo que restringe e controla o fluxo do tráfego de dados entre redes, mais comumente entre uma rede interna e a Internet.
    - Todo o tráfego de dentro para fora da rede e vice-versa deve passar pelo firewall;
    - Só o tráfego definido pela política de segurança da rede é permitido passar pelo firewall;
    - O próprio sistema de firewall deve ser resistente a tentativas de ataque.



Firewall
ponto central de controle

Firewalls

- **Tipos de Firewalls**
  - ***Packet Filtering***
    - Nesse tipo de mecanismo, a tomada de decisão referente a aceitação ou rejeitação um pacote é realizada em função da análise do conteúdo de um pacote (nível de rede) e de uma série de regras pré-configuradas no dispositivo.
  - ***Stateful Firewalls***
    - Em um *stateful filter* existe uma tabela de estados que armazena informações sobre as conexões. A partir dessa tabela de estados é possivel identificar "quem", "o que" e "para quem".
    - Na definição das regras de um *firewall stateful* é possivel definir critérios que envolvam informações das seguintes camadas: Aplicação (nem sempre), Transporte e Rede.

Firewalls

- **Limitações**
  - Não pode proteger a empresa contra usuários internos;
  - Não pode proteger a empresa de ataques que utilizem conexões que não passam pelo fw (acesso remoto via *dial-up*);
  - Não é capaz de bloquear novos ataques;
  - Não substituí o sistema de anti-vírus.

Detecção e Prevenção de Intrusão

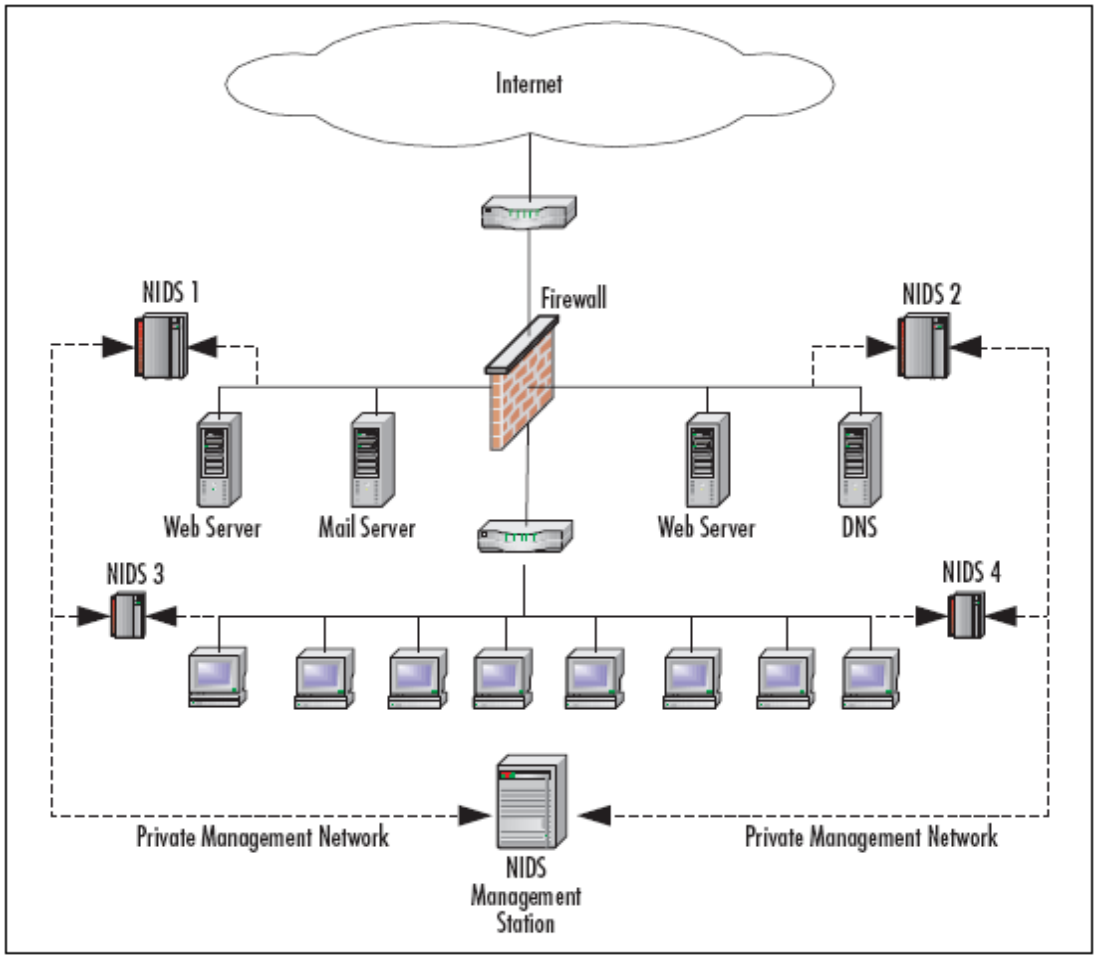
- **Sistemas de Detecção de Intrusão (1)**
  - **Detecção de Intrusão**
    - É o processo de identificação e notificação de atividades maliciosas, atividades não autorizadas e ataques que tenham como alvo, um computador, uma rede ou a infra-estrutura de comunicação.
  - **Sistemas de Detecção de Intrusão ou *Intrusion Detection Systems* (IDSs)**
    - É o conjunto de *hardware* e *software* cujo objetivo é identificar determinados eventos que se deseja evitar. Esses eventos são capturados por sensores distribuídos ao longo do ambiente monitorado.
    - Tão logo um evento seja capturado, o mesmo é submetido ao analizador de evento – um componente capaz de identificar o que de fato é ou não um ataque ou atividade intrusiva.

Detecção e Prevenção de Intrusão

- **Sistemas de Detecção de Intrusão (2)**
  - **Classificação**
    - Parâmetro: Escopo de atuação
      - *Network Intrusion Detection Systems* (NIDS)
      - *Host Intrusion Detection Systems* (HIDS)
    - Parâmetro: Técnicas de Detecção
      - Baseada em Assinaturas
      - Baseada em Anomalia

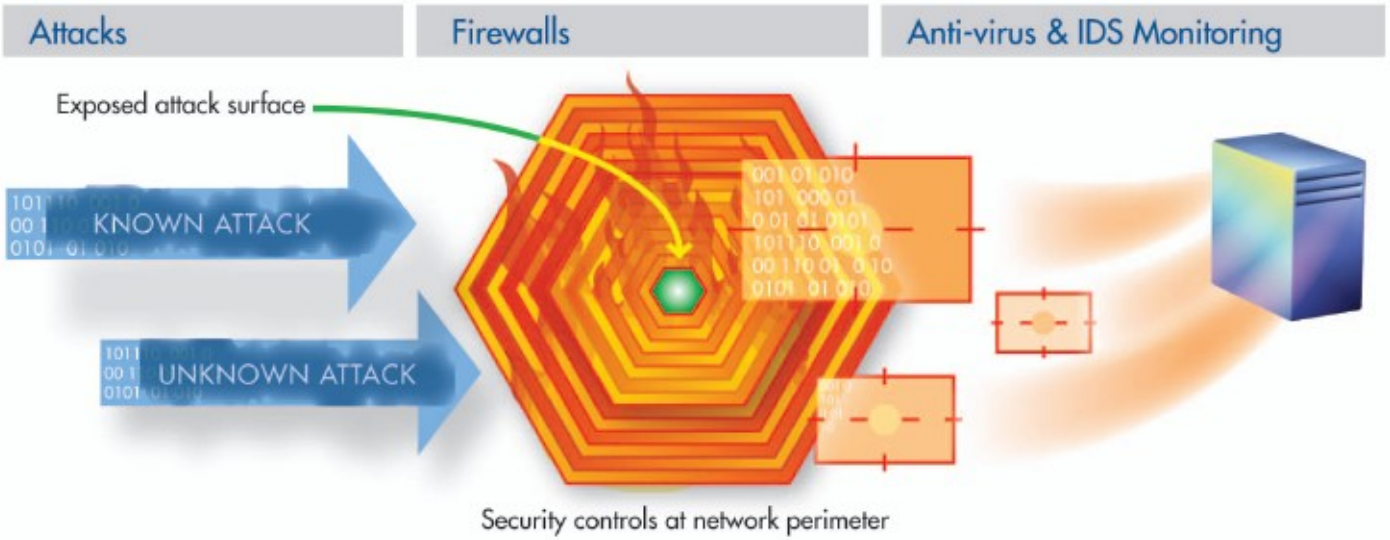
Detecção e Prevenção de Intrusão

- **Sistemas de Detecção de Intrusão (3)**
  - **Cenário Distribuído com Sensores de NIDS e HIDS**



Detecção e Prevenção de Intrusão

- **Sistemas de Prevenção de Intrusão (1)**
  - O conceito prevenção de intrusão além muito intuitivo pode ser facilmente entendido a partir do entendimento do modelo de defesa ilustrado na figura a seguir.



Detecção e Prevenção de Intrusão

- **Sistemas de Prevenção de Intrusão (2)**
  - Sistemas de Prevenção de Intrusão ou *Intrusion Prevention Systems* (IPSs)
    - Ao contrário dos IDSs, que é uma ferramenta passiva, o IPS é uma mecanismo de defesa pró-ativo. Portanto, tem como objetivo detectar e previnir a ocorrência de ataques conhecidos.
      - IPS => Firewall + IDS
  - A definição ideal de IPS contempla ainda:
    - Análise de vulnerabilidades
    - Atualização dos hosts vulneráveis

Redes Virtuais Privadas

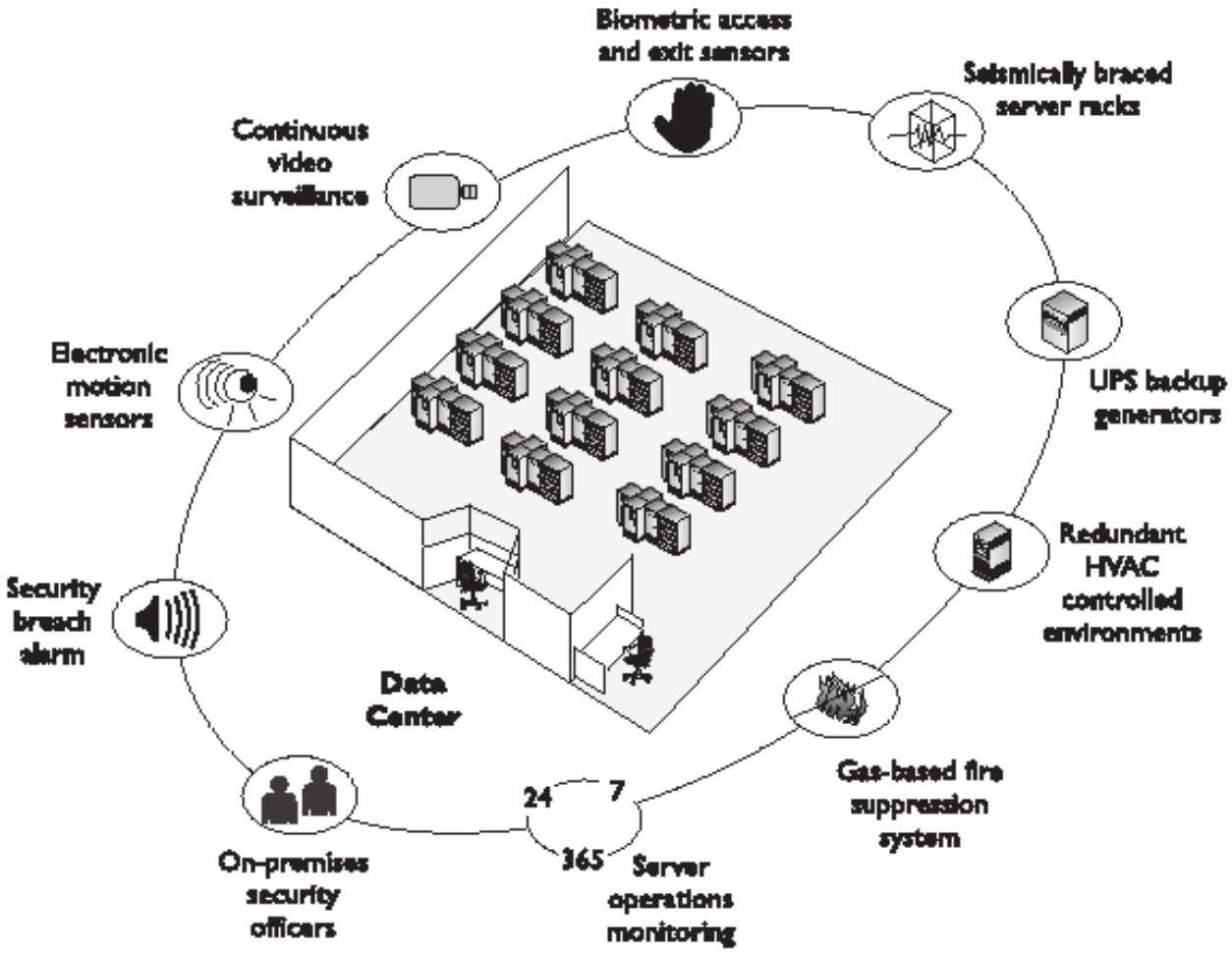
- **O que é uma *Virtual Private Network* (VPN)?**
  - Rede privada implantada sobre a infra-estrutura de uma rede pública;
  - Consiste na criação de "túneis" para a transferência de informações de modo seguro, entre redes corporativas ou usuários remotos.
  - O conceito de VPN surgiu da necessidade de se utilizar redes de comunicação não confiáveis para trafegar informações de forma segura.

Redes Virtuais Privadas

- **Quais as vantagens em utilizar VPNs?**
  - Elimina a necessidade de aluguel de linhas dedicadas
    - Uma empresa, para conectar a matriz e uma filial por meio de uma rede privada tradicional, necessita de uma linha dedicada. Já para conectar a matriz e duas filiais, duas linhas adicionais são necessárias.
  - Diminui a necessidade de ligações de longa distância para o acesso remoto
    - Oferecem uma maior flexibilidade de uso (já que pontos de acesso à Internet estão disponíveis em vários locais onde linhas dedicadas não estão acessíveis)

Outros Controles

- **Segurança Física**



Referências

[1] Microsoft Corporation. **Modelagem de Ameças**. Patterns & practices (2004)

[2] Microsoft Corporation. **Ameaças e Contramedidas**. (2004)

[3] Cert.br. **Cartilha de Segurança na Internet: Parte VIII**.Disponivel em: http://www.cert.br

[4] Antispam.br. Disponivel em: **AntiSpam**. http://www.antispam.br

[5] Os vídeos apresentados nesta aula (slide 4 e 12) foram produzidos por um dos grupos de trabalho do **Comitê Gestor da Internet no Brasil** e estão disponíveis no site: http://www.antispam.br/videos/

[6] **OWASP –** Open Web Application Security Project. http://www.owasp.org

[7] **Social Engineering: Exposing the Danger Within.** http://www.gartner.com/gc/webletter/security/issue1/index.html

Referências

[8] Diffie, W.; Hellman, M. **New directions in cryptography**. In: IEEE Transactions on Information Theory (1976), v. 22, p. 644-654.

[9] **Building Internet Firewalls**.Disponivel em: http://www.unix.org.ua/orelly/networking/firewall/

[10] **Snort 2.0 Intrusion Detection (**Autores: Jay Beale e James C. Foster**)**

[11] **All-in-One is All You Need (**Autora: Shon Harris**)**

[12] **Autenticação Biométrica**. Disponível em: http://mega.ist.utl.pt/~ic-aas/2002/Slides/biometria.pdf (Leitura Fortemente Recomendada)