Mecanismos para Controles de Segurança

Marcos Aurelio Pchek Laureano
laureano@ppgia.pucpr.br

Roteiro

- Autenticação e Autorização
- Combate a ataques e invasões
- Privacidade nas comunicações
- Processos de Segurança

Autorização

- Processo de conceder ou negar direitos a usuários ou sistemas
- Listas de controle de acessos (*Acess Control Lists* – ACL)
- Gera os perfis de acesso

Sistemas de Recursos Humanos

	Diretor	**Gerente**	**Secretária**
Dados Pessoais	Ler, Gravar, Excluir	Ler, Gravar, Excluir	Ler, Gravar
Dados Bancários	Ler, Gravar, Excluir	Ler, Gravar	Ler
Salário	Ler, Gravar	Ler	Nada

Autenticação

- Meio para obter a certeza de que o usuário ou o objeto é realmente quem está afirmando ser
- Permite trilhas de auditoria
- Assegura
  - controle de acesso
  - legitimidade do acesso

Autenticação

- Baseado em três métodos distintos
  - Identificação positiva (O que você sabe)
  - Identificação proprietária (O que você tem)
  - Identificação Biométrica (O que você é)

Combate a ataques e invasões

- Destinados a suprir a infra-estrutura para
  - proteção
  - controle de acesso
  - combate a ataques e invasões
- Basicamente
  - Firewall
  - Detector de Intrusos

Firewall

- Reforça a norma de segurança entre uma rede interna segura e uma rede não-confiável
- meio de dividir o mundo em duas ou mais redes
  - uma ou mais redes seguras
  - uma ou mais redes não-seguras

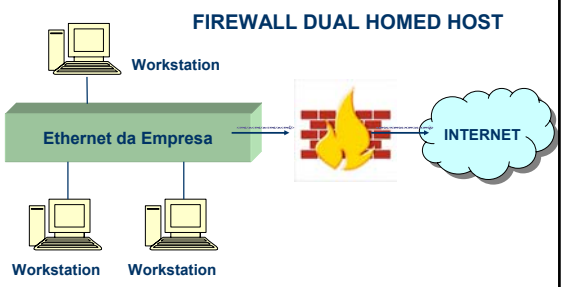
Firewall

- Um firewall pode ser
  - PC
  - roteador
  - computador de tamanho intermediário
  - mainframe
  - estação de trabalho UNIX
  - a combinação de todos os anteriores

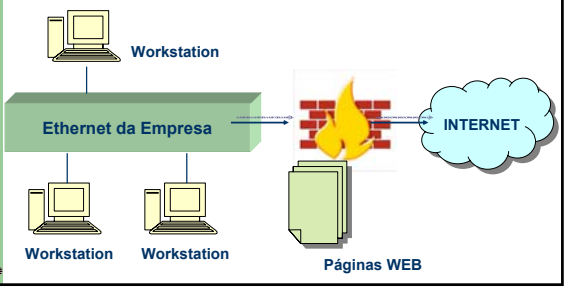
Firewall

- Divididos em 2 grandes classes
  - Filtros de pacotes
    - firewall dual homed host
  - Servidores proxy
    - acesso a internet

Filtro de Pacotes



Servidor Proxy



Detector de Intrusos

- *Intrusion Detection System* - IDS
- Automatiza a tarefa de analisar dados da auditoria
- Utiliza várias técnicas
  - análise estatística
  - inferência
  - inteligência artificial
  - *data mining*
  - redes neurais

Classificação de IDS

- Quanto à Origem dos Dados
  - Host Based IDS (HIDS)
  - Network Based IDS (NIDS)
- Quanto à Forma de Detecção
  - Detecção por assinatura
  - Detecção por anomalia
  - Detecção Híbrida

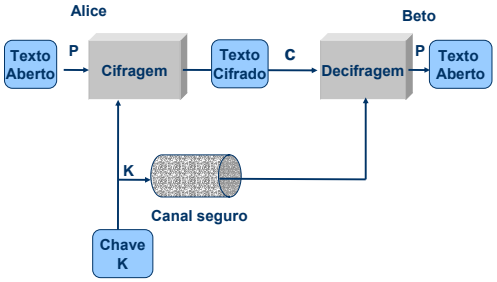
Privacidade das Comunicações

- Criptografia
  - Simétrica ou chave privada (compartilhada)
  - Assimétrica ou chave pública
    - Assinatura Digital
- *Virtual Private Network* - VPN
- *Public Key Infrastructure - PKI*
- Esteganografia

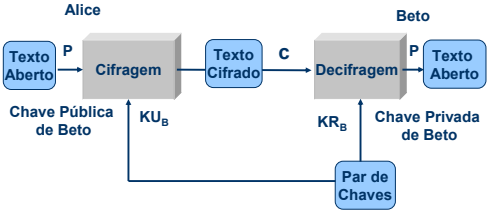
Criptografia

- criptografia tem origem grega
  - kriptos = escondido, oculto
  - grifo = grafia,escrita
- define a arte ou ciência de escrever em cifras ou em códigos
- através de técnicas torna uma mensagem incompreensível

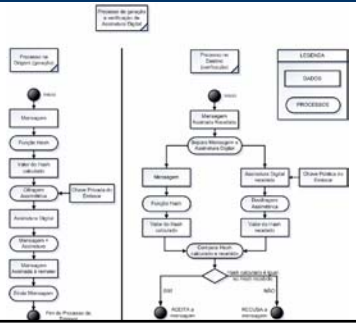
Criptografia Simétrica



Criptografia Assimétrica



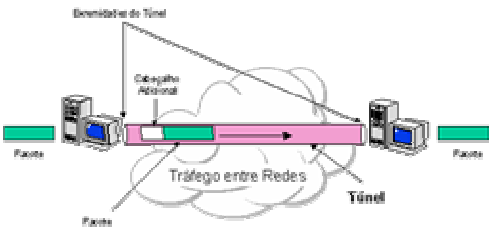
Assinatura Digital



Virtual Private Network - VPN

- São túneis de criptografia entre pontos autorizados
  - transferência segura, entre redes corporativas ou usuários remotos.

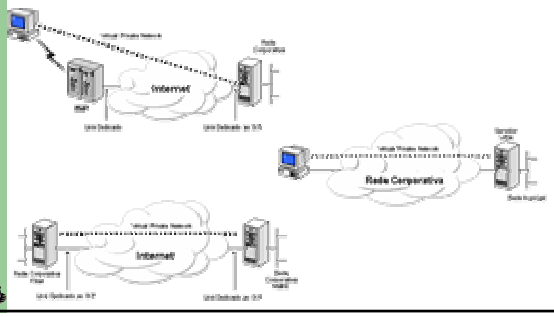
Túnel VPN



Característica de uma VPN

- Autenticação de Usuários
  - Verificação da identidade do usuário
- Gerenciamento de Endereço
  - O endereço do cliente não é divulgado
- Criptografia de Dados
- Gerenciamento de Chaves
- Suporte a Múltiplos Protocolos
  - IP (Internet Protocol), IPX (Internetwork Packet Exchange), etc.

Aplicações de uma VPN



Public Key Infrastructure

- Infra-estrutura de Chaves Públicas (ICP)
- Estabelece e garante a confiabilidade de chaves públicas de criptografia
  - atrela as chaves públicas às suas entidades
  - possibilita que outras entidades verifiquem a validade das chaves públicas
- Consegue assegurar confidencialidade, integridade e não-repúdio

Esteganografia

- Do grego "escrita coberta"
- Esconder a EXISTÊNCIA da mensagem
  - através de artifícios em imagens ou textos
- Muito utilizado através da história

Esteganografia
Segurança Monetária Suiça

- A: As cifras com a tinta Iriodin®: O número mágico.
- B: As cifras em marca d'água
- C: As cifras em talhe doce: O número que tinge
- D: O número perfurado (microperf ®)
- E: A tinta com efeito óptico variável: O número camaleão
- F: As cifras com ultravioleta
- G: As cifras metalizadas: O número cintilante
- H: O efeito basculante
- 1: Frente e verso
- 2: Marca d'água do rosto
- 3: Guillochis
- 4: Kinegram®: A cifra dançante
- 5: Microtexto
- 6: Símbolo para deficientes visuais

Service Level Agreement

- Acordo de Nível de Serviço
- A qualidade dos serviços prestados é fundamental
- São acordos formais entre fornecedores de serviço e clientes (internos e externos)
  - definem condições, responsabilidades e níveis de desempenho para os serviços

Service Level Agreement

- Podem ser definidos
  - serviços de tecnologia
  - serviços operacionais necessários ao funcionamento do negócio
    - Iluminação durante um jogo de futebol noturno
- Comum ocorrer em áreas de TI

Service Level Agreement

- Deve conter
  - Objetivos e escopo de acordo
  - Políticas do acordo
  - Atualização do SLA
  - Responsabilidades
  - Inventário dos serviços e atividades
  - Gerenciamento de segurança e problemas
  - Determinação de níveis de severidade, prioridade, objetivos e valores
  - Penalidades e benefícios por nível de serviço
  - Medições de desempenho

Outros processos

- A segurança é composto de outras atividades, tais como:
  - Análise e Gerência de Riscos
  - Planos de Continuidade
  - Estratégias de Contingência
  - Políticas de Segurança
  - Auditorias
  - Legislação
  - Outros

Então....

- Dúvidas ??
- Perguntas ??
- Comentários ??