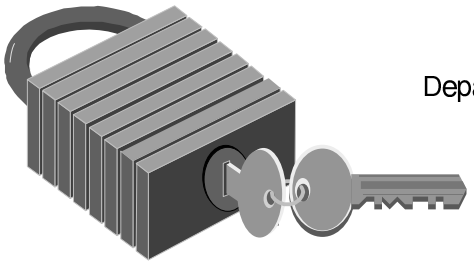
Segurança da Informação

Prof. Ricardo S. Puttini

Universidade de Brasília - UnB
Departamento de Eng. Elétrica - ENE

puttini@unb.br



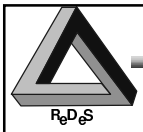
ROTEIRO

I - PRINCÍPIOS DE SEGURANÇA DA INFORMAÇÃO
- Informações, operações e componentes dos sistemas de informação
- Confidencialidade, integridade, disponibilidade
- Ameaças à segurança e medidas de proteção

II - POLÍTICA DE SEGURANÇA DA INFORMAÇÃO
- Processos da segurança
- Identificação de Elementos Vulneráveis e Possíveis Atacantes
- Avaliação de Riscos e Ordenação
- Análise de Custo-Benefício das Proteções

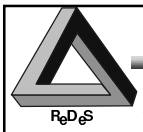
III - GERÊNCIA DAS TÉCNICAS DA SEGURANÇA DA INFORMAÇÃO
- Bom senso, segurança das pessoas, do ambiente e segurança física
- Segurança lógica: softwares, sistemas operacionais, redes
- Segurança de Redes e Sistemas Distribuídos: abordagens OSI e Internet

IV - CONCLUSÃO



I - SEGURANÇA DOS SISTEMAS DE INFORMAÇÃO

- Fatos e Princípios da Segurança dos SI
- Informações, Operações e Componentes dos SI
- Propriedades da Segurança
  - Confidencialidade
  - Integridade
  - Disponibilidade
- Vulnerabilidades e Formas de Ataque
- Tipos de Ameaças e Ataques à Segurança
- Medidas de Proteção



PRINCÍPIOS DE SEGURANÇA DE SI

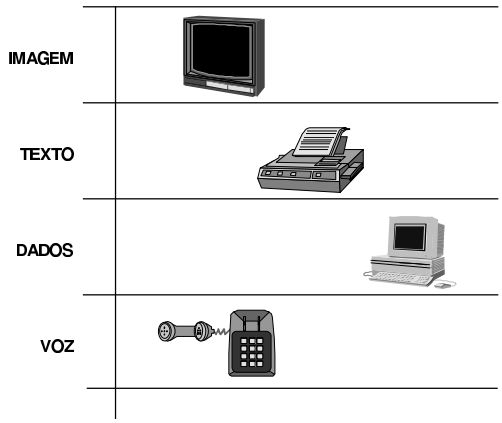
- a segurança dos Sistemas de Informação envolve um conflito das organizações contra oponentes humanos
- o oponente deve ser respeitado por ser capaz de imaginar tudo o que o defensor pode imaginar
- toda vulnerabilidade representa ao menos uma possibilidade de ponto de ataque
- com frequência, as técnicas para atacar os sistemas de informação não são sofisticadas
- **Princípio da mais fácil penetração**: o ataque pode ser efetuado por qualquer meio de penetração, não necessariamente o mais óbvio nem aquele no qual existe a defesa mais sólida
- **Princípio da vida útil**: só se deve proteger algo enquanto ele ainda tem valor

PRINCÍPIOS DE SEGURANÇA DE SI

- a mais sofisticada tecnologia de segurança não dá cobertura a práticas administrativas comprometedoras
- historicamente, a segurança tem sido vista como um empecilho ao uso eficiente dos sistemas de informação
- **princípio da efetividade**: é necessário praticar realmente os controles para que sejam efetivos
- sistemas de informação com base em redes têm maiores e mais sérios problemas de segurança:
  - mais usuários, localidades e recursos a serem protegidos
  - mais pontos e formas de ataque
  - técnicas de segurança tradicionais ineficazes

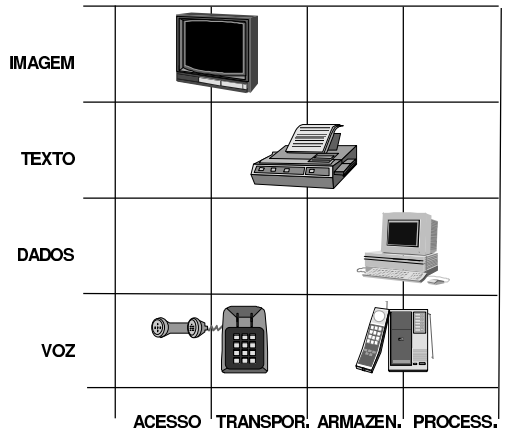
SEGURANÇA DOS SISTEMAS DE INFORMAÇÃO

- Informações tratadas



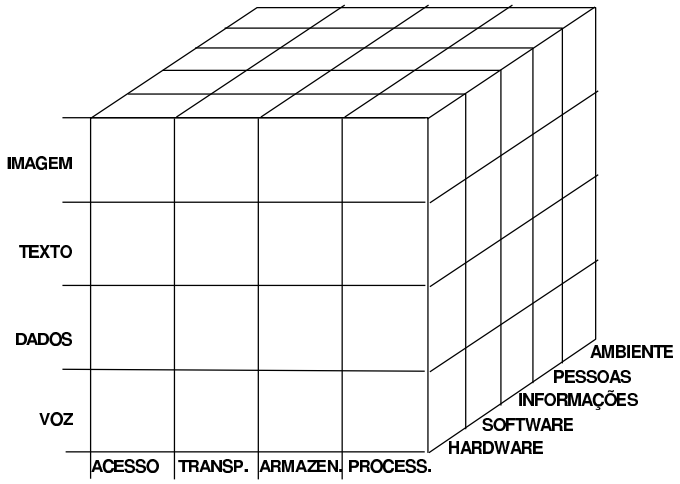
SEGURANÇA DOS SISTEMAS DE INFORMAÇÃO

- Informações tratadas e classes de operações



SEGURANÇA DOS SISTEMAS DE INFORMAÇÃO

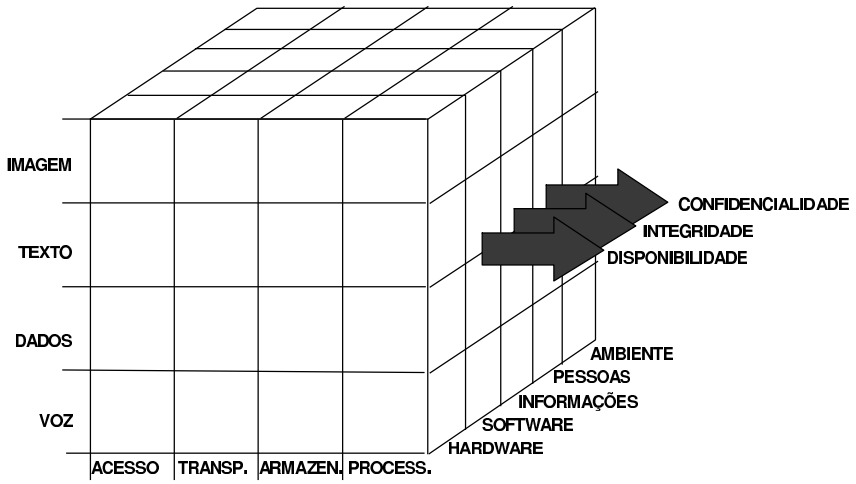
- Informações tratadas, classes de operações e componentes



SEGURANÇA DOS SISTEMAS DE INFORMAÇÃO

- Qualquer componente vulnerável pode ser alvo de um ataque
  - elementos para geração e acesso: terminais, impressoras...
  - elementos para transporte de informação: hubs, pontes, roteadores, sub-redes
  - elementos para armazenamento: memória, discos, fitas...
  - elementos para processamento da informação: computadores, PABX...
  - softwares que controlam os componentes e oferecem serviços aos usuários
  - dados que são manipulados pelos serviços de informação
  - pessoas que usam, gerenciam ou administram os serviços
- Qualquer pontos vulnerável pode ser explorado para causar perdas ou prejuízos
  - qualquer tipo de informações tratado
  - qualquer das classes de operações

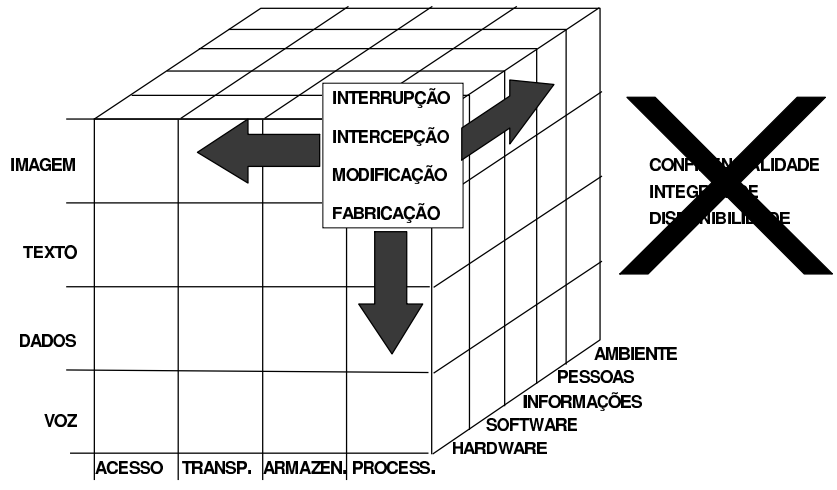
PROPRIEDADES/OBJETIVOS DA SEGURANÇA



PROPRIEDADES/OBJETIVOS DA SEGURANÇA

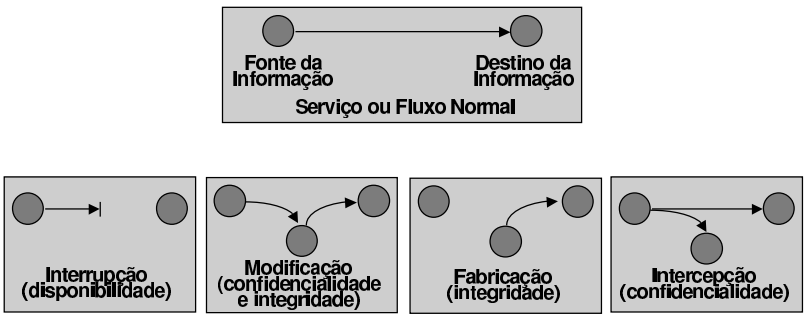
- confidencialidade
  - a informação não deve nem ficar acessível, nem ser divulgada para um usuário, uma entidade ou um processo não autorizado
- integridade
  - a informação não deve ser alterada ou destruída de maneira não autorizada
- disponibilidade
  - o acesso aos serviços oferecidos pelo sistema deve ser sempre possível para um usuário, entidade ou processo autorizado
  - Operações que procuram ocupar ilegalmente os recursos do sistema devem ser detectadas

AMEAÇAS À SEGURANÇA E VULNERABILIDADES



AMEAÇAS À SEGURANÇA E VULNERABILIDADES

- Perturbações potenciais dos serviços dos SI em redes

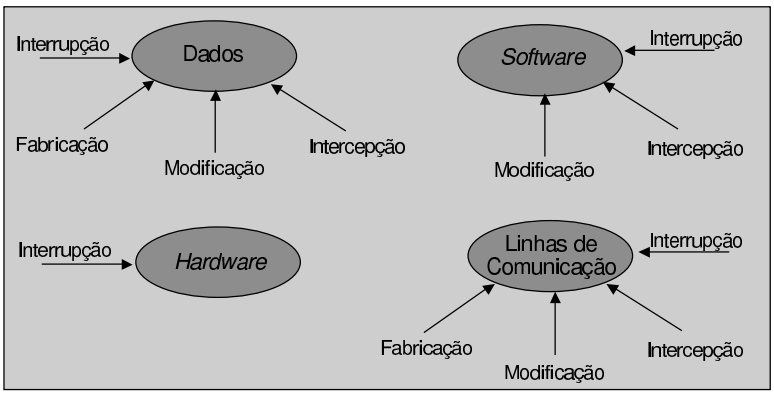


AMEAÇAS À SEGURANÇA E VULNERABILIDADES

- interrupção
  - Componente do sistema é destruído ou torna-se indisponível
  - Exemplo: rompimento de uma linha de comunicação
- intercepção
  - Componente do sistema é acessado por partes não autorizadas
  - Exemplo: cópia ilícita de de um sinal de TV que trafega via satélite
- modificação
  - Componente do sistema é acessado e sofre alterações por partes não autorizadas
  - Exemplo: modificação do valor de um pagamento por cartão de crédito durante o trânsito pela rede
- fabricação
  - Parte não autorizada insere objetos espúrios em um componente do sistema
  - Exemplo: inserção de mensagens espúrias, como no caso de geraçào de um depósito durante a madrugada a partir de uma agência bancária fechada

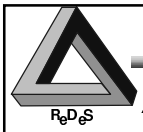
AMEAÇAS À SEGURANÇA E VULNERABILIDADES

- Tipos de ameaças aos SI de uma rede



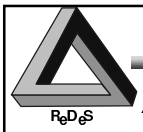
AMEAÇAS À SEGURANÇA E VULNERABILIDADES

- Tipos de ameaças aos SI de uma rede - Exemplos
  - Hardware
    - roubo de computadores, discos, disquetes
    - danos a cabos e mal funcionamento por configuração errônea
    - destruição de circuitos por descarga elétrica, micro-cortes de corrente, quedas repetidas de tensão, ventilaçào inadequada
    - danos devido a humidade, temperatura, etc
    - uso sem autorização
    - desgaste natural, inclusive agravado por limpeza e manutenção inadequadas
  - Software
    - apagamento
    - cópia não autorizada ou ilegal
    - corrupção, por exemplo, por virus ou falha em meios de armazenamento
    - erros de análise, concepção ou codificação (*bugs*)



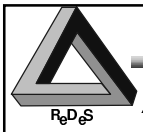
AMEAÇAS À SEGURANÇA E VULNERABILIDADES

- Tipos de ameaças aos SI de uma rede - Exemplos
  - Dados/Informações
    - apagamento deliberado ou não
    - roubo ou cópia não autorizada em nós intermediários de rede, etc
    - perda devido a erros de rede, de hardware e de software ou simplesmente por obsolescência
    - corrupção por substituição mal intencionada, erros de digitaçào, etc
  - Serviços e Operação de redes
    - interrupção das transmissões por defeito ou corte de cabos, quedas de nós de rede, etc
    - interferência, devido a ruidos eltro-magnéticos, danos a cabos e conectores, etc
    - sobrecarga, devido a geraçào de tráfego espúrio ou presnça de virus, etc



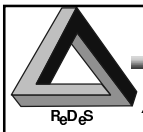
AMEAÇAS À SEGURANÇA - CLASSIFICAÇÃO

- Critérios de classificação
  - Propriedade da segurança ameaçada/comprometida
  - Possibilidades de prevenção e detecção
  - Freqüência relativa
  - Severidade relativa
  - Forma de ataque
  - Enquadramento legal
- Ameaças x Proteções - Relacionamentos Múltiplos
  - 1 ameaça impacta vários aspectos da segurança dos SI (vulnerabilidades, tipo e forma das proteções, etc)
  - 1 ameaça leva à utilização de várias medidas de proteção
  - 1 proteção permite contrabalançar várias ameaças



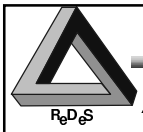
AMEAÇAS E ATAQUES

- **Alçapões** ou **Portas Laterais** ou **Portas de Fundos**: meios de entrada escondidos em um sistema, intencionais ou acidentais
  - propr. ameaç.: confidencialidade, integridade, disponibilidade
  - prevenção: muito difícil, teste e auditoria de código
  - detecção:muito difícil: por acaso
  - freqüência: alta, pode acontecer com todo hardware, rede, programa de computador, sistema operacional, banco de dados
  - severidade: muito alta
  - forma: fabricação-> interrupção, intercepção, modificação, fabricação
  - enquadr. legal: proteção consumidor ?
- **Inépcia**: erros humanos, acidentes, omissões
  - propr. ameaç.: confidencialidade, integridade, disponibilidade
  - prevenção: muito difícil, treinamento e suporte ao usuário
  - detecção:às vezes fácil, às vezes muito díficil
  - freqüência: alta, é o risco mais comum
  - severidade: muito alta
  - forma: modificação, fabricação
  - enquadr. legal: leis trabalhistas ?



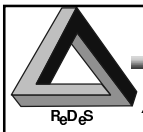
AMEAÇAS E ATAQUES

- **Negação de uso**: fechamento de portas, modificação de nomes, apagamento de programas...
  - propr. ameaç.: disponibilidade
  - prevenção: muito difícil, proteção de áreas do usuário na memória e nos discos, reconfiguração sistemática de portas, verificação de modificações de nomes, detecção de atividade suspeita
  - detecção:fácil, o serviço para
  - freqüência: baixa
  - severidade: alta
  - forma: interrupção
  - enquadr. legal: proteção do consumidor ?, leis trabalhistas ?
- **Emanações**: vazamentos de sinais eletromagnéticos
  - propr. ameaç.: confidencialidade
  - prevenção: muito difícil, escudos e blindagens
  - detecção:impossível
  - freqüência: alta, caso do celular, satélites, televisão
  - severidade: alta
  - forma: intercepção-> modificação, fabricação
  - enquadr. legal: proteção ambiental ?, direito autoral ?



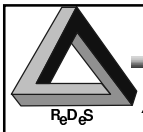
AMEAÇAS E ATAQUES

- **Desfalque/malversação**: roubo de dinheiro através de meios computacionais
- **Ataque salame**: soma de pequenos valores para obter um montante vultoso
  - propr. ameaç.: integridade
  - prevenção: difícil, controles de software/SGBD, auditoria/teste de programas
  - detecção:difícil, auditoria diária sistemática de bancos de dados, observação do estilo de vida dos usuários
  - freqüência: esporádica
  - severidade: alta
  - forma: modificação, fabricação
  - enquadr. legal: proteção da propriedade e do consumidor, leis trabalhistas
- **Não uso**: não utilização de computadores, não fornecimento de dados...
  - propr. ameaç.: disponibilidade, integridade
  - prevenção: difícil, manuais de utilização, formação ética
  - detecção:difícil, registro de utilização, acompanhamento do consumo de recursos: armazenamento, comunicações
  - freqüência: esporádica
  - severidade: alta
  - forma: interrupção
  - enquadr. legal: leis trabalhistas



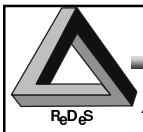
AMEAÇAS E ATAQUES

- **Incêndio** e **incidentes naturais**
  - propr. ameaç.: integridade, disponibilidade
  - prevenção: difícil, dispositivos específicos, backup de dados e programas e configurações de equipamentos, duplicação de centros de processamento
  - detecção:fácil
  - freqüência: conhecida para cada bairro/localidade, pelos bombeiros, polícia, seguradoras
  - severidade: alta
  - forma: interrupção
  - enquadr. legal: proteção da propriedade, regulamentação de seguros
- **Falsificação**: criação ilegal de documentos ou registros, que aparentam ser reais e oficiais
  - propr. ameaç.: integridade
  - prevenção: difícil
  - detecção:difícil, verificação cruzada
  - freqüência: alta
  - severidade: alta
  - forma: fabricação
  - enquadr. legal: falsificação de documentos, falsificação de identidade



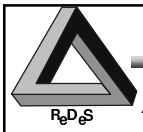
AMEAÇAS E ATAQUES

- **Fraude**: exploração de um SI para enganar uma organização
  - propr. ameaç.: integridade
  - prevenção: difícil, controles de software sobre a entrada de dados
  - detecção:difícil, controles de software, auditoria de bancos de dados
  - freqüência: indeterminada, exemplo de transações bancárias fora do expediente
  - severidade: alta
  - forma: fabricação
  - enquadr. legal: proteção da propriedade, leis trabalhistas ?
- **Falhas de hardware**
  - propr. ameaç.: confidencialidade, integridade, disponibilidade
  - prevenção: impossível, mas há como contornar: backup de dados e programas e configurações de equipamentos, duplicação de centros de processamento, programas de manutenção
  - detecção:às vezes fácil, às vezes muito díficil
  - freqüência: comum, estimativas de MTBF conhecidas
  - severidade: alta
  - forma: interrupção, intercepção-> modificação, fabricação
  - enquadr. legal: proteção consumidor ?, contratos de serviço ?



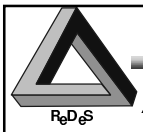
AMEAÇAS E ATAQUES

- **Imitação**: uso dos códigos de acesso de outrem para obter acesso a computadores e realizar outras operações
  - propr. ameaç.: confidencialidade, integridade, disponibilidade
  - prevenção: muito difícil, controle de acesso com dispositivos biométricos, modens com chamada reversa, política de senhas e de validação
  - detecção:muito difícil, auditoria de registros de uso
  - freqüência: esporádica, caso dos hackers
  - severidade: alta
  - forma: intercepção, modificação-> interrupção, intercepção, modificação, fabricação
  - enquadr. legal: ?
- **Informação incorreta** ou **informação caduca**
  - propr. ameaç.: integridade
  - prevenção: muito difícil, controles de SGBD
  - detecção:muito difícil, controles e auditoria de SGBD
  - freqüência: comum
  - severidade: alta
  - forma: interrupção, fabricação
  - enquadr. legal: direitos individuais, comerciais e tributários



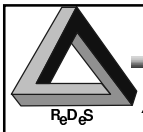
AMEAÇAS E ATAQUES

- **Dano intencional** a programas ou dados: destruição usando dispositivos eletromagnéticos, programas maliciosos, ferramentas de gerência...
  - propr. ameaç.: integridade
  - prevenção: muito difícil, guarda das instalações, regulamentação do acesso
  - detecção:pode ser muito difícil ou muito tardia
  - freqüência: baixa
  - severidade: alta
  - forma: interrupção
  - enquadr. legal: proteção da propriedade, uso indevido
- **Bombas lógicas**: modificação de um programa para fazê-lo executar de modo diferente, dadas algumas circunstâncias especiais
  - propr. ameaç.: confidencialidade, integridade, disponibilidade
  - prevenção: muito difícil, teste e auditoria de código, recompilação, backup de dados e software
  - detecção:pode ser difícil, auditoria
  - freqüência: baixa
  - severidade: alta
  - forma: fabricação-> interrupção, intercepção, modificação, fabricação
  - enquadr. legal: direito autoral ?



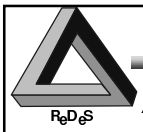
AMEAÇAS E ATAQUES

- **Embuste**: uso do computador para enganar ou intimidar, com algum objetivo final
  - propr. ameaç.: confidencialidade
  - prevenção: muito difícil
  - detecção:muito difícil
  - freqüência: baixa
  - severidade: alta
  - forma: fabricação
  - enquadr. legal: direito do consumidor ?
- **Erro de roteamento**: entrega de mensagens a destinatário inválido ou não autorizado
  - propr. ameaç.: confidencialidade
  - prevenção: muito difícil, verificação de programas, configuração de equipamentos e de rede
  - detecção:pode ser fácil
  - freqüência: pode ser comum
  - severidade: alta
  - forma: intercepção
  - enquadr. legal: inviolabilidade da correspondência ?



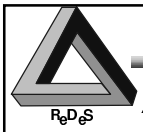
AMEAÇAS E ATAQUES

- **Analisadores de rede**
  - propr. ameaç.: confidencialidade
  - prevenção: criptografia
  - detecção:muito difícil ou impossível
  - freqüência: cada vez mais comum
  - severidade: alta
  - forma: intercepção-> interrupção, modificação, fabricação
  - enquadr. legal: ?
- **Riscos ocupacionais**: radiação, síndromes musculares...
  - propr. ameaç.: disponibilidade
  - prevenção: difícil, exercícios, afastamento periódico
  - detecção:difícil ou tardia, procedimentos administrativos, exames de saúde programados
  - freqüência: cada vez mais comum
  - severidade: alta
  - forma: interrupção
  - enquadr. legal: leis de proteção ambiental, leis trabalhistas



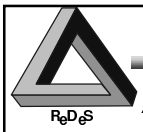
AMEAÇAS E ATAQUES

- **Sobrecarga**
  - propr. ameaç.: disponibilidade
  - prevenção: muito difícil, verificação de projeto, gerência proativa de desempenho, cuidados na distribuição de login e outros recursos
  - detecção:fácil
  - freqüência: comum em novos sistemas
  - severidade: alta
  - forma: interrupção
  - enquadr. legal: acordos e contratos de nível de serviço, proteção ao consumidor
- **Carona física ou eletrônica**: acesso a instalações ou a sistemas depois de um usuário autorizado que não terminou corretamente a sessão de uso
  - propr. ameaç.: confidencialidade, integridade, disponibilidade
  - prevenção: muito difícil, guardas, procedimentos administrativos, controles de sistema operacional
  - detecção:muito difícil, auditoria de modelos e perfis de uso
  - freqüência: comum
  - severidade: alta
  - forma: intercepção, modificação-> interrupção, intercepção, modificação, fabricação
  - enquadr. legal: leis sobre uso indevido, falsificação de identidade



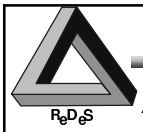
AMEAÇAS E ATAQUES

- **Pirataria**: processo de cópia ilegal de software e documentação para outros usos
  - propr. ameaç.: confidencialidade, integridade, disponibilidade
  - prevenção: muito difícil, proteções de software, licensas datadas
  - detecção:difícil
  - freqüência: alta
  - severidade: alta
  - forma: intercepção-> modificação, fabricação
  - enquadr. legal: direito autoral, lei de patentes
- **Erros de programação**
  - propr. ameaç.: confidencialidade, integridade, disponibilidade
  - prevenção: impossível devido à grande variedade de erros
  - detecção:às vezes difícil
  - freqüência: comum
  - severidade: alta
  - forma: fabricação
  - enquadr. legal: ?, contrato fornecedor-cliente ?



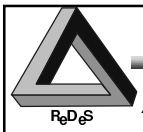
AMEAÇAS E ATAQUES

- **Sabotagem**: dano físico ou lógico, tiro, explosão, incêndio, corte de energia, modificação de rótulos e de arquivos...
  - propr. ameaç.: integridade, disponibilidade
  - prevenção: muito difícil, segurança física, backup, duplicação
  - detecção:pode ser fácil ou difícil
  - freqüência: baixa
  - severidade: alta
  - forma: interrupção, modificação, fabricação
  - enquadr. legal: proteção da propriedade, leis trabalhistas ?
- **Catadores**: coleta de lixo computacional (listagens, fitas, discos, cópias carbono...), recuperação de arquivos apagados...
  - propr. ameaç.: confidencialidade
  - prevenção: difícil, destruição de documentos impressos e fitas de impressão, apagamento físico e reformatação de discos e fitas
  - detecção:muito difícil ou impossível
  - freqüência: provavelmente comum
  - severidade: alta
  - forma: intercepção
  - enquadr. legal: espionagem industrial, comercial



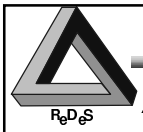
AMEAÇAS E ATAQUES

- **Simulação** e **modelagem**: operações que permitem prepara outros ataques, com maior sucesso ou melhores resultados
  - propr. ameaç.: confidencialidade, integridade, disponibilidade
  - prevenção: muito difícil ou impossível
  - detecção:muito difícil ou impossível
  - freqüência: esporádica
  - severidade: alta
  - forma: intercepção-> modificação, fabricação
  - enquadr. legal: uso indevido ?
- **Softwares de remendo**: ferramentas que permitem ao operador iniciar, parar e modificar procedimentos que estão tendo comportamento errôneo
  - propr. ameaç.: confidencialidade
  - prevenção: difícil, senhas, múltipla autorização
  - detecção:difícil
  - freqüência: esporádica
  - severidade: alta
  - forma: interrupção, modificação, fabricação
  - enquadr. legal: ?



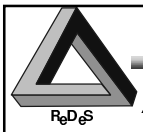
AMEAÇAS E ATAQUES

- **Roubo de equipamentos**, **Roubo de informações** (vazamento, canais escondidos, vermes, cópias de programas, escuta telefônica, captura de sinais de TV e rádio), **Roubo de serviços** (conexões de dados, chamadas telefônicas, ciclos de processamento, vermes)
  - propr. ameaç.: confidencialidade, integridade, disponibilidade
  - prevenção: muito difícil
  - detecção:muito difícil
  - freqüência: provavelmente alta
  - severidade: alta
  - forma: intercepção-> interrupção, intercepção, modificação, fabricação
  - enquadr. legal: roubos e furtos, direito autoral ?
- **Cavalo de Tróia**: qualquer programa que aparenta fazer uma tarefa, enquanto na verdade faz outra coisa
  - propr. ameaç: confidencialidade, integridade, disponibilidade
  - prevenção: muito difícil, verificação de alterações de software, versões de referência
  - detecção:muito difícil, detecção de atividade anormal, auditoria
  - freqüência: indeterminada
  - severidade: alta
  - forma: interrupção, intercepção, modificação, fabricação
  - enquadr. legal: ?



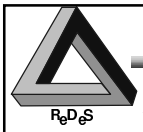
AMEAÇAS E ATAQUES

- **Controle de versões de software**
  - propr. ameaç.: integridade
  - prevenção: difícil, softwares de controle de versão
  - detecção:difícil, softwares de controle de versão, versões de referência e atualizações sistemáticas
  - freqüência: comum
  - severidade: indeterminada
  - forma: modificação, fabricação
  - enquadr. legal: regras/política interna, contratos com forneedores
- **Vírus**
  - propr. ameaç.: integridade, disponibilidade
  - prevenção: pode ser difícil, verificação de softwares, versões de referência
  - detecção:pode ser difícil, detecção de atividade anormal
  - freqüência: muito alta
  - severidade: usualmente baixa, mas pode ser alta
  - forma: interrupção, intercepção, modificação, fabricação
  - enquadr. legal: proteção ambiental ?, direito autoral ?



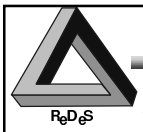
AMEAÇAS E ATAQUES

- Escuta dos meios de transmissão
- Grampeamento telefônico
- Captura de sinais de micro-ondas e satélites
  - propr. ameaç.: confidencialidade
  - prevenção: criptografia
  - detecção: difícil ou impossível
  - freqüência: alta, caso do celular, satélites, televisão
  - severidade: alta
  - forma: intercepção
  - enquadr. legal: leis sobre escuta telefônica e espionagem industrial



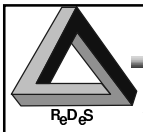
PROTEÇÃO DOS SISTEMAS DE INFORMAÇÃO

- Medidas de proteção ou defesas contra ataques ou acidentes
- Medidas físicas:
  - guarda da sala de equipamentos
  - o confinamento dos computadores em ambientes blindados...
  - constituem a segurança física
- Medidas técnicas/lógicas:
  - através de mecanismos lógicos, ou com base em softwares
  - garante-se a segurança das informações e o controle da utilização delas
  - constituem a segurança técnica/lógica
- Medidas organizacionais:
  - restrições de natureza administrativa, como a obrigação de atribuir um identificador a cada usuário do sistema
  - constituem a segurança organizacional ou administrativa



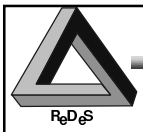
PROTEÇÃO DOS SISTEMAS DE INFORMAÇÃO

- medidas físicas e organizacionais permitem proteger tanto o hardware quanto os elementos lógicos (software e informações) do sistema
- medidas técnicas/lógicas protegem apenas as informações e os softwares
- em um sistema real, uma segurança eficaz requer a utilização simultânea de mecanismos dos três tipos acima
- a escolha de mecanismos específicos é função da política de segurança adotada no ambiente de utilização do sistema, ou seja na empresa ou organização usuária



PROTEÇÃO DOS SISTEMAS DE INFORMAÇÃO

- Escolha de medidas de proteção adequadas e implementação
  - Medidas de prevenção
  - Medidas de detecção
  - Medidas de limitação de danos
- Processo de escolha
  - Avaliação de ameaças e riscos e da correlação destes com prejuízos
  - Escolha de proteções em função de avaliação dos custos
  - Critérios para escolha das proteções
    - Núcleo de segurança básico
    - Adequaçào técnica das medidas de proteção
    - Análise de riscos: confrontação dos prejuízos potenciais com os custos das medidas consideradas tecnicamente apropriadas
- Implementação das medidas, dos processos e da política de segurança



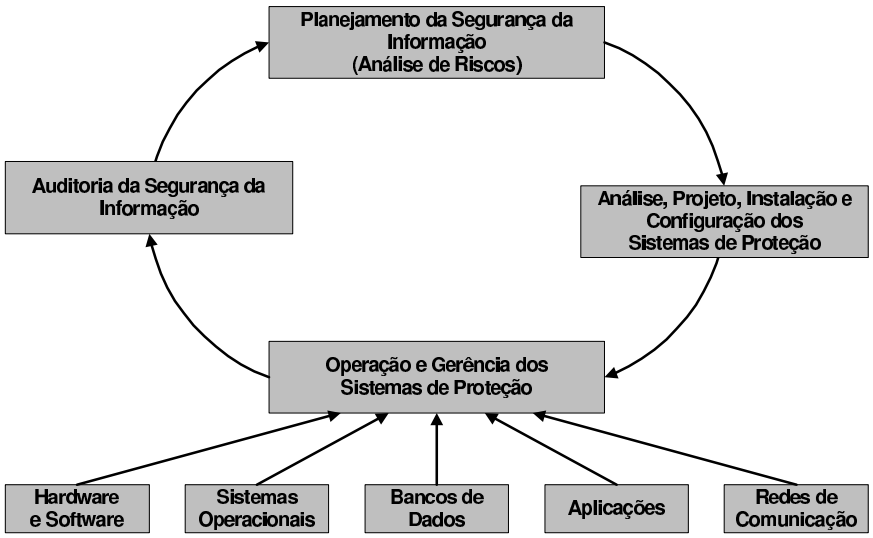
II - POLÍTICA DE SEGURANÇA

- Processos e Política da Segurança
- Seleção de Elementos Vulneráveis
- Levantamento de Possíveis Atacantes
- Avaliação de Riscos e Ordenaçào
- Análise de Custo-Benefício das Proteções

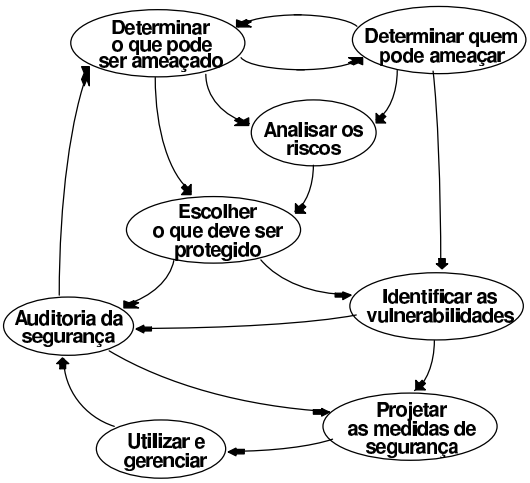
PROCESSOS DA SEGURANÇA

- Levantamento dos recursos de segurança existentes: técnicas, pessoas, processos de trabalho, custos
- Estabelecimento e documentação do processo relativo à segurança da informação na empresa
- Determinação daquilo que pode ser ameaçado e por quem
- Análise e avaliação dos riscos
- Determinação do que deve ser protegido
- Identificação das vulnerabilidades e as formas de ataque
- Projeto e implementação de medidas de segurança (físicas, organizacionais e lógicas)
- Utilização e gerência das medidas de segurança implementadas
- Avaliação/Auditoria da segurança e revisão dos processos e técnicas utilizados

PROCESSOS E POLÍTICA DE SEGURANÇA

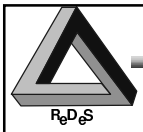


PROCESSOS E POLÍTICA DE SEGURANÇA



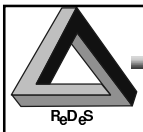
SELEÇÃO DE ELEMENTOS VULNERÁVEIS

- O que pode ser ameaçado
  - hardware
    - objetos e equipamentos
    - material (por exemplo, o cobre) e insumos (papel, fitas...)
  - software
    - software-produto
    - software-elemento operacional
  - informações
    - econômicas ou de mercado de empresas privadas
    - econômicas de instituições do governo
    - econômicas e de mercado (globalmente)
    - sobre indivíduos
    - financeiras, jurídicas ou legais, administrativas
    - técnicas (métodos, procedimentos) e científicas
    - pessoais
  - pessoas
  - ambiente



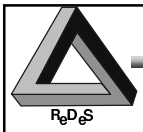
LEVANTAMENTO DE POSSÍVEIS ATACANTES

- Quem ameaça a segurança
  - incidentes externos ou eventos da natureza
  - empregados através de ações sem intenção ou por acidente (inépcia)
  - empregados através de ataques e intrusões acobertadas
  - empregados através de ações de sabotagem às claras
  - ex-empregados
  - pessoal externo obtendo acesso não autorizado: pessoal de suporte/manutenção, hackers



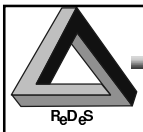
LEVANTAMENTO DE RISCOS E VULNERABILIDADES

- Avaliação dos riscos
  - prejuízos financeiros (diretos, processos judiciais, idenizações...)
  - prejuízos de imagem (publicidade adversa, perda de confiança, imagem de incompetência...)
  - revelação de segredos do negócio
  - divulgação de savoir-faire, etc
- Vulnerabilidades
  - Pontos fracos relativamente à segurança: ambientais, físicos, hardware, software, humanos, media...
  - Prováveis formas de ataque



CLASSIFICAÇÃO/ORDENAÇÃO DOS RISCOS

- Classificação dos riscos
  - ordenação de riscos, vulnerabilidades, severidades
  - levantamento de freqüência de ataques
  - valoração da severidade
  - avaliação de prejuizos
- Análise de custo/benefício
  - avaliação de custo das proteções
  - cálculo de custo/benefício



CLASSIFICAÇÃO/ORDENAÇÃO DOS RISCOS

- Avaliação dos riscos - Análise de custo/benefício - Bens, vulnerabilidades e ataques

Bens	Confidencialidade	Integridade	Disponibilidade
hardware		sabotagem	roubo sabotagem
software	pirataria acesso ilegal	vírus	licença insuf. erros de progr.
dados	vazamento inferência		
pessoas	contrat. concorr.		doenças contrat. concorr.
ambiente			incêndio inundação

CLASSIFICAÇÃO/ORDENAÇÃO DOS RISCOS

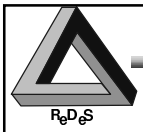
- Avaliação dos riscos - Análise de custo/benefício - Ordenação de riscos
  - equipe de análise comparativa de riscos
  - escolha do critério de comparação: probabilidade de ocorrência, severidade...
  - riscos comparados 2 a 2:
    - cada ataque é comparado com cada um dos outros uma e somente uma vez
    - cada membro da equipe vota por um ataque (1 voto) ou pelo outro (1 voto), conforme avaliação pessoa do peso do risco
    - membros da equipe podem dividir o voto (0,5 voto e 0,5 voto), quando os riscos forem de mesmo peso

CLASSIFICAÇÃO/ORDENAÇÃO DOS RISCOS

- Avaliação dos riscos - Análise de custo/benefício - Ordenação de riscos
  - tabulação - probabilidade de ocorrência:

Total de Votos						
7,5	Erros de Progr.	Erros de Progr.				
10,0	Roubo	3	Roubo			
		2				
1,5	Incêndio	3,5	5	Incêndio		
		1,5	0			
11,0	Vírus	1	3	0	Vírus	
		4	2	5		

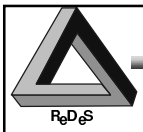
  - ordenação: Vírus (11,0), Roubo (10,0), Erros de Programação (7,5), Incêndio (1,5)
  - mesmo procedimento de valoração deve ser realizado para a probabilidade de ocorrência e a severidade das ameaças



CLASSIFICAÇÃO/ORDENAÇÃO DOS RISCOS

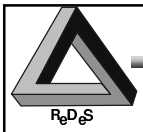
- Avaliação dos riscos - Análise de custo/benefício

		ataque: Vírus proteção: anti-Vírus	ataque: Roubo proteção: seguro e guardas
1	chances de ocorrência se não houver proteção (número de ocorrências por ano)	10	7
2	severidade: prejuízos financeiros, prejuízos de imagem, custos de recuperação após incidente ($)	5500,00	14000,00
3	chances de ocorrência se houver proteção (número de ocorrências por ano)	2	1
4	severidade do evento, havendo proteção (= item3 * item2 / item1)	1100,00 (=2*5500/10)	2000,00 (=1*14000/7)
5	benefícios da proteção (= item4 - item2)	-4400,00 (1100-5500)	-12000,00 (2000-14000)
6	custos da prevenção	500,00	15800,00
7	alteração do custo relativo ao risco (= item5 - item 6)	-3900,00 (-4400+500)	+3800,00 (-12000+15800)



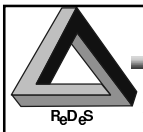
PROJETO, IMPLANTAÇÃO DE PROTEÇÕES

- Projeto
  - Escolha, em função do custo, de ações e técnicas de segurança física, organizacional ou lógica que devem ser colocadas em prática
  - Processo interativo com várias retro-alimentações e reavaliações de riscos e custos
  - Necessidade de verificação das várias possibilidades de contraposição entre proteções e ataques
- Aquisições, instalação e configuração
- Treinamento



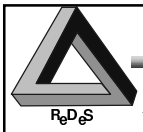
GERÊNCIA E AUDITORIA DA SEGURANÇA

- Gerência da segurança
  - ativação e operação dos mecanismos de segurança
  - detecção e relatório de eventos relativos à segurança
  - limitação de danos e reação a eventos relativos à segurança
  - registro para a auditoria de segurança
- Auditoria da segurança
  - revista e exame de registros do sistema e das atividades
  - teste da pertinência das medidas de segurança
  - teste da conformidade com a política de segurança
  - detecção de pontos vulneráveis e falhas da segurança
  - recomendação de modificações da política e das medidas de segurança



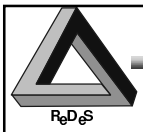
DOCUMENTAÇÃO DA POLÍTICA DE SEGURANÇA

- Responsabilidades dos usuários
  - modificações de *password*, formatos dos mesmos
  - verificações de arquivos, bd, etc para detectar intrusões
  - tratamento do 'lixo' informacional
- Responsabilidades dos administradores do SI
  - medidas de segurança e comportamento esperado dos administradores
  - procedimentos de monitoração, registro e controle de incidentes
- Modo apropriado de utilização dos recursos do SI
  - quem e quando pode usar recursos
  - o que pode e o que não pode ser feito
  - modos de controle de uso, inclusive monitoraçào existente
- Ações a executar quando um problema de segurança for detectado
  - o que fazer, quem deve ser notificado
  - passos a serem seguidos para conter um ataque e limitar seus efeitos



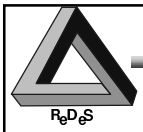
INTERESSES DA POLÍTICA DE SEGURANÇA

- Seriedade no tratamento dos aspectos de segurança
- Interesse e postura proativa
- Consciência e ponderaçào dos riscos
- Postura ética
- Atendimento a requisitos/exigências legais
- Planejamento e integração do uso das técnicas das segurança
- Conscientização dos usuários e administradores dos SI



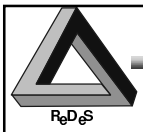
III - GERÊNCIA DAS TÉCNICAS DA SEGURANÇA DE REDES

- Tipos de Controles e Proteções
- Bom Senso
- Segurança das Pessoas e do Ambiente
- Segurança Física
- Segurança Lógica
  - Segurança de Programas
  - Segurança de Sistemas Operacionais
  - Segurança de Computadores Pessoais
  - Segurança de Bancos de Dados
  - Segurança de Redes



CONTROLES E PROTEÇÕES

- Bom senso
- Segurança física: controles e dispositivos
- Segurança lógica
  - criptografia e protocolos seguros
  - controle de acesso
  - segurança multinivelada para pessoas, programas, dados, sistemas
  - sistemas operacionais: identificação, autenticação, proteção, na concepção e na implementação
  - programas: no desenvolvimento, na execução
  - bancos de dados: acesso, robustez, inferências
  - computadores pessoais: acesso, proteção
  - redes: acesso, trocas de informação, meios de comunicação
- Segurança administrativo-organizacional: procedimentos para todos os controles, pessoas e ambiente

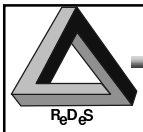


BOM SENSO

- Proteções conhecidas, de baixo ou nenhum custo

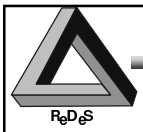
- *Backup*
  - ferramenta operacional
  - sistemática diária e semanal
  - eliminação de arquivos inúteis e duplicatas
  - armazenamento e rotulação
  - testes de restauração

- Prevenção de roubo
  - marcagem de equipamentos
  - rotulação, fechamento e selagem
  - confinamento, registro de números de série
  - contrato de seguro
  - criptografia de arquivos



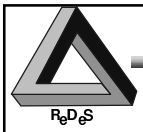
BOM SENSO

- Prevenção de vírus
  - treinamento e suporte a usuários
  - desabilitação de *drives*
  - proteção de diretórios e arquivos executáveis
  - verificação de modificações no ambiente dos usuários
  - esquadrinhamento da memória
  - detecção de atividade espúria
- Controle de acesso
  - modificação sistemática de senhas
  - uso de softwares de bloqueio
  - modems com chamada de retorno (*call-back*)
  - escolha de mensagens de acolha pouco reveladoras
  - apresentação de mensagem de acolha sobre política de segurança



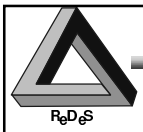
BOM SENSO

- Uso de ferramentas de segurança presentes nos sistemas
  - computadores pessoais
  - sistemas operacionais de rede
  - ferramentas de auditoria
- Prevenção de ataques externos
  - uso de softwares de bloqueio
  - confinamento de impressoras e procedimento de impressão seguro
  - procedimento de destruição de lixo
  - uso de discos removíveis
  - desabilitação de *drives*
  - detecção de inatividade
  - bloqueio de consoles e estações
  - modems com chamada de retorno
  - escolha de mensagens de acolha
  - desabilitação de logins de fábrica: suporte/manutenção remotos, administradores de sistema



BOM SENSO

- Prevenção de falhas prematuras do hardware
  - controle de temperatura
  - cuidados de transporte
  - cuidados com ferramentas de diagnóstico
  - reformatação anual
- Preparação para desastres
  - poucos arquivos em diretórios raiz
  - cópia da configuração de *firmware*
  - treinamento e suporte a usuários
  - preparação e divulgação dos procedimentos de segurança
- Conhecimento de técnicas de recuperação de dados
  - treinamento e suporte a usuários



SEGURANÇA FÍSICA

Ameaças e Vulnerabilidades

Incidentes naturais ou do ambiente

- inundações
- fogo
- calor
- energia

Vandalismo

Acesso não autorizado a instalações e recursos

Controles e Proteções

Suprimento de energia contínuo e supressão de descargas

Plano de Contingência

- *back-up* no local e algures
- identificão de componentes
- plano de desligamento e evacuação
- instalação reserva
- plano de retomada

Proteções contra intrusos

- guarda
- amarração de equipamentos
- detecção de saídas
- controle de acesso de seres humanos

Tratamento do lixo sensível e das emissões eletro-magnéticas

Controle de acesso e autentificação

SEGURANÇA DAS PESSOAS E DO AMBIENTE

Ameaças e Vulnerabilidades

comportamento das pessoas

comportamento das organizações

Controles e Proteções

Leis de proteção para programas e informações

- *copyrigth*
- patentes
- segredos negociais

Proteções de código de programas, documentos e bancos de dados

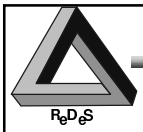
Regulamentação de contratos de emprego

Repressão ao cibercrime

Ética

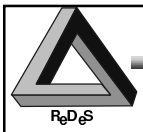
SEGURANÇA TÉCNICA/LÓGICA - BASES

- Criptografia e protocolos seguros
  - esquemas com uma ou com duas ou mais chaves
  - protocolo de assinatura digital
  - jogo de cartas mental
  - voto por computador
  - transferência com significado da mensagem revelado apenas no final
  - assinatura de contratos
  - certificação de correio
  - distribuição de chaves de criptografia
- Controle de Acesso
- Segurança Multinível



SEGURANÇA TÉCNICA/LÓGICA - CRIPTOGRAFIA

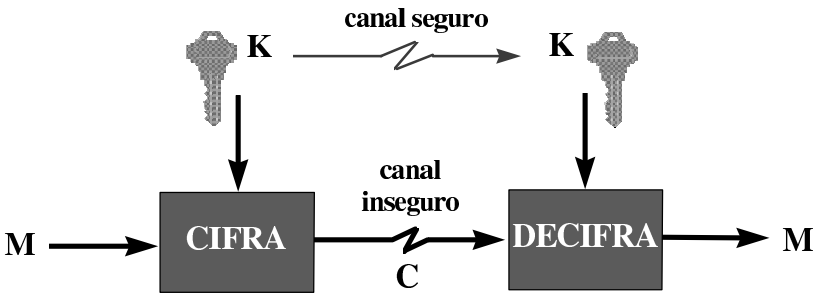
- Métodos de Criptografia - Características
  - Serviços de segurança providos
  - Algoritmos
  - Protocolos de Utilização
  - Gerência de Chaves Criptográficas



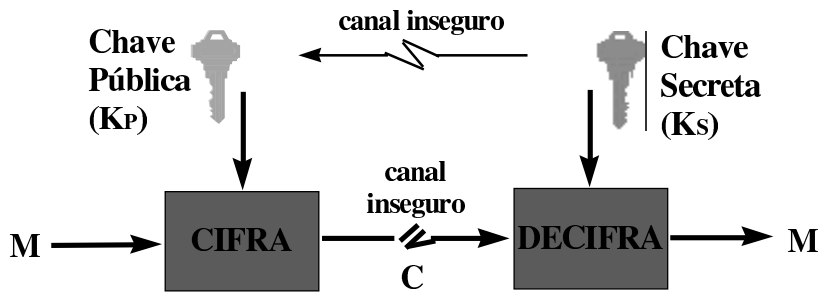
CRIPTOGRAFIA - SERVIÇOS DE SEGURANÇA

- Confidencialidade/Privacidade/Segredo
  - Confiança em que a mensagem possa ser lida apenas pelo receptor desejado
- Autentificação da Origem
  - Garantia sobre quem originou a mensagem
- Integridade da Mensagem
  - Confiança em que a mensagem não tenha sido modificada desde o momento da criação

CRIPTOSISTEMA C/CHAVE SECRETA (SIMÉTRICO)

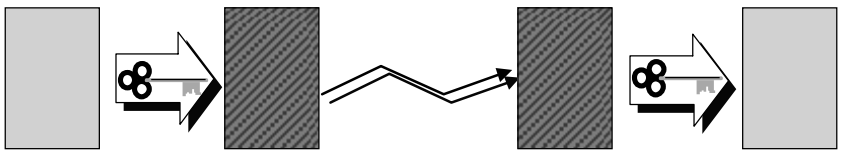


CRIPTOSISTEMA C/CHAVE PÚBLICA (ASSIMÉTRICO)



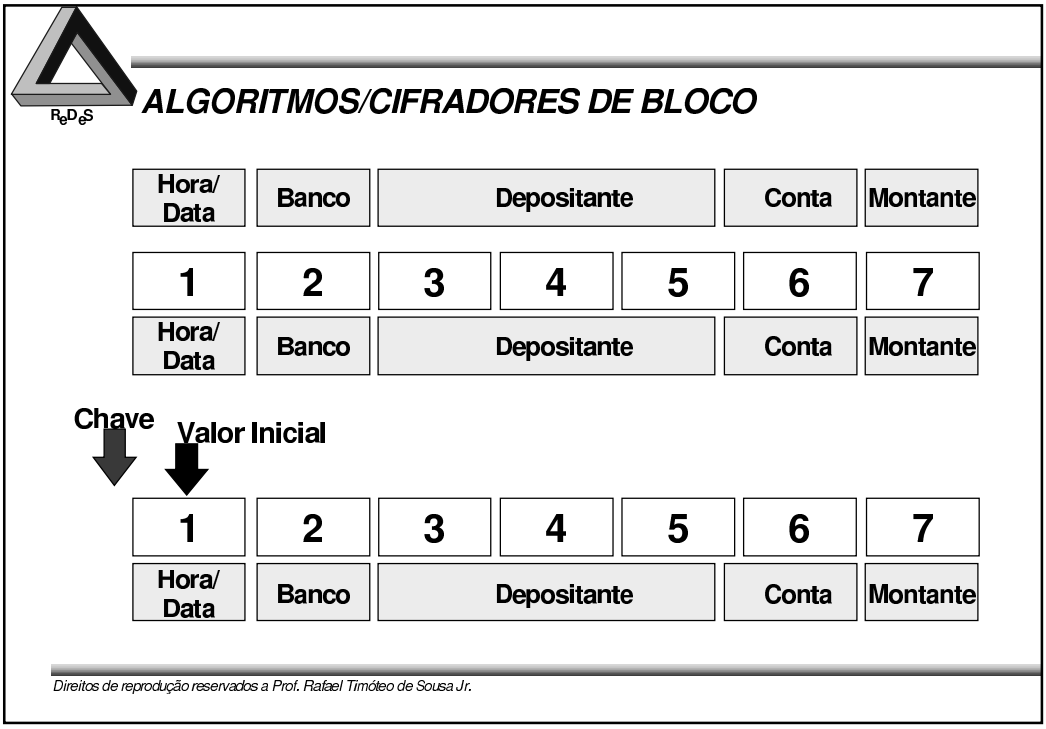
ALGORITMOS - CRIPTOGRAFIA TRADICIONAL

- Cryptografia com 'Chave Secreta' ou 'Simétrica'
- Mesma chave usada para cifrar e decifrar



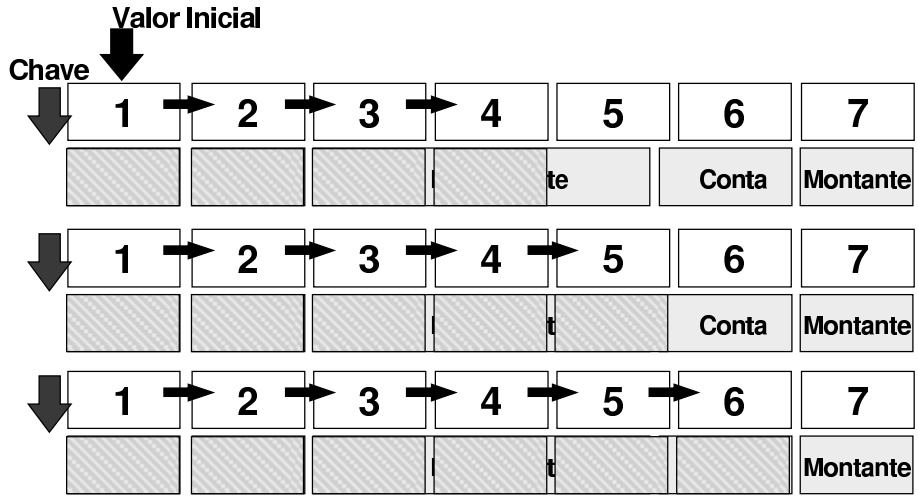
ALGORITMOS/CIFRADORES DE BLOCO SIMÉTRICOS

- DES
  - Blocos de 8-bytes ou 64-bits
  - 16 interações sucessivas, cada uma constando de substituição seguida de permutação de bits da mensagem original
  - Tamanho efetivo da chave fixo: 56 bits + 8 bits de paridade
  - Em média, a chave pode ser quebrada em 2^{56-1} = 3,6 x 10^{16} tentativas
  - Padrão americano: US FIPS 46-1
- Triplo-DES
  - Blocos de 8-bytes
  - 2 ou 3 três chaves usadas comumente
- RC2
  - Blocos de 8-bytes
  - Tamanho efetivo da chave variável: até 256 bits
  - Propriedade da RSA, exportável
  - Tamanho da código = metade de DES
  - Velocidade = 2 vezes DES

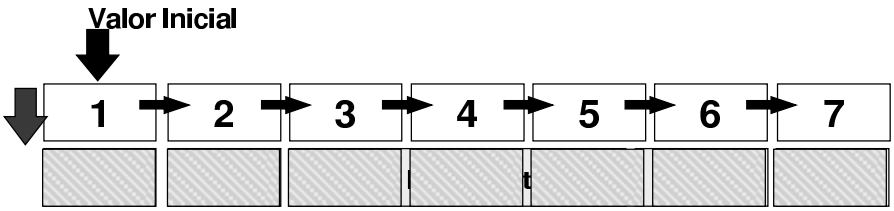

ALGORITMOS/CIFRADORES DE BLOCO
Hora/ Data
Banco
Depositante
Conta
Montante
1
2
3
4
5
6
7
Chave
Valor Inicial
Direitos de reprodução reservados a Prof. Rafael Timóteo de Sousa Jr.


ALGORITMOS/CIFRADORES DE BLOCO
Valor Inicial
Chave
Banco
Depositante
Conta
Montante
Direitos de reprodução reservados a Prof. Rafael Timóteo de Sousa Jr.

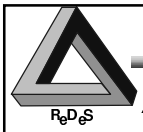
ALGORITMOS/CIFRADORES DE BLOCO



ALGORITMOS/CIFRADORES DE BLOCO

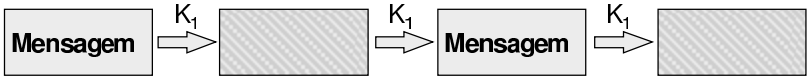


- Cifragem em blocos, usualmente de 64-bit
- Cifragem de blocos em cadeia (CBC) bastante comum
- Em geral, mais lenta que a cifragem em cadeia, porém mais fácil de realizar por software

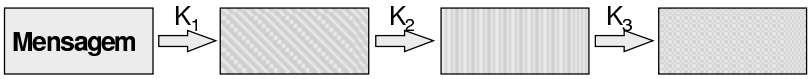


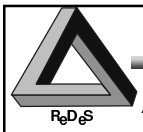
ALGORITMOS/TRIPLO-DES

- Triplo-DES usando apenas uma chave K_1
  - = DES



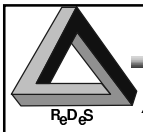
- Triplo-DES usando três chaves K_1, K_2, K_3
  - = DES com chave de 168-bits





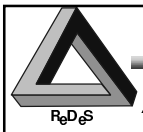
ALGORITMOS/CIFRADORES DE CADEIA SIMÉTRICOS

- RC4
  - Cifrador de cadeia de bytes (byte stream)
  - Operação XOR aplicada entre uma seqüência pseudo-randômica chaveada e os dados: a mesma para cifrar e decifrar
  - Tamanho da chave variável: até 2048 bits
  - Propriedade da RSA, esportável
  - Tamanho do código = 1/10 de DES
  - Velocidade = de 40 a 100 vezes DES



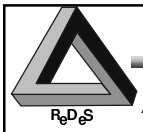
ALGORITMOS - CRIPTOGRAFIA TRADICIONAL

- Vantagens
  - Relativamente Segura
  - Amplamente utilizada
  - Rápida
- Desvantagens
  - Requer compartilhamento da chave secreta
  - Chaves **devem** guardadas com segurança
  - Grande número de chaves
  - Administração complexa
  - Não permite a não-repudiação



ALGORITMOS - TROCA DE CHAVE Diffie-Hellman

- Problema comum a DES, RC2, RC4: acordo prévio entre emissor e receptor quanto à chave de criptografia
- Algoritmo Diffie-Hellman
  - permite aos dois lados derivar uma chave sem necessidade de trocar nenhuma informação secreta
  - tem base na dificuldade de calcular logaritmos discretos
  - troca de chave simétrica
  - vulnerabilidade *man-in-the-middle*
- Troca de chave através de um canal não-seguro
  - Confidencialidade garantida
  - Autentificação não garantida



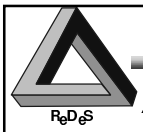
ALGORITMOS - TROCA DE CHAVE Diffie-Hellman

	A		B
1.	p,g	→	p,g

p = número primo, g = base do logaritmo

2. $y_1=g^{x1} \bmod p$ $\quad y_2=g^{x2} \bmod p$

x_1 = valor privado da 1a. parte
x_2 = valor privado da 2a. parte



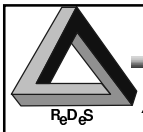
ALGORITMOS - TROCA DE CHAVE Diffie-Hellman

	A		B
1.	p,g	→	p,g
2.	$y_1=g^{x1} \bmod p$		$y_2=g^{x2} \bmod p$
3.	y_2	← →	y_1

y_1 = valor público da 1a. parte
y_2 = valor público da 2a. parte

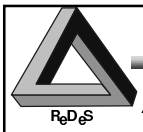
4. $z=y_2^{x1} \bmod p$ $\quad z=y_1^{x2} \bmod p$

z = chave secreta



ALGORITMO/CIFRADOR COM CHAVE PÚBLICA - RSA

- Bases matemáticas
  - dificuldade de fatorar o produto de dois números primos
  - inversibilidade da exponenciação em módulo, se usados determinados pares de números primos como expoentes
- Chave pública e chave privada
- Velocidade: 100 vezes mais lento que DES



ALGORITMO/CIFRADOR COM CHAVE PÚBLICA - RSA

- Base Matemática
  - Encontrar 2 fatores primos do número 77
  - Encontrar 2 fatores primos do número

    34.812.398.461.263.861.234.861.324.986.123.846.

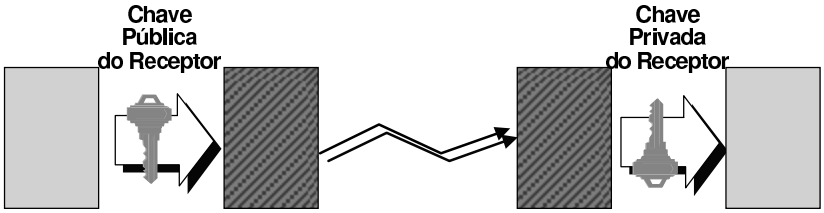
    198.234.674.365.874.223.487.129.867.356.512.390.

    348.723.487.231.785.345.987.234.586.234.230.476.

    897.234.634.598.734.587.987.235.879.823.458.789.

    234.589.789.342.683
  - Tempo de fatoração de um simples módulo de 200 dígitos RSA é maior que70,000,000 MIPS-years
  - Mesmo nas máquinas mais rápidas, a vantagem é sempre do cifrador, pois chaves maiores podem ser usadas com maior eficiência do que a dos métodos de fatoração

ALGORITMO/CIFRADOR COM CHAVE PÚBLICA - RSA



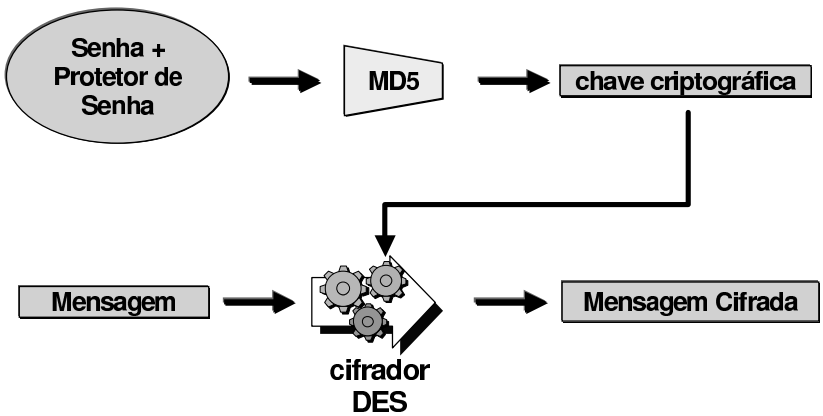
ALGORITMO/CIFRADOR COM CHAVE PÚBLICA - RSA

- Chave pública
  - n produto de dois números primos, p and q
  - e primo relativo de (p-1) x (q-1)
- Chave privada
  - $n = p \times q$
  - $d = e^{-1} (\text{mod } (p\text{-}1) \times (q\text{-}1))$
- Cifragem (usando a chave pública)
  - $c = m^e (\text{mod } n)$
  - e vale tipicamente 65536 (2^{16})
- Decifragem (usando a chave privada)
  - $m = c^d (\text{mod } n)$
  - d vale de 2^{510} a 2^{512} para módulo de 512-bits
  - Operação mais demorada que a cifragem

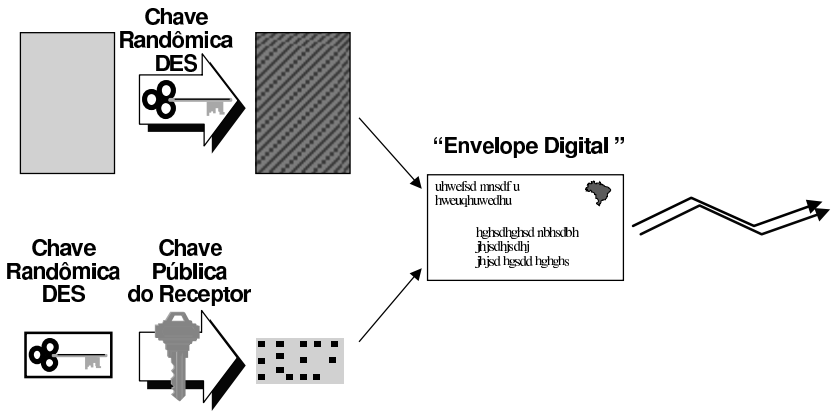
ALGORITMOS - DIGESTORES DE MENSAGENS

- Mensagem de entrada arbitrária
- Tamanho fixo de saída do digestor
- Irreversível
- Exemplos: MD2, MD5 da RSA Labs, ambos gerando mensagens digeridas de 128-bits

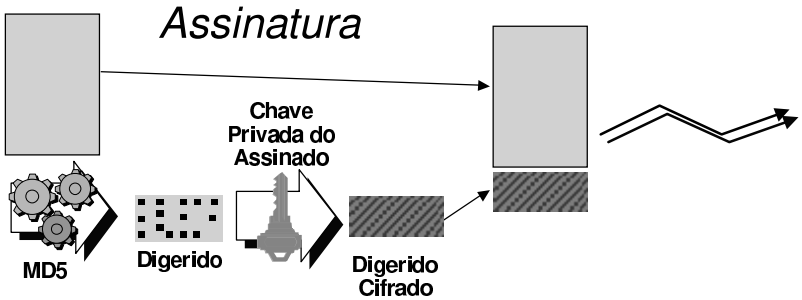
PROTOCOLOS - CPTOGRAFIA BASEADA EM SENHA



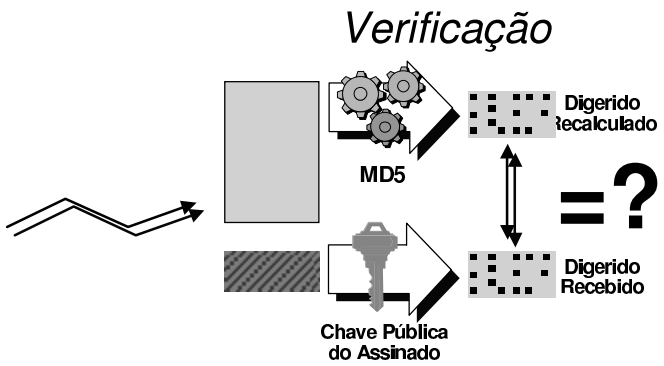
PROTOCOLOS - PRIVACIDADE - ENVELOPE DIGITAL



PROTOCOLOS - AUTENTIF. - ASSINATURA DIGITAL



PROTOCOLOS - AUTENTIF. - ASSINATURA DIGITAL



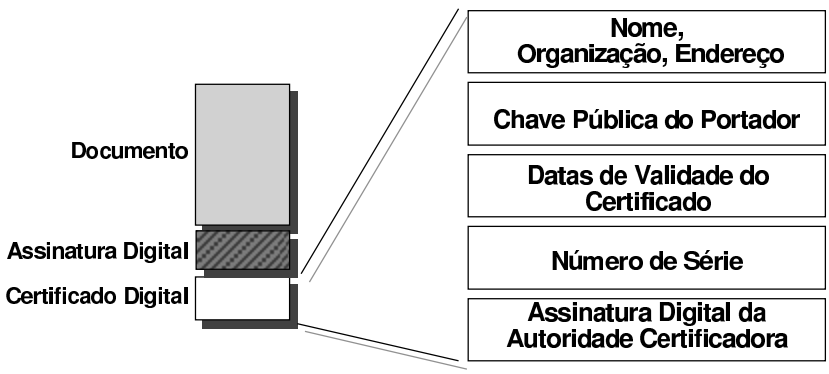
PROTOCOLOS - GERÊNCIA DE CHAVES

- Chaves privadas
  - Muito grandes, não permitem memorização
  - Necessidade de proteção para mantê-las privadas
- Chaves Públicas
  - Devem ser amplamente divulgadas
  - Conveniente ligá-las a um nome
- Dilema da incerteza sobre identidade do dono de uma chave
  - Qualquer um pode gerar um par de chaves pública/privada
  - Qualquer um pode dar um nome a uma chave pública
  - Qualquer um pode divulgar uma chave pública em um diretório público
  - Dilema: Como saber *com certeza* que o nome em uma chave pública representa realmente o receptor com quem se quer comunicar?
  - Solução: Certificados Digitais

PROTOCOLOS - CERTIFICADOS DIGITAIS

- Características
  - Como uma carteira de identidade eletrônica, um Certificado Digital assegura que alguma autoridade fez checagens razoáveis da identidade do portador
  - Um Certificado Digital notariza a ligação entre uma chave pública e um Emissor, assim como o R.G. prova a identidade de alguém

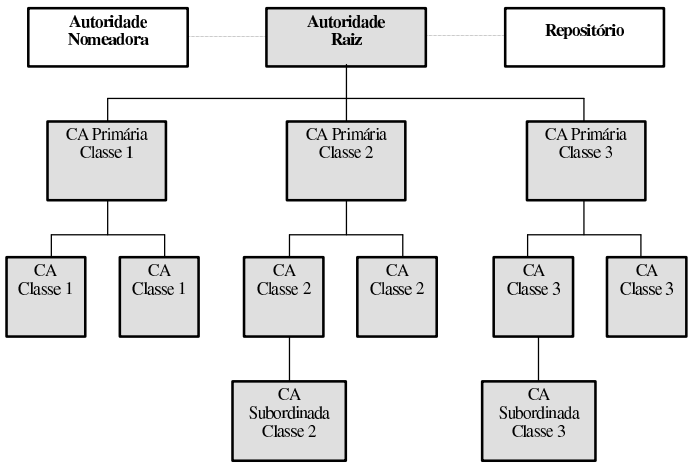
PROTOCOLOS - CERTIFICADOS DIGITAIS

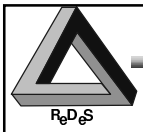


PROTOCOLOS - AUTORIDADES CERTIFICADORAS

- São o equivalente eletrônico dos cartórios (notários): "terceira parte confiável"
- Emitem, autenticam e gerenciam certificados digitais
- Serviço contínuo, confiável, operando 24 horas por dia, 7 dias por semana, e acessíveis globalmente pelos clientes
- Recursos tecnológicos
  - protocolos e padrões de segurança
  - sistema de mensagens seguro
  - infraestrutura adequada: instalações seguras, banco de dados, *home-page*
  - serviço de suporte ao cliente
- Conjunto de *práticas*:
  - normas e procedimentos de utilização dos serviços pelos clientes
  - resolução de disputas

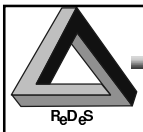
PROTOCOLOS - AUTORIDADES CERTIFICADORAS





SEGURANÇA LÓGICA - CONTROLE DE ACESSO

- permite às entidades da rede ter acesso seletivo aos recursos da mesma
- pedidos de acesso controlados e tentativas não autorizadas gravadas em livros de registro (log)
- esquemas:
  - proteção de acesso entre dispositivos
  - autentificação de usuários
  - proteção de arquivos e dados
  - autorização para uso de aplicações distribuídas



SEGURANÇA LÓGICA - CONTROLE DE ACESSO

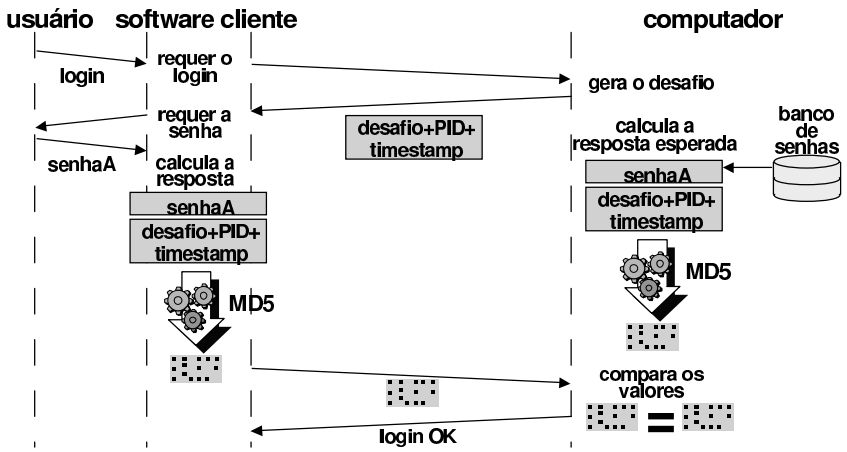
- Métodos de controle de acesso entre equipamentos
  - proteção de portas: modem com *call-back*, modem silencioso, PABX ativo
  - autentificação de nós de rede
- Métodos de controle de acesso para usuários
  - acesso livre
  - utilização de um par <identificação, senha> e controle da lista de usuários, procedimentos de seleção de senhas
  - autenticação mútua
  - senhas descartáveis ou autenticação por pergunta-resposta
  - senha com dispositivo passivo
  - senha com dispositivo ativo
  - dispositivo biométrico

CONTROLE DE ACESSO - AUTENTIF. DE USUÁRIOS

- Senhas estáticas
  - o usuário dispõe de um nome de conta e de uma senha secreta
  - senha criptografada guardada em um banco de senhas no computador
  - algoritmo de criptografia em UNIX: versão modificada de DES
  - problemas:
    - escolher uma senha adequada
    - manter a senha secreta
  - software CRACK - ftp://info.cert.org/pub/tools/crack/
    - tenta adivinhar senhas guardadas no arqivo /etc/passwd
    - usa dicionário de senhas e combinações típicas
    - avisa ao administrador e opcionalmente ao usuário sobre senhas ruins
  - software NPASSWD - ftp://ftp.cc.utexas.edu/pub/npasswd/
    - bloqueia senhas ruins no momento em que o usuário as escolhe
    - usa dicionário e verifica regras de formação
  - proteção do arquivo de senhas e verificação da idade das senhas
  - uso de protocolo criptográfico na escolha e comunicação de senhas

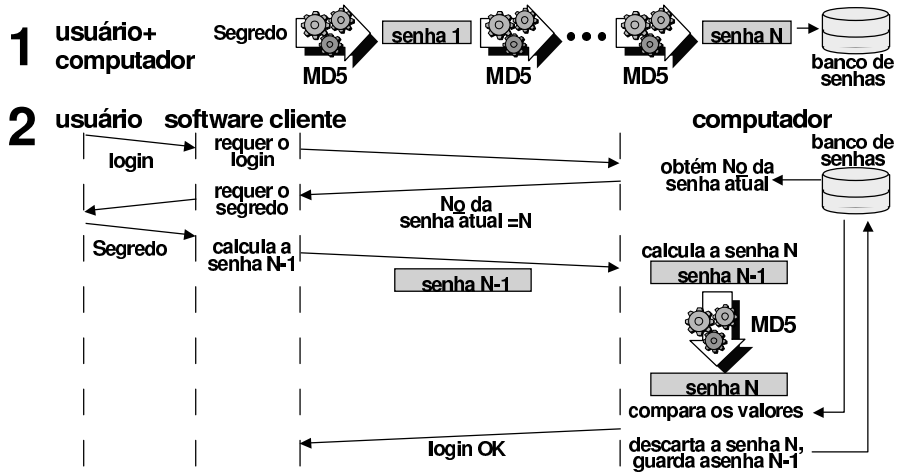
CONTROLE DE ACESSO - AUTENTIF. DE USUÁRIOS

- esquema desafio-resposta

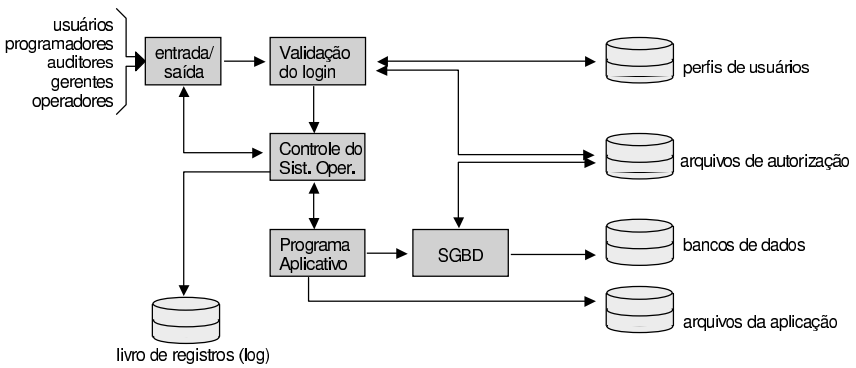


CONTROLE DE ACESSO - AUTENTIF. DE USUÁRIOS

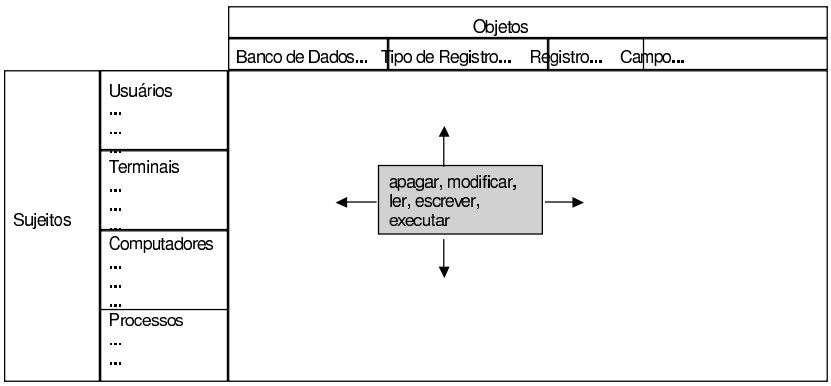
- esquema senha descartável S/KEY - RFC 1760



CONTROLE DE ACESSO AOS DADOS

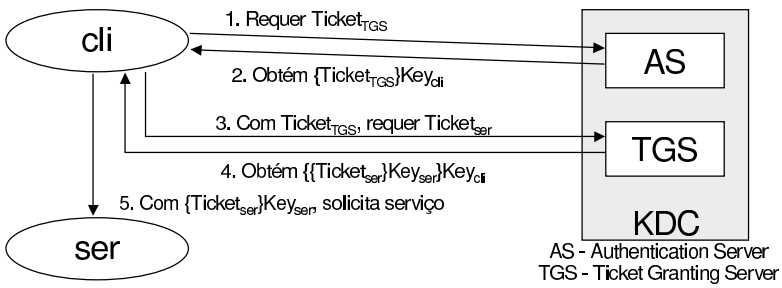


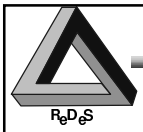
CONTROLE DE ACESSO AOS DADOS



CONTROLE DE ACESSO-APLICAÇÕES DISTRIBUÍDAS

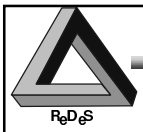
- Kerberos - ftp://athena-dist.mit.edu/pub/kerberos/
  - usa DES e MD5
  - aplicações e servidores precisam ser "kerberizados"
  - usuários, aplicações e servidores compartilham chaves criptográficas com um centro distribuidor de chaves (KDC)
  - através do KDC, um participante autentifica-se junto a qualquer outro





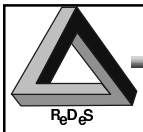
SEGURANÇA LÓGICA - SEGURANÇA MULTINÍVEL

- Aplicável a pessoas, programas, dados, sistemas operacionais, mensagens
- Conceitos básicos
  - objetos: memória, arquivos, processos em execução na memória, diretórios, dispositivos de hardware, estruturas de dados, instruções, senhas, canais de comunicação
  - usuários: pessoas, programas, dispositivos de hardware, sistemas
  - sensibilidade: grau de proteção desejado para um objeto
  - credencial: grau de permissão dado aos usuários para usar objetos



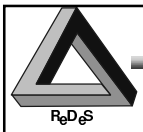
SEGURANÇA LÓGICA - SEGURANÇA MULTINÍVEL

- categorização da sensibilidade dos objetos
  - público < confidencial < secreto < supersecreto
  - público < pessoalbase < pessoalgerência < pessoaldireção
- compartimentalização dos objetos
  - arquivos: vendas, empregados, contabilidade...
  - canais: locais, remotosinternos, remotosexternos...



SEGURANÇA LÓGICA - SEGURANÇA MULTINÍVEL

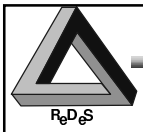
- Procedimentos:
  - **classe de um objeto** dada pela combinação <sensibilidade, compartimentos>
  - **credencial de um usuário** dada pela combinação <sensibilidade, compartimentos>
  - **regra necessidade-de-uso**: acesso a objetos sensíveis permitido apenas para usuários que precisam deles para trabalhar
  - **regra do privilégio mínimo**: um usuário deve ter acesso apenas ao menor número de objetos que lhe permitam trabalhar com sucesso



SEGURANÇA LÓGICA - SEGURANÇA MULTINÍVEL

- regra formal: um usuário (U) pode acessar um objeto (O) somente se:
  - a credencial do usuário tem sensibilidade pelo menos tão alta quanto a sensibilidade do objeto
  - o usuário tem necessidade de uso de todos os compartimentos da classe do objeto
- expressão matemática verificável:

  O ≤ U se e somente se (
  sensibilidadeO ≤ sensibililidadeU
  e
  compartimentosO ⊆ compartimentosU)



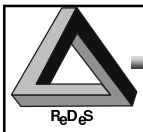
SEGURANÇA LÓGICA - SEGURANÇA MULTINÍVEL

- Exemplo
  - arquivos - sensibilidade: público < confidencial < secreto < supersecreto

    relatório anual <público, -->
    balanço mensal <confidencial, contabilidade>
    plano quinquenal <secreto, vendas, empregados, contabilidade>
    caixa2 <supersecreto, contabilidade>
  - usuários - credenciais:

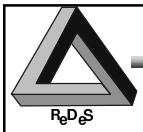
    João Folha (jornalista) <público, -->
    José Soma (auxiliar escrit.) <confidencial, contabilidade>
    Pedro Cofre (diretor financ.) <supersecreto, vendas, contabilidade>
    Paulo Rico (presidente) <supersecreto, vendas, empregados, contabilidade>
  - direitos de acesso:

    João Folha relatório anual
    José Soma relatório anual, balanço mensal
    Pedro Cofre relatório anual, balanço mensal, caixa2 (plano quinquenal não !?)
    Paulo Rico todos os arquivos



SEGURANÇA LÓGICA - SEGURANÇA MULTINÍVEL

- Reforços complementares
  - operações permitidas dos usuários sobre os objetos:
    - *read, write, execute*
    - *iniciate, suspend, resume, terminate*
    - *create, modify, destroy*
  - restrições de contexto, tempo, seqüência
  - restrições de fluxo de informações



SEGURANÇA DE PROGRAMAS

Ameaças e Vulnerabilidades

Ligadas ao acesso às informações
- alçapão
- cavalo de Troia
- ataque salame
- vazamentos

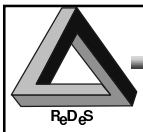
Ligadas ao serviço do sistema
- programas gulosos
- programas com iterações infinitas
- virus
- vermes

Controles e Proteções

No desenvolvimento (prevenção)
- revisões cruzadas
- modularidade, encapsulamento, ocultação
- teste independente
- gerência de configuração

Na operação (limitação de danos)
- programas verificados
- suspeita mútua
- confinamento
- histórico de acessos

Controles administrativos
- padrões de desenvolvimento
- separação de responsabilidades
- mecanismos de contratação
- monitoração de empregados



SEGURANÇA DE SISTEMAS OPERACIONAIS

Ameaças e Vulnerabilidades

Mesmas dos Programas e também...

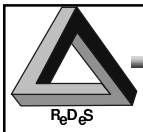
Efeitos de um usuário sobre outro

Interações entre usuários

Controles e Proteções

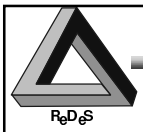
Na concepção do sistema
- modelo de segurança e mecanismos
- verificação
- métodos de implementação

Na operação/interação com usuários
- proteção da memória
- proteção dos arquivos
- controle de acesso a objetos e recursos
- autentificação dos usuários



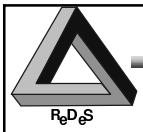
SEGURANÇA DE COMPUTADORES PESSOAIS

Ameaças e Vulnerabilidades	Controles e Proteções
Mesmas dos Programas e Sistemas Operacionais e também... Desinteresse/insensibilidade aos problemas Ferramentas inapropriadas ou inexistentes	• proteção do equipamento • *backup* e proteção dos meios magnéticos • controles dos softwares • proteção dos arquivos • proteção contra cópia • mecanismos de distribuição de software



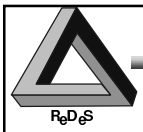
SEGURANÇA EM BANCOS DE DADOS

Ameaças e Vulnerabilidades	Controles e Proteções
Ameaças ligadas aos usuários: • erros de coleta, manipulação, digitação... • entrada de valores aceitáveis mas incorretos • operações conflitantes ou fora de sequência • Duplicações • Tentativas de acesso não autorizado Ameaças à informação sensível: • revelação parcial • ataque por inferência Bloqueio/Negação de informações devido a controles de segurança	Controles de Sistema Operacional e procedimentos de retomada Controles de correção de elementos Controles de integridade e de consistência de elementos e da estrutura do BD Controles de sensibilidade de Dados Controles contra inferência Proteção multi-nível



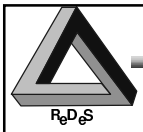
BD - EXIGÊNCIAS DE SEGURANÇA

- Integridade:
  - Física: os dados do BD devem ser imunes a problemas de falta de energia, paradas do sistema operacional...
  - Estrutural ou lógica: preservação da estrutura e coerência interna do BD
  - Elementar: os dados contidos em todos os elementos (registros, campos, relações...) devem ser confiáveis
- Confidencialidade:
  - Auditoria: rastreamento de quem fez acesso/modificou elementos do BD
  - Controle de acesso: o usuário só deve ter acesso a dados para os quais tem autorização
  - Autenticação: todo usuário tem que ser identificado corretamente para permitir o controle de acesso e os procedimentos de auditoria
- Disponibilidade:
  - Os usuários têm acesso ao BD e a todos os dados para os quais têm autorização



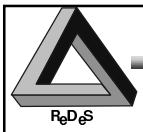
BD - AMEAÇAS À SEGURANÇA

- Acontecimentos externos:
  - Fogo, falta de energia, acidentes com discos
  - Problema no sistema operacional
- Ameaças ligadas aos usuários:
  - Usuários cometem erros de coleta, manipulação, digitação...
  - Entrada de valores aceitáveis mas incorretos
  - Operações conflitantes ou fora de sequência
  - Duplicações
  - Tentativas de acesso não autorizado
- Ameaças à informação sensível:
  - revelação parcial
  - ataque por inferência
- Bloqueio/Negação de informações devido a controles de segurança



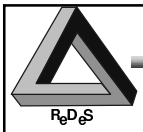
BD - CONTROLES DE SEGURANÇA

- Controles de Sistema Operacional e procedimentos de retomada
- Controles de correção de elementos
- Controles de integridade e de consistência de elementos e da estrutura do BD
- Controles de sensibilidade de Dados
- Controles contra inferência
- Proteção multi-nível



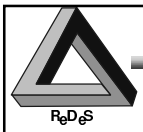
BD - CONTROLES DE SEGURANÇA

- Controles de Sistema Operacional e Procedimentos de Retomada
  - proteção de arquivos, verificação de entradas e saídas
  - back-up periódico
  - registro de transações (transaction log) e procedimento de recuperação após erro
- Controles de correção de elementos
  - verificação de tipos de dados, verificação de domínio de valores
  - controles de acesso: conflitos, sequenciamentos, duplicações, autorizações
  - registro de modificações (change log), procedimento "desfazer"



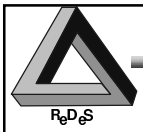
BD - CONTROLES DE SEGURANÇA

- Controles de integridade e de consistência de elementos e da estrutura do BD
  - procedimento de atualização em duas fases: intenção-efetivação (intent-commit)
  - redundâncias: códigos de detecção e correção de erros, campos duplicados (shadow fields)
  - registro de modificações (change log), procedimento "refazer"
  - reserva (locking), atomicidade do ciclo "busca e modificação" (query-update)
  - verificação de relações entre domínios de campos
  - restrições de estado: classificações, número de elementos de classe
  - restrições de transição



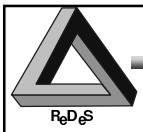
BD - CONTROLES DE SEGURANÇA

- Controles de Sensibilidade de Dados
  - decisão de acesso: disponibilidade dos dados, aceitação de acesso, autenticidade dos usários
  - controles contra revelação parcial: controle de precisão, de limites, de resultados negativos em buscas, de existência, do valor provável...
  - histórico de acessos e rastreamento de informações entregues aos usuários, análise de questões, filtragem...



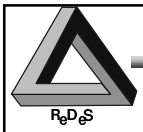
BD - CONTROLES DE SEGURANÇA

- Controles contra Inferência
  - controle contra o ataque direto disfarçado
  - controle contra ataques indiretos através de somas, contagem de elementos, médias, rastreamento...
  - supressão de respostas
  - disfarce dos resultado: combinação de resultados, amostragem randômica, pertubação da precisão dos dados
  - histórico de acessos e rastreamento de informações entregues aos usuários, análise de questões, filtragem...



BD - CONTROLES DE SEGURANÇA

- Proteção Multinível
  - acesso e utilização de elementos em função de direitos de acesso
    - sensibilidade do elemento: vários níveis de sensibilidade de elementos, de agregados, de relações...
    - direitos de acesso de usuários: necessidades específicas, sub-conjuntos, visões do BD...
  - particionamento do BD
  - criptografia e ferrolho de integridade
  - visões do BD: sub-conjuntos do BD que contêm exatamente a informação para a qual o usuário tem autorização de acesso
  - frontal confiável, filtro comutativo
    - só o frontal interage com o usuário
    - tem a possibilidade de alterar as buscas e questões
    - repassa ao SGBD somente operações autorizadas
    - recebe os resultados do SGBD, verifica a validade dos dados e restringe a divulgação em função de direitos de acesso do usuário



SEGURANÇA EM REDES

Ameaças e Vulnerabilidades

Escuta do meio

Análise do tráfego

Disfarce

Repetição

Modificação ou destruição de mensagens

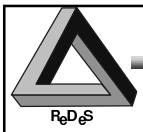
Geração de tráfego não autorizado

Controles e Proteções

Serviços de segurança
- autenticação de entidades e origem dos dados
- o controle de acesso aos recursos da rede
- a confidencialidade dos dados
- a integridade dos dados
- a não rejeição ou não repudiação

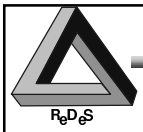
Mecanismos de segurança
- criptografia
- assinatura numérica
- mecanismo de controle de acesso
- mecanismo de integridade dos dados
- troca de autenticação
- tráfego de desnorteamento
- controle de roteamento e barreiras (firewalls)
- notarização
- mecanismos genéricos

Gerência da segurança



SEGURANÇA EM REDES

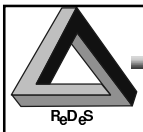
- Exigências de segurança específicas do emissor
  - que a mensagem chegue somente ao destinatário escolhido e não a um outro
  - que a mensagem não será modificada durante a tranferência
  - que a mensagem será conhecida apenas pelo destinatário escolhido
  - que o destinatário não poderá negar ter recebido uma mensagem que foi efetivamente entregue. O conteúdo da mensagem também não deve ser negado
  - que ninguém o acuse de ter enviado uma mensagem que na realidade ele não enviou



SEGURANÇA EM REDES

- Exigências de segurança específicas do receptor
  - que a mensagem provém realmente do emissor declarado
  - que a mensagem não foi modificada durante a transferência
  - que o emissor não possa negar ter enviado uma mensagem efetivamente enviada e recebida, inclusive no que se refere a seu conteúdo
  - de que ninguém o acuse de ter recebido uma mensagem que em verdade não recebeu

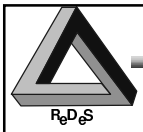
- Exigências de segurança comuns ao emissor e ao receptor
  - que ninguém tenha conhecimento de que estão tendo um diálogo
  - que o meio de comunicação não seja sabotado



SEGURANÇA EM REDES

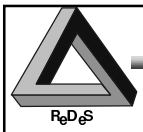
- Ameaças passivas
  - visam a divulgação não autorizada de informações, como o conteúdo das mensagens e mesmo a existência de diálogo entre emissor e receptor
  - escuta do meio
  - análise do tráfego

- Ameaças ativas
  - objetivam modificar ou destruir sem autorização as informações ou tornar indisponíveis serviços para os usuários
  - disfarce: o atacante imita um usuário autorizado para ter acesso e até atacar outros elementos do sistema (arquivos, bancos de dados, sistemas operacionais...)
  - repetição: o atacante grava uma sequência de mensagens para repetí-la em outra ocasião
  - a modificação ou a destruição de mensagens
  - geração de tráfego não autorizado (por exemplo: vermes)



SEGURANÇA - REDES OSI

- Organização das proteções com base nos conceitos de arquitetura e gerência da segurança
- Arquitetura da Segurança
  - serviços e Mecanismos de segurança no contexto OSI
  - serviços de segurança integrados nas camadas OSI
  - mecanismos de prevenção, detecção e reação a ameaças e ataques
  - posição dos Serviços e Mecanismos no Modelo OSI
- Gerência da Segurança
  - 1 das 5 áreas de gerência de rede OSI
  - controle dos serviços de segurança
  - controle das informações e mecanismos relativos ao fornecimento dos serviços de segurança
  - operação dos serviços e mecanismos de segurança, detecção de eventos e registro para auditoria



SEGURANÇA - REDES OSI - ARQUITETURA 7498-2

- Cinco serviços de segurança
  - autenticação tanto de entidades pares quanto da origem dos dados (authentication),
  - controle de acesso aos recursos da rede (access control),
  - confidencialidade dos dados (confidenciality),
  - integridade dos dados (integrity),
  - não rejeição ou não repudiação (non-repudiation)

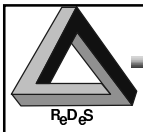
SEGURANÇA - REDES OSI - ARQUITETURA 7498-2

- Posição dos Serviços de Segurança nas Camadas OSI
  - leva em conta a estrutura de camadas do modelo OSI
  - respeita as necessidades de otimizar as diferentes maneiras de garantir a segurança
  - evita sobreposições
  - garante o rigor dos serviços sem comprometer a independência entre as camadas

SEGURANÇA - REDES OSI - ARQUITETURA 7498-2

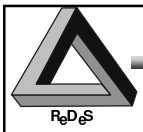
- Posição dos Serviços de Segurança nas Camadas:

	CAMADAS						
SERVIÇOS	1	2	3	4	5	6	7
Autenticação da entidade par			X	X			X
Autenticação da origem dos dados			X	X			X
Controle de acesso			X	X			X
Confidencialidade em modo conectado	X	X	X	X		X	X
Confidencialidade em modo não conectado		X	X	X		X	X
Confidencialidade seletiva de um campo de protocolo						X	X
Confidencialidade do fluxo de informação	X		X				X
Integridade em modo conectado com recuperação				X			X
Integridade em modo conectado sem recuperação			X	X			X
Integridade seletiva de um campo							X
Integridade em modo não conectado			X	X			X
Integridade seletiva em modo não conectado							X
Não rejeição com prova da origem							X
Não rejeição com prova da entrega							X



SEGURANÇA - REDES OSI - ARQUITETURA 7498-2

- Mecanismos de segurança específicos:
  - criptografia
  - assinatura numérica
  - mecanismo de controle de acesso
  - mecanismo de integridade dos dados
  - troca de autenticação
  - inserção de tráfego
  - controle de roteamento
  - notarização
- Mecanismos de segurança genéricos
  - funcionalidades confiáveis/segurança multinível
  - rótulo de segurança
  - detecção de eventos relevantes para a segurança e registro para auditoria de segurança
  - ações de restabelecimento da segurança

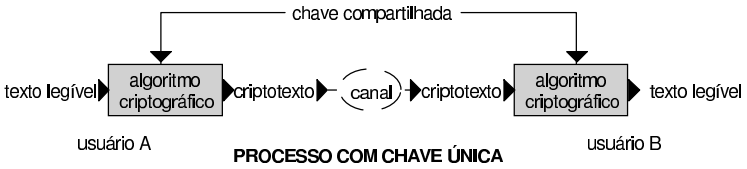


SEGURANÇA OSI - MECANISMOS ESPECÍFICOS

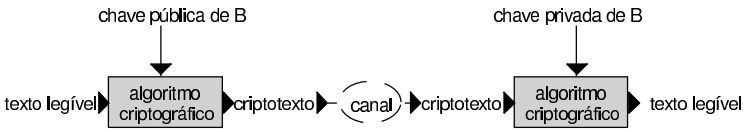
- Criptografia:
  - mecanismo de base utilizado em quase todos os serviços de segurança
    - autenticação
    - integridade
    - confidencialidade
  - dois tipos de processos criptográficos:
    - com chave secreta única compartilhada entre emissor e receptor
    - com 2 chaves: uma pública, uma privada

SEGURANÇA OSI - MECANISMOS ESPECÍFICOS

- Criptografia:



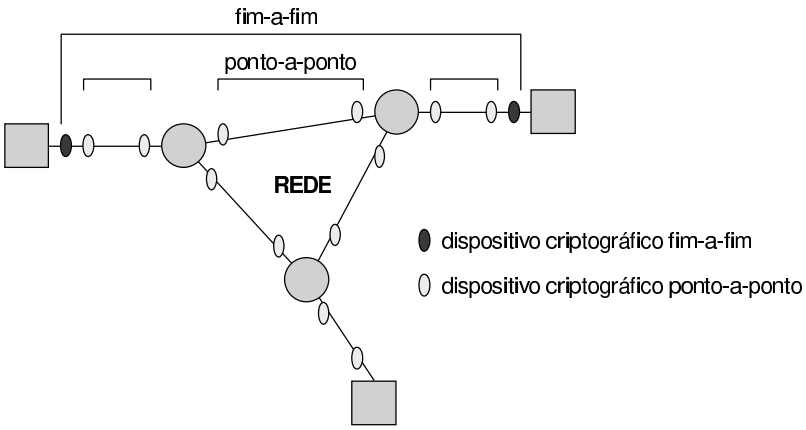
PROCESSO COM CHAVE ÚNICA

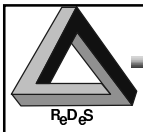


PROCESSO COM CHAVES PÚBLICA E PRIVADA

SEGURANÇA OSI - MECANISMOS ESPECÍFICOS

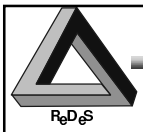
- Criptografia:





SEGURANÇA OSI - MECANISMOS ESPECÍFICOS

Criptografia ponto-a-ponto	Criptografia fim-a-fim
• mensagem exposta no emissor e nos nós de rede intermediários	• mensagem cifrada no emissor e nos nós de rede intermediários
• realizada pelo computador emissor • transparente para o usuário • algoritmo pertencente ao computador • um só algoritmo para todos os usuários • pode ser feita em *hardware* • todas ou nenhuma mensagem cifrada	• realizada pelo processo emissor • o usuário realiza a cifragem • o usuário define o algoritmo • um algoritmo para cada usuário • implementada em *software* • o usuário define as mensagens a cifrar
• uma chave ou par de chaves para cada par de nós • provê autentificaçào entre nós	• uma chave ou par de chaves para cada par de usuários • provê autentificaçào de usuários



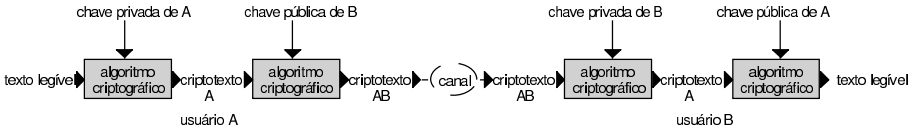
SEGURANÇA OSI - MECANISMOS ESPECÍFICOS

- Assinatura numérica:
  - o uso da criptografia permite colocar, de modo protegido, a assinatura do emissor em cada unidade de dados dos protocolos (PDU) OSI
  - o receptor tem a possibilidade de verificar a autenticidade dessa assinatura
  - isso serve para colocar em prática os serviços de autenticação, alguns serviços de integridade e constitui parte dos serviços de não rejeição
  - esquemas:
    - simples, provendo autenticação
    - duplo, provendo autenticação e confidencialidade
    - com arbitragem, provendo notarização

SEGURANÇA OSI - MECANISMOS ESPECÍFICOS

- Assinatura numérica:

ASSINATURA DIGITAL PROVENDO AUTENTICAÇÃO



ASSINATURA DIGITAL PROVENDO AUTENTICAÇÃO E CONFIDENCIALIDADE

SEGURANÇA OSI - MECANISMOS ESPECÍFICOS

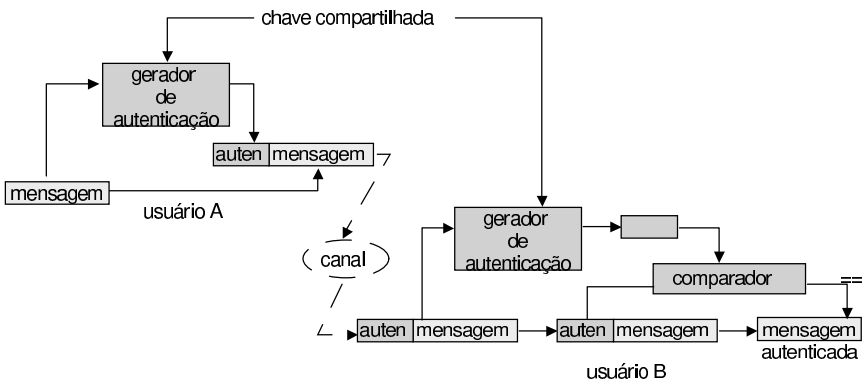
- Mecanismo de controle de acesso:
  - permite às entidades da rede ter acesso seletivo aos recursos da mesma
  - todo pedido de acesso é controlado e tentativas não autorizadas são gravadas em um livro de registro (log)
  - usado somente em serviços de controle de acesso

SEGURANÇA OSI - MECANISMOS ESPECÍFICOS

- Mecanismo de integridade dos dados:
  - o emissor adiciona a uma PDU uma informação de controle, calculada sobre os dados da própria PDU e criptografada
  - o receptor recalcula a informação de controle a partir da PDU recebida: a comparação do valor recebido com o valor recalculado permite verificar se houve alteração das informações durante o transporte
  - usado em serviços de integridade e de não rejeição
- Troca de autenticação:
  - garantida da identificação de uma entidade através da troca de informações
  - serve para a autenticação de entidades pares
- Autenticação de mensagens - verificações:
  - que o conteúdo das mensagens não foi alterado
  - que o emissor é autêntico
  - que a mensagem não está caduca
  - que a mensagem está na seqüência correta

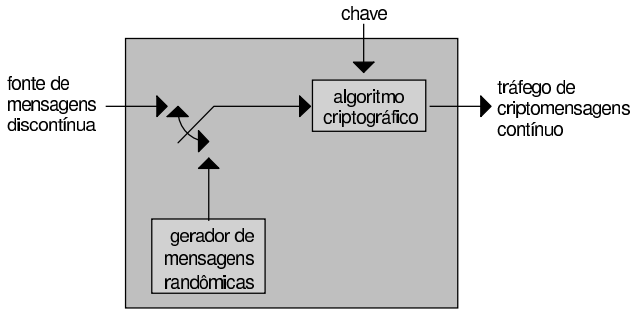
SEGURANÇA OSI - MECANISMOS ESPECÍFICOS

- Mecanismos de integridade dos dados e troca de autenticação: autenticação de mensagens



SEGURANÇA OSI - MECANISMOS ESPECÍFICOS

- Inserção de Tráfego:
  - tráfego gerado para despistar ou desnortear intrusos e observadores não autorizados
  - serve para garantir a confidencialidade



SEGURANÇA OSI - MECANISMOS ESPECÍFICOS

- Controle de roteamento
  - permite que uma rota preferencial seja utilizada numa comunicação, de modo a evitar a circulação de informações em sub-redes inseguras ou desprotegidas
  - permite obrigar a passagem das mensagens por um nó específico
  - permite modificar periodicamente as rotas das mensagens
  - serve para garantir a confidencialidade

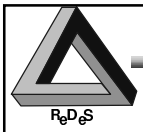
SEGURANÇA OSI - MECANISMOS ESPECÍFICOS

- Notarização
  - qualquer entidade de um sistema aberto pode fazer o registro de certos dados (por exemplo, o registro do envio de um determinado arquivo a uma entidade par) junto a uma terceira entidade confiável, chamada notário
  - o notário é capaz de garantir mais tarde a fidedignidade de características como conteúdo, origem, data e entrega referentes a tais dados ou à operações a eles associadas
  - serve para garantir a não rejeição

SEGURANÇA OSI - MECANISMOS ESPECÍFICOS

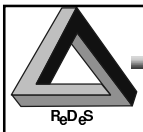
- Posição dos Mecanismos de Segurança nas Camadas:

	CAMADAS						
MECANISMOS	1	2	3	4	5	6	7
Criptografia	X	X	X	X		X	
Assinatura digital			X	X		X	X
Controle de acesso			X	X			X
Integridade dos dados			X	X		X	
Troca de autenticação			X	X			X
Inserção de tráfego			X				X
Controle de roteamento			X				
Notarização						X	X



SEGURANÇA OSI - MECANISMOS GENÉRICOS

- Mecanismos de segurança genéricos:
  - funcionalidades confiáveis:
    - segurança multi-nível: níveis de segurança atribuídos aos objetos do sistema e direitos de acesso atribuídos aos usuários
  - rótulo de segurança:
    - atribuído a cada recurso para designar seus atributos de segurança
  - detecção de eventos relevantes para a segurança e registro para auditoria de segurança
  - restabelecimento da segurança:
    - sob demanda de outros mecanismos, são efetuadas ações para restabelecer a segurança
    - aborto de operações
    - invalidação temporária de uma entidade
    - modificação de parâmetros da segurança
    - atualização de uma lista negra



SEGURANÇA - REDES OSI - ARQUITETURA 7498-2

- Aplicação dos Serviços e Mecanismos de Segurança
  - função da política de segurança adotada no sistema aberto
  - implementação da política de segurança:
    - informações sobre a segurança armazenadas na SMIB (Security Management Information Base)
    - distribuição das informações de segurança através de canais OSI ou não
    - operação dos serviços e mecanismos de segurança através de funções de Gerência da Segurança

SEGURANÇA - REDES OSI - GERÊNCIA 7498-4

- Funções básicas de suporte às atividades de Gerência da Segurança
  - controle de acesso aos objetos envolvidos com a gerência OSI (10164-9)
  - função de relatório de alarmas de segurança (10164-7)
  - função de registro para auditoria de segurança (10164-8)

- Objetivos principais da funções de Gerência da Segurança
  - alteração do modo de operação do sistema aberto, através da ativação e da desativação dos serviços de segurança
  - seleção dos parâmetros dos serviços de segurança
  - fornecimento de relatórios de eventos relativos à segurança e o fornecimento de informações estatísticas
  - manutenção e análise dos registros de histórico relativos à segurança

SEGURANÇA - REDES OSI - GERÊNCIA 7498-4

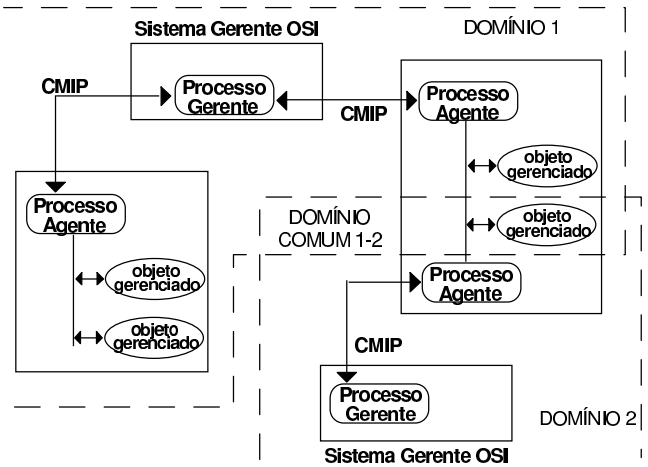
- Exigências básicas:
  - diferentes políticas de segurança podem ser adotadas nos sistemas abertos
  - domínio de segurança: entidades que obedecem a uma mesma política de segurança
  - distribuição das informações de gerência entre todas as entidades do domínio de segurança.
  - informações de segurança: chaves de criptografia, rotas preferenciais para certas informações...
  - proteção dos protocolos de gerência, assim como os canais de comunicação que conduzem as informações de gerência OSI

SEGURANÇA - REDES OSI - GERÊNCIA 7498-4

- Função de Controle de Acesso
  - Proteção do acesso a recursos de gerência: apenas usuários autorizados podem ter acesso a recursos de gerência, havendo níveis de acesso:
    - acesso para ler e escrever, apenas para ler ou nenhum acesso
    - acesso apenas para objetos específicos
    - proibição até do estabelecimento de comunicações para gerência
  - Notificações de gerência não devem ser enviadas para destinatários não autorizados
  - Entidades não autorizadas não devem ter acesso a operações de gerência
  - Proteção das informações de gerência contra divulgação indesejável
  - Dois tipos de controles de acesso:
    - Para associação de aplicações de gerência
    - Para operações de gerência

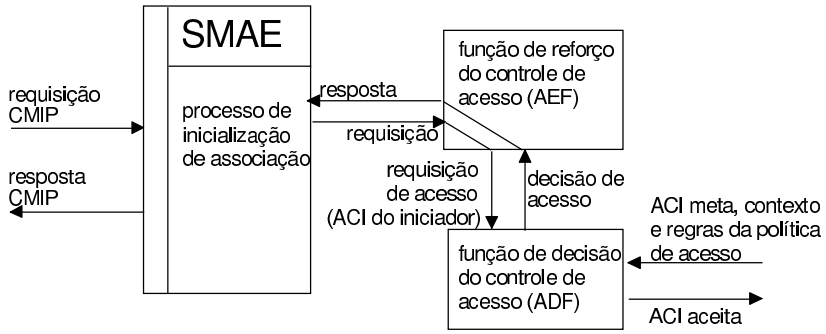
SEGURANÇA - REDES OSI - GERÊNCIA 7498-4

- Funções de Controle de Acesso:



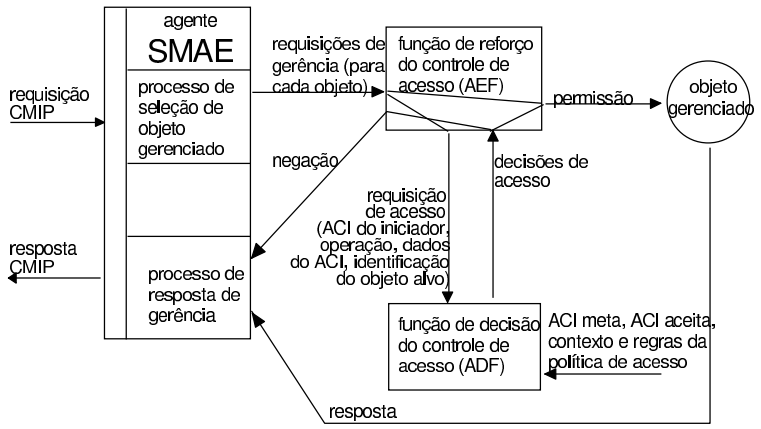
SEGURANÇA - REDES OSI - GERÊNCIA 7498-4

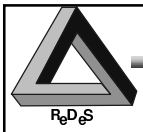
- Função de Controle de Acesso para Associação de Gerência:



SEGURANÇA - REDES OSI - GERÊNCIA 7498-4

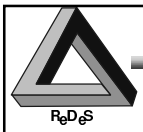
- Função de Controle de Acesso para Operações de Gerência:





SEGURANÇA - REDES OSI - GERÊNCIA 7498-4

- Função de Relatório de Alarmas de Segurança
  - veicula alarmas de segurança que são notificações de eventos relativos à segurança
  - eventos detectados por mecanismos de segurança ou processos correlacionados:
    - Operações errôneas nos serviços e mecanismos de segurança,
    - Atentados contra a segurança,
    - Violações da segurança.
  - o tipo, a causa e a gravidade desses eventos são informações entregues aos processos de gerência de rede, executados por seres humanos e entidades de gerência artificiais
  - classificação dos eventos quanto à gravidade: indeterminado, menor, crítico, maior



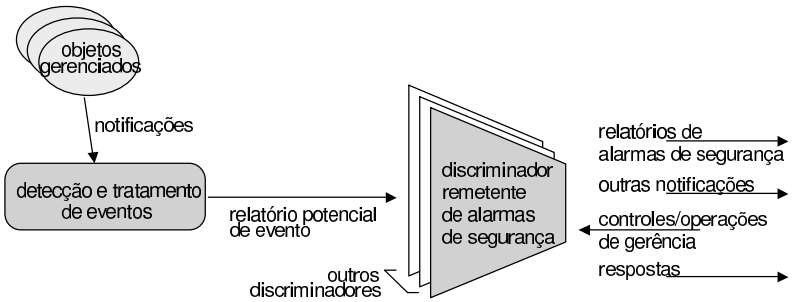
SEGURANÇA - REDES OSI - GERÊNCIA 7498-4

- Alarmas de Segurança - tipos e causas de eventos

Tipos	Causas
violação de integridade	informação duplicada perda de informação detecção de modificação de informação informação fora de sequência informação inesperada
violação operacional	serviço recusado fora de serviço erro de procedimento outra razão
violação física	intromissão nos cabos detecção de intrusão outra razão
violação de serviço ou mecanismo de segurança	falha de autenticação vacilo da confidencialidade tentativa de acesso não autorizado outra razão
violação no domínio do tempo	informação atrasada chave vencida atividade fora de hora

SEGURANÇA - REDES OSI - GERÊNCIA 7498-4

- Função de Relatório de Alarmas de Segurança



SEGURANÇA - REDES OSI - GERÊNCIA 7498-4

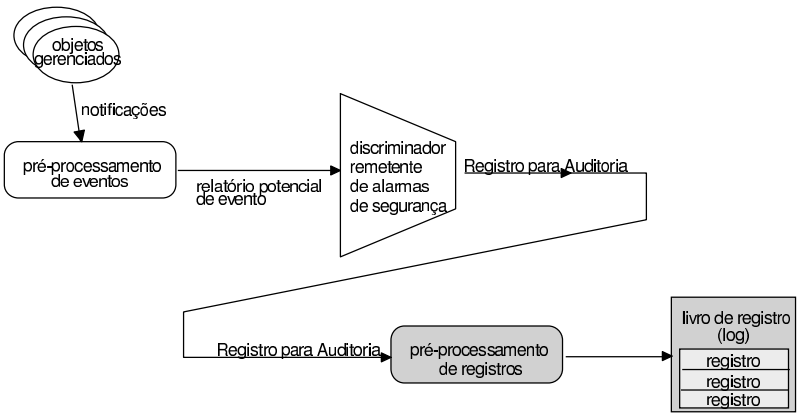
- Função de Registro para Auditoria de Segurança
  - Registro de eventos relativos à segurança
  - Permite comparar a utilização planejada para o sistema aberto com a sua utilização real
  - Avaliação do atendimento dos requisitos de segurança definidos pela política de segurança em vigor
  - Detecção de desvio com relação à política de segurança
  - Identificação de pontos vulneráveis ou maus funcionamentos relativos à segurança

SEGURANÇA - REDES OSI - GERÊNCIA 7498-4

- Função de Registro para Auditoria de Segurança:
  - Relatórios dos eventos que interessam para auditoria de segurança devem ser enviados ao Livro de Registro (log) situado no sistema aberto local ou num sistema remoto
  - Para enviar os relatórios de eventos a um sistema remoto, deve ser usado um discriminador de repasse de eventos no sistema local
    - seleciona os relatórios a serem enviados
    - determina o sistema aberto destinatário
  - Gravação no Livro de Registros (log)
    - um construtor de discriminador é associado ao log e captura os eventos determinados pela política de segurança vigente
  - Eventos gravados no registro de Auditoria
    - Conexões e Desconexões
    - Todo evento relativo à utilização de mecanismos de segurança
    - Operações de gerência de rede
    - Contabilização da utilização dos recursos gerenciados

SEGURANÇA - REDES OSI - GERÊNCIA 7498-4

- Função de Registro para Auditoria de Segurança:



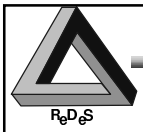
Direitos de reprodução reservados a Prof. Rafael Timóteo de Sousa Jr.

REDES OSI - SEGURANÇA DA GERÊNCIA DE REDE

- Segurança - item fundamental na gerência dos sistemas abertos
- segurança das funções de gerência do modelo OSI
- segurança da comunicação de informações de gerência OSI
- uma operação de gerência OSI é possível somente se a função de controle de acesso tiver sido acionada:
  - para autorizar os acessos a recursos de gerência
  - para autorizar operações sobre os objetos gerenciados envolvidos em tal operação.

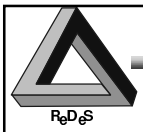
REDES OSI - SEGURANÇA DA GERÊNCIA DE REDE

- mecanismos e serviços da Arquitetura de Segurança, quando adequados, podem servir para qualquer processo ou atividade de gerência
  - emprego de meios e procedimentos de acordo com a política de segurança adotada
  - mecanismos como a criptografia e a assinatura numérica podem ser usados para garantir o segredo da informação de gerência ou a identidade de processos gerentes e agentes
  - a notarização das operações de gerência pode servir a verificações posteriores que permitam comprovar certos dados
  - diversas aplicações: gerência de contabilização, garantia de qualidade de serviços de rede...



REDES TCP/IP - MECANISMOS DE SEGURANÇA

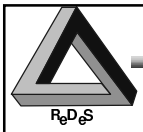
- diversos dispositivos e mecanismos para a proteção dos serviços
- tecnologias e mecanismos de proteção
  - dispositivos e equipamentos de rede
  - softwares
  - protocolos utilizados
- atividades de gerência voltadas para aspectos de segurança
  - protocolos de gerência
  - registro de acessos e eventos
  - auditoria



REDES TCP/IP - MECANISMOS DE SEGURANÇA

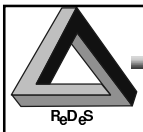
- organizados segundo o modelo de camadas TCP/IP
  - proteções para a rede física e serviços de transmissão
  - proteções para a formação de rede e transporte da informação
  - proteções para suporte à interoperação e para aplicações de rede

APLICAÇÃO (Telnet, SMTP, FTP...)
TRANSPORTE (TCP, UDP, ICMP)
INTER-REDE (IP)
INTRA-REDE/SUB-REDE (Ethernet, Token Ring, X.25, FDDI...)



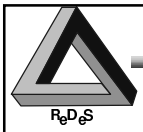
TCP/IP - PROTEÇÕES - CAMADAS FÍSICA/ENLACE

- Incidentes que podem ser prevenidos nestas camadas
  - incidentes de origem natural ou do ambiente
  - ataques visando revelar ou modificar informações sigilosas
    - escuta do meio (ondas eletromagnéticas ou cabeamento)
    - subseqüente análise do tráfego
- Proteções para impedir ou reduzir a probabilidade de tais ataques
  - cabeamento e equipamentos de comunicação
  - canais de comunicação e equipamentos de acesso
  - criptografia das comunicações



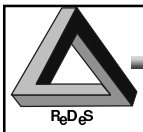
TCP/IP - PROTEÇÕES - CAMADAS FÍSICA/ENLACE

- Cabeamento interno
  - cuidados de instalação - técnicas de engenharia civil e elétrica
    - proteção contra incêndios
    - proteção contra vazamentos de água
    - controle de descargas elétricas
    - aterramento
  - cuidados de operação e manutenção
    - cabos e equipamento de cabeamento periodicamente inspecionados
    - verificação de pontos vulneráveis a desgaste, danos materiais, etc
    - verificação da existência de grampeamento que permita a "escuta" e, possivelmente, a interpretação das informações transmitidas



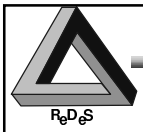
TCP/IP- PROTEÇÕES - CAMADAS FÍSICA/ENLACE

- Equipamentos de comunicação
  - colocados em salas protegidas e de acesso restrito
  - permissão de acesso
    - somente para técnicos e pessoal de gerência de rede
    - pessoas acompanhadas pelos mesmos
  - equipamentos de interface com a rede pública
    - DG, PABX, modems e multiplexadores, antenas
    - técnicos de operadoras públicas devem ser acompanhados



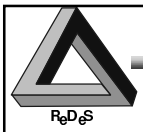
TCP/IP - PROTEÇÕES - CAMADAS FÍSICA/ENLACE

- Canais de comunicação de longa distância
  - Canais satélite
    - dificuldade de decompor o sinal satélite para observar ou modificar as informações na forma de dados
    - necessidade de descobrir satélite, transponder e frequências usadas
    - tratamento do método de acesso, separação dos canais, interpretação do conjunto de protocolos da pilha utilizada
    - necessidade de contornar outros mecanismos de proteção (criptografia, assinatura numérica, etc) eventualmente utilizados
    - mais provável que eventuais atacantes explorem meios mais simples de penetração na rede
  - Linhas dedicadas
    - pontos terminais vulneráveis:permitem identificár facilmente as comunicações originadas ou destinadas a determinada empresa
    - melhor proteger fisicamente os pontos terminais dessas linhas
    - a maior parte dos eventos relativos à segurança de rede têm relação com ataques realizados a partir do interior da empresa proprietária da rede
    - ataques menos prováveis através de cabos ou equipamentos das operadoras de telecomunicações



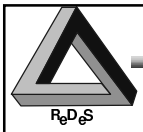
TCP/IP - PROTEÇÕES - CAMADAS FÍSICA/ENLACE

- Canais de comunicação de longa distância
  - Linhas discadas e equipamentos de acesso
    - modems por linha discada fundamentais para conexões com clientes, usuários remotos, usuários em trânsito, etc
  - características dos modems e equipamentos de acesso auxiliares
    - capacidade de interromper as comunicações, caso a ligação telefônica seja interrompida ou por parte do chamador ou por parte dos aplicativos chamados
    - impossibilidade de reprogramação de funções por parte do usuário
    - configuração de um banco de modems apenas para conexões saintes e outro banco de modems apenas para conexões entrantes
    - possibilidade de esquemas de chamada de retorno (call-back) para números previamente definidos
    - possibilidade de utilização de modems com capacidade de criptografar as transmissões



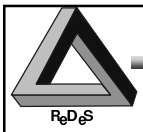
TCP/IP - PROTEÇÕES - CAMADAS FÍSICA/ENLACE

- Criptografia
  - aplicada a todas as informações transmitidas, mesmo aquelas que não têm necessidade de proteção
  - custo do equipamento e da gerência de chaves versus desempenho
  - comparação com criptografia mais seletiva em outras camadas



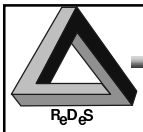
TCP/IP - PROTEÇÕES - REDE/TRANSPORTE

- autentificação entre nós para formação de redes: IPsec
- controle do roteamento das mensagens: *firewall*
- registro de acesso, prevenção contra o estabelecimento de canais para outras formas de ataque: *firewall*, *proxy*
- formação de redes privadas: endereços reservados, *firewall*, *proxy*
- registro de acessos aos programas servidores: TCP *Wraper*



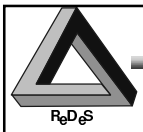
TCP/IP - IPsec

- ftp://ietf.cnri.reston.va.us/internet-drafts/draft-ietf-ipsec-arch-02.txt
- IPsec - Arquitetura de Segurança para o IP-Internet Protocol
- Segurança apenas da camada IP, não é uma Arquitetura de Segurança global da Internet
- Serviços e mecanismos de para IP versão 4 (Ipv4) e IP versão 6 (Ipv6)
  - 2 cabeçalhos especificos para pacotes IP
    - IP Authentication Header (AH): projetado para prover integridade e autentificação sem confidencialidade aos datagramas IP
    - IP Encapsulating Security Payload (ESP): prjetado para prover integridade, autentificação e confidencialidade aos datagramas IP
  - Estabelecimento de Associações de Segurança
  - Uso de método de gerência de chaves criptográficas



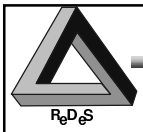
TCP/IP - IPsec

- Associações de Segurança, conceito fundamental tanto para IP-ESP quanto para IP-AH
  - Associação de Segurança: combinação de um *Security Parameter Index* (SPI) com o *Destination Address* dos datagramas IP
    - a Associação é feita em apenas um sentido da comunicação
    - sessões de comunicações protegidas entre dois sistemas normalmente usam dois SPI, um em cada direção
  - Parâmetros do SPI
    - algoritmo de autentificação e modo de utilização do mesmo com o IP-AH
    - chaves usadas com o algoritmo de autentificação associado ao IP-AH
    - algoritmo de cifragem e modo de utilização do mesmo com o IP-ESP
    - chaves usadas com o algoritmo de cifragem associado ao IP-ESP
    - indicador de presença/ausência e tamanho de uma sincronização criptográfica ou campo de vetor de inicialização para o algoritmo de cifragem
    - validade das chaves ou data obrigatória de modificação das chaves
    - validade da própria Associação de Segurança
    - *Source Address(es)* da Associação de Segurança
    - nível de sensibilidade (por exemplo, Secreto ou Não-classificado) dos dados protegidos durante a transmissão



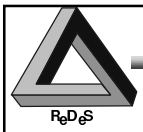
TCP/IP - IPsec

- IP Authentication Header (IP-AH)
  - Utilização
    - entre dois ou mais sistemas implementando AH
    - entre dois ou mais gateways implementando AH
    - entre um sistema ou gateway implementando AH e um conjunto de sistemas ou gateways em uma sub-rede confiável
  - Função: transportar a informação de autentificação do datagrama IP
  - Operação
    - o emissor aplica uma função de autentificação criptografica ao datagrama IP usand uma chave secreta de autentificação
    - o emissor aplica uma função de autentificação antes de enviar o pacote IP autentificado
    - o receptor verifica a correção da autentificação no momento da recepção
    - o algoritmo de autenticação pré-definido é o MD5 usando chave de 128-bits
    - o uso do AH aumenta o custo de processamento do protocolo IP e a latência das comunicações



TCP/IP - IPsec

- IP Encapsulating Security Payload (ESP)
  - Utilização
    - entre dois ou mais sistemas implementando ESP
    - entre dois ou mais gateways implementando ESP
    - entre um sistema ou gateway implementando ESP e um conjunto de sistemas ou gateways em uma sub-rede confiável
    - a criptografia de gateway a gateway é mais útil na construção de redes privadas virtuais através de uma rede não confiável como a Internet
    - ESP não é um substituto da criptografia de sistema a sistema, as duas devem ser usadas conjuntamente
  - Operação
    - o ESP encapsula ou um datagrama IP completo ou apenas o protocolo da camada superior (TCP, UDP, ICMP...)
    - o emissor criptografa o conteúdo do ESP usando o Data Encryption Standard (DES), no modo Cipher-Block Chaining (CBC)
    - o emissor anexa um cabeçalho IP legível ESP criptografado
    - o cabeçalho legível é usado para transportar os dados protegidos através da inter-rede
    - o uso do ESP pode ter impacto substancial no desempenho da rede



TCP/IP - IPsec

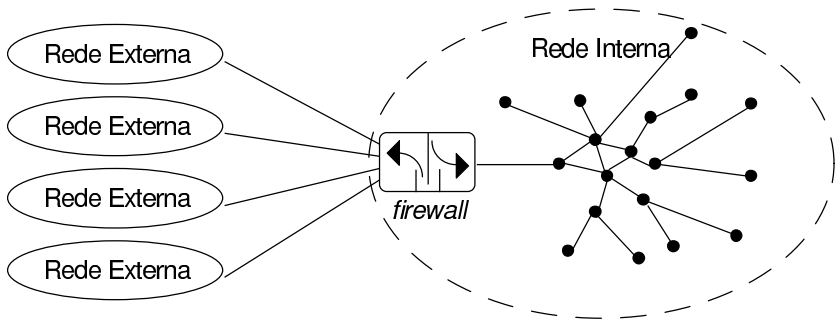
- Gerência de chaves criptográficas
  - o protocolo de gerência de chaves não é especificado
  - a ligação entre o protocolo de gerência de chaves e o AH ou ESP existe apenas como informaçàо no Security Parameters Index (SPI)
  - possíveis métodos de gerência de chaves para IPsec
    - distribuição de chaves manual
    - sistema de distribuição de chaves centralizado como o do Kerberos Authentication System
    - uso do algoritmo de troca de chaves Diffie and Hellman que não requer um sistema de distribuição central
    - distribuição automatizada de chaves
      - armazenamento das chaves de cada sistema no DNS - Domain Name System
      - suporta não somente a segurança do IP, como também de outros protocolos da pilha Internet

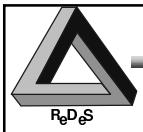
TCP/IP - FIREWALL

- Mecanismo de proteção
  - controle do tráfego tanto no nível das mensagens do protocolo IP, quanto das comunicações TCP e UDP
  - controle do roteamento IP
  - bloqueio de comunicações não autorizadas
- Dispositivos
  - roteadores centralizadores do tráfego
  - filtros de tráfego bloqueiam a transmissão de certas categorias de tráfego: origem, destino, serviço
  - com ou sem auxílio de outro computador ou nó de rede
- Aplicação
  - para controlar o tráfego interno
  - para controlar o tráfego externo: usado na fronteira entre a rede TCP/IP interna (INTRANET) e redes TCP/IP externas

TCP/IP - FIREWALL - FILTRO

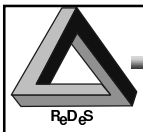
- *Firewall* simples - Roteador





TCP/IP - FIREWALL - FILTRO

- Configuração da filtragem
  - permitir um certo fluxo de dados autorizado
  - dificultar ou impossibilitar que um atacante, via alguma rede externa, penetre na rede interna.
  - modos de configuração
    - filtragem de pacotes IP, com base nos campos de endereços de origem e destino
    - filtragem das PDU TCP e UDP, com base na porta de origem ou destino
    - supressão de tráfego, através da identificação do protocolo da aplicação usuária
    - restrições adicionais em função do contexto: horário, função veiculada na PDU, por exemplo o pedido de estabelecimento de uma conexão ou confirmação de conexão, etc

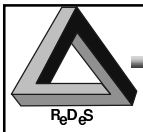


TCP/IP - FIREWALL - FILTRO

- Exemplo: regras de filtragem para SMTP (e-mail, porta 25 TCP):
  - pacotes são rejeitados se não forem especificamente permitidos pelo filtro

A	Host interno * AgenCorreio	Porta * 25	Host externo Bandido *	Porta * *	Ação bloqueia permite	Comentário Não confiamos em "Bandido" Aceitamos conexões para a porta SMTP do nosso e-mail
B	Host interno *	Porta *	Host externo *	Porta *	Ação bloqueia	Comentário Outros pacotes são rejeitados
C	Host interno *	Porta *	Host externo *	Porta 25	Ação permite	Comentário Qualquer Host interno pode enviar e-mail para fora

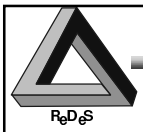
- Problema de regras incorretas, por exemplo regra C:
  - conexões originadas em qualquer porta dos Hosts internos são direcionadas para a porta 25 dos Hosts externos
  - restrição com base apenas no número da porta (25) dos Hosts externos
  - 25 é a porta "normal" do SMTP, mas um atacante pode originar uma conexão a partir da porta 25 de qualquer Host externo e ter acesso a qualquer porta de qualquer Host interno
- nececessidade de usar outras regras de filtragem



TCP/IP - FIREWALL - FILTRO

- Filtragem com base no controle de campos de protocolos:
  - pacotes TCP sem campo ACK são mensagens de estabelecimento de conexões
  - pacotes TCP com campo ACK são comunicações em curso
  - verificando o campo ACK, pode-se proibir atacantes de iniciar conexões
  - regras com base nos campos de protocolo "origem", "destino", "flags"

D	Origem	Porta	Destino	Porta	Ação	Flags	Comentário
	(*Hosts* internos)	*	*	**25**	**permite**		**Nossos pacotes para as portas SMTP dos *Hosts* externos**
	*	**25**	*	*	**permite**	**ACK**	**Respostas dos *Hosts* externos às nossas mensagens**



TCP/IP - FIREWALL - FILTRO

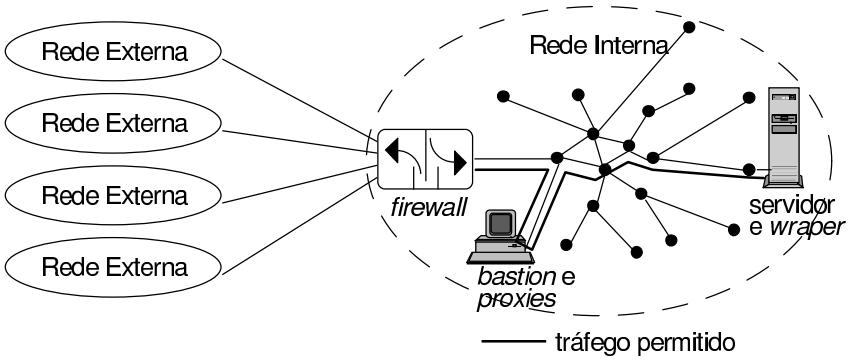
- Outros problemas de filtragem
  - *address spoofing*: um atacante descobre um endereço de um Host interno, usa esse endereço para obter acesso via conexão TCP
  - opção *source route* do IP
  - protocolos que usam portas de controle e portas de dados (FTP: portas 21 e 20)
  - protocolos com serviços envolvendo números de porta randômicos (RPC)
  - protocolos com base em datagramas (UDP)
  - virtualmente sem proteção para ataques via de protocolos de alto nível
- Soluções mais confiáveis somente com auxílio de outro computador ou nó de rede
  - *gateways* de aplicação
  - softwares de registro de operações

TCP/IP - FIREWALL - FILTRO

- Restrições de tráfego típicas
  - rejeitadas todas as mensagens usando protocolos desconhecidos
  - rejeitadas mensagens entrantes usando protocolos conhecidos, mas considerados perigosos: telnet, rlogin, rexec, rpc, TFTP, printer, finger, name, time, domain, NNTP, HTTP, SNMP, NFS, X, etc.
  - permitidas as mensagens usando SMTP (correio eletrônico) e FTP (transferência de arquivos)
  - permitido o fluxo de mensagens usando protocolos especiais da própria empresa ou de empresas parceiras: EDI, homebanking, TEF (transferência eletrônica de fundos), controle de processos, etc
- Proteção do tráfego permitido
  - uso de um computador interno (*bastion*) exclusivamente como *gateway* das aplicações autorizadas através de *proxies*
  - uso de software de registro de acesso (*wraper*) nos servidores internos

TCP/IP - FIREWALL

- *Firewall* auxiliado por *bastion*, *proxies* e *wrapers*

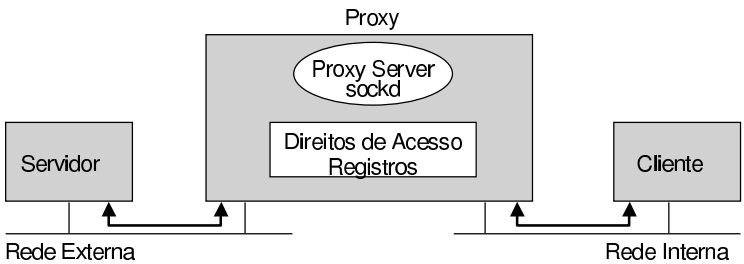


TCP/IP - FIREWALL - BASTION E PROXIES

- todo o tráfego que passar pelo *firewall* deve ser destinado para, ou originado no, *bastion*
- o *bastion* deve ser controlado por um sistema operacional limitado ao extremo em suas funções:
  - sem ferramentas de programação, editores, programas de configuração e pesquisa de arquivos e processos, etc
  - sem configuração de contas regulares de usuários
  - roda servidores de correio eletrônico, de transferência de arquivos
  - roda proxies Telnet, FTP, gopher, WEB, etc.
  - roda servidor DNS (Domain Name Server) para permitir que a rede interna tenha visibilidade sobre as redes externas acessíveis
- gerência da segurança no *bastion* e no *firewall*
  - todas as facilidades de registro para auditoria, providas pelo sistema operacional, ativadas: registro de logins, registro de operações, registro de arquivos acessados, etc
  - eventos registrados devem ser objeto de verificação sistemática por parte da gerência de rede, se possível diariamente

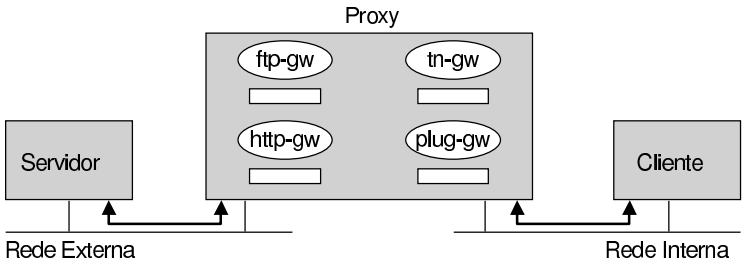
TCP/IP - PROXY

- *proxy* genérico
  - exemplo SOCKS - ftp://ftp.nec.com/pub/security/socks.cstc/
  - uso transparente, porém exige modificação do software cliente
  - registro de eventos para auditoria e possibilidade de autentificação



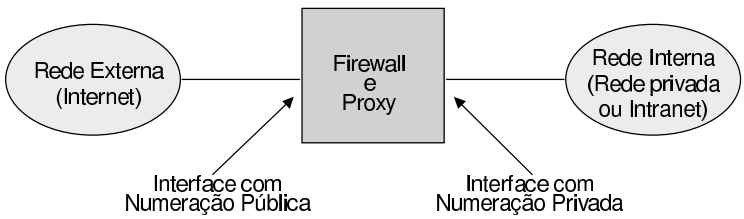
TCP/IP - PROXY

- *proxy* de aplicação
  - exemplo TIS - ftp://ftp.tis.com/pub/firewalls/toolkit/
  - não transparente, porém sem modificação do software cliente
  - registro de eventos para auditoria e funcionalidades de aplicação



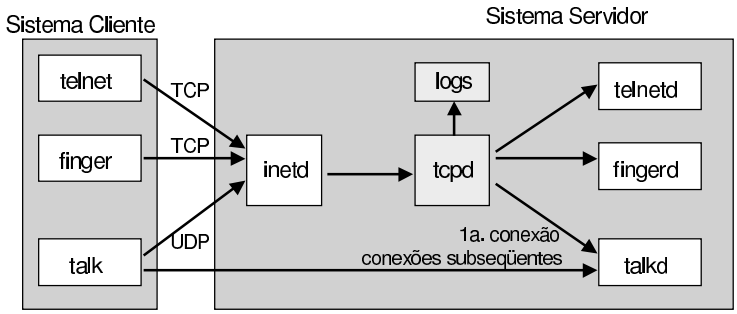
TCP/IP - FIREWALL + PROXIES - REDES PRIVADAS

- RFC 1597 - endereços reservados
  - classe A10.0.0.0 - 10.255.255.255
  - classe B172.16.0.0 - 172.31.255.255
  - classe C192.168.0.0 - 192.168.255.255
- Impossível o roteamento direto, acesso através do *firewall*



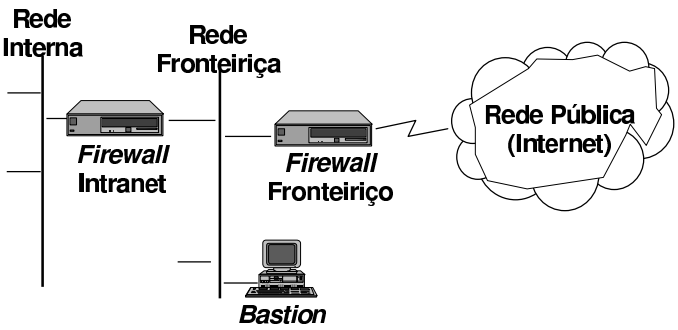
TCP/IP - TCP WRAPER

- Filtro de aplicação tcpd - ftp://ftp.win.tue.nl/pub/security/
  - opera no mesmo computador que os programas servidores
  - registra acessos válidos e inválidos e possibilita usar armadilhas
  - é capaz de filtrar conexões



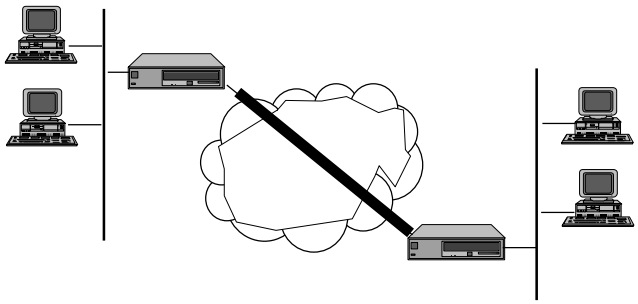
TCP/IP - COMBINAÇÃO DE PROTEÇÕES

- *Firewall* + *Bastion* + *Firewall*
  - um intruso, conseguindo invadir o *bastion*, esbarra em uma segunda barreira



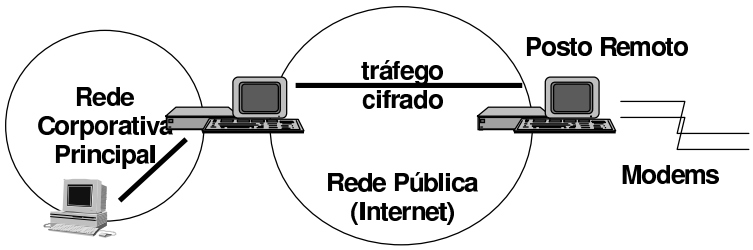
TCP/IP - COMBINAÇÃO DE PROTEÇÕES

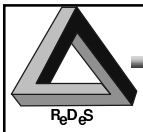
- Firewall + Criptografia + Firewall
  - aplicações não-confiáveis, como NFS, podem ser usadas com segurança
  - os dados não podem ser monitorados por um intruso
  - tráfego falso não pode circular pela rede
  - o funcionamento normal do *firewall* não se altera



TCP/IP - COMBINAÇÃO DE PROTEÇÕES

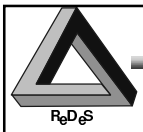
- Firewall + Criptografia + Equipamento de Acesso
  - Sistema remoto acessa de modo transparente a rede corporativa
  - Suporta acesso discado, provendo um posto remoto de acesso para usuários em trânsito via PPP ou emulação de terminal





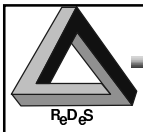
TCP/IP - PROTEÇÕES - CAMADA APLICAÇÃO

- Situação de fato: “tudo o que não é formalmente proibido, é permitido”
  - comportamento normal dos intrusos
  - comportamento até mesmo de usuários regulares
- Restringir drasticamente o uso de serviços da rede não é uma solução aceitável
- Garantir a disponibilidade dos serviços apenas para os usuários que realmente necessitem
  - considerar os diversos perfis de usuário
  - tomar cada um dos serviços de rede separadamente
  - tabular um cruzamento de usuários contra serviços, com cada necessidade especificada
- Usar proteções que devem cobrir serviços completos da rede



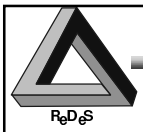
TCP/IP - PROTEÇÕES - CAMADA APLICAÇÃO

- Regras genéricas básicas de proteção preventiva dos serviços
  - uso obrigatório das proteções de acesso dos sistemas operacionais
    - mecanismos para identificação de usuários
    - uso de senhas e atualização periódica das mesmas
    - classificação dos usuários ou organização de grupos de usuários
    - definição dos direitos de uso de aplicativos e arquivos de dados em função do tipo de usuário e de grupos de usuários
    - delimitação das áreas de trabalho em discos e em memória
  - restringir a utilização de serviços FTP (transferência de arquivos), Telnet (emulação de terminal) e SMTP (correio eletrônico)
    - em função do cargo, do departamento, da unidade de lotação dos usuários e se possível do terminal utilizado
    - por exemplo, um caixa bancário, não deve ter direito a nenhum dos serviços, pois não tem necessidade deles no seu trabalho



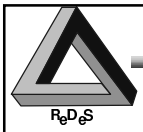
TCP/IP - PROTEÇÕES - CAMADA APLICAÇÃO

- Regras genéricas básicas de proteção preventiva dos serviços
  - proibir transferência de arquivos por usuários anônimos (anonymous ftp)
  - proibir procedimentos remotos perigosos
    - login remoto via aplicação diferente de Telnet
    - procedimentos de execução remota
    - procedimento de obtenção de informações remotamente
    - por exemplo, em UNIX, não devem ser ativados os processos rlogin, rsh, rexec, finger, etc
  - proibir mecanismos de interoperação com base no estabelecimento de sistemas ou usuários confiáveis
    - trusted hosts, trusted users
    - login automático, sem verificação de senha
  - proibir ou limitar sistema de arquivos distribuído, como NIS/NFS, por exemplo



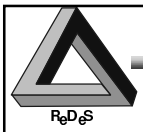
TCP/IP - PROTEÇÕES - CAMADA APLICAÇÃO

- Proteções de aplicações e mecanismos de interoperação
  - aquisição de um sistema unificado de controle de acesso global aos sistemas e aplicativos da Rede
  - implantação de um sistema para controle dos direitos de uso de recursos da Rede: kerberos
  - implantação de um suporte seguro para controle da interoperação entre aplicativos: secure-RPC, SSL - Secure Sockets Layer, secure-DNS
  - implantação de correio eletrônico com funcionalidades específicas de segurança: PEM - Privacy Enhanced Mail, X.400, S-MIME - Secure Multimedia Mail Extension
  - implantação de protocolos de aplicação com funcionalidades específicas de segurança S-HTTP - Secure Hypertext Transfer Protocol, secure-Java, SET - Secure Electronic Transactions



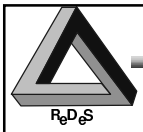
TCP/IP - PROTEÇÕES - CAMADA APLICAÇÃO

- Proteção dos dados utilizados
  - arquivos
  - registros de bancos de dados ou campos nesses registros
  - backup incremental diário
  - backup global periódico (por exemplo, semanal)
  - arquivos considerados mais sensíveis devem ser criptografados na máquina e obrigatoriamente antes de qualquer transmissão
  - utilização de criprografia seletiva: PGP - Pretty Good Privacy



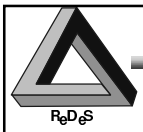
TCP/IP - PROTEÇÕES - CAMADA APLICAÇÃO - WEB

- Configuração dos servidores WEB
  - mecanismo de *basic authentication* de HTTP 1.0
  - controle de acesso a arquivos
  - arquivos de registro de atividades do servidor
- Proteção das comunicações navegador-servidor WEB
  - HTTPS (HTTP + SSL), S-HTTP
  - utilização de Autoridade Certificadora
  - *firewall* e *proxy* HTTP
- Proteção das comunicações servidor WEB - servidor banco de dados
  - criptografia
- Execução de programas CGI e Java em ambiente protegido

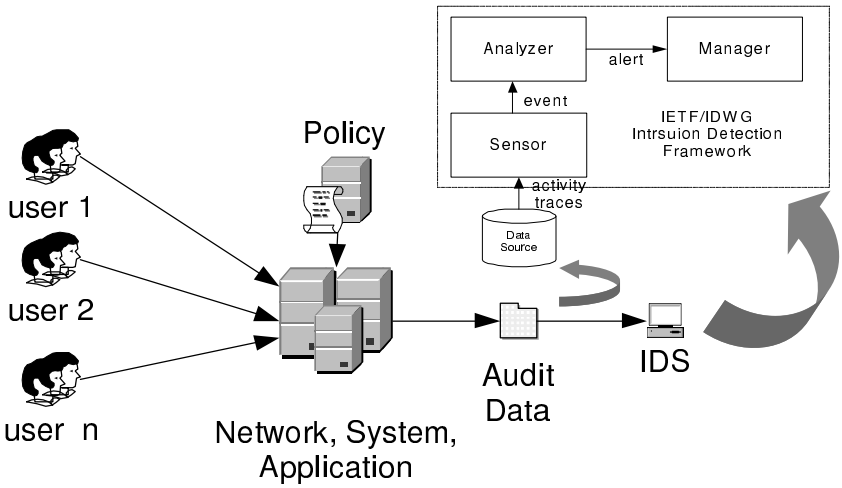


SISTEMAS DE DETECÇÃO DE INTRUSÃO

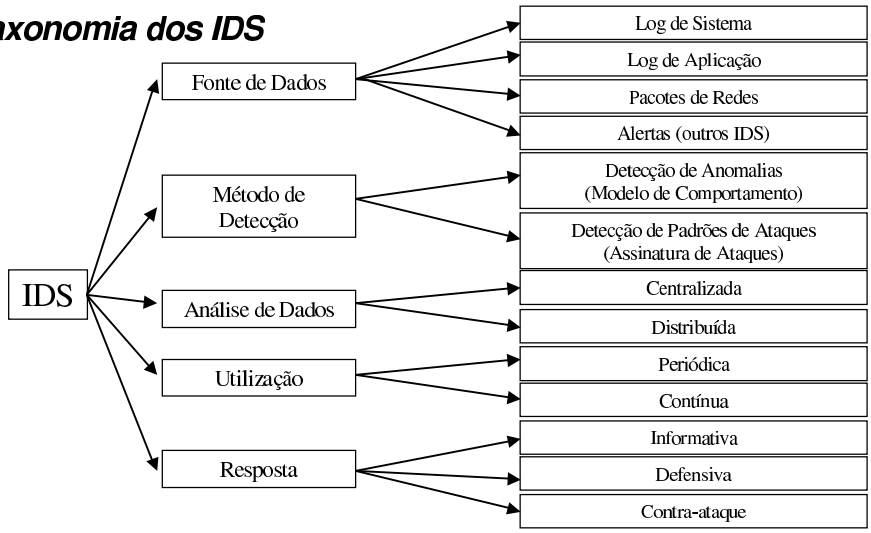
- Definições
  - Toda atividade visando comprometer a integridade, a confidencialidade e a disponibilidade de um recurso
  - Exploração de falhas de segurança
  - Encadeamento malicioso de operações autorizadas (abuso de privilégios)
- Detecção de Intrusão
  - Ação complementar à implantação de mecanismos de segurança
  - Limitação das conseqüências de um ataque (segurança corretiva)
- IDS: *Intrusion Detection System*



Modelo de um Sistema de Detecção de Intrusão

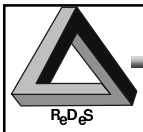


Taxonomia dos IDS



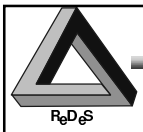
Métodos de Detecção

- Abordagem por comportamento
  - Modelo do comportamento "normal" (sistema especialista, modelo estatístico, inteligência artificial, etc.)
  - Detecção de desvios do comportamento (anomalias)
  - Vantagem: capacidade de generalização (novos ataques)
  - Desvantagens: não se sabe o que se está detectando, necessidade de atualização (médio/longo prazo) do modelo
- Abordagem por cenário
  - Modelo de padrões de ataques (assinatura)
  - Vantagem: identificação do ataque que esta sendo realizado
  - Desvantagem: não detecta novos ataques (atualização da base de assinaturas)



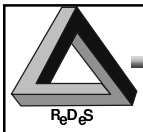
Exemplos de Sistemas de Detecção de Intrusão (1/2)

- Fonte de Dados
  - Sistema: ISS, Tripwire, etc.
  - Aplicação: IDS para aplicação de e-mail, etc.
  - Rede: snort, Cisco IDS, RealSecure, etc.
  - Alertas: Tivoli Risk Management, etc.
- Método de Detecção
  - Comportamento (anomaly): apenas acadêmicos
  - Cenário (misuse): quase a totalidade dos produtos comerciais



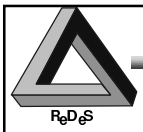
Exemplos de Sistemas de Detecção de Intrusão (2/2)

- Análise de Dados
  - A maioria dos sistemas comerciais tem um console de análise de dados e gerenciamento centralizado
  - Alguns sistemas comerciais possuem coleta e pré-processamento de dados distribuída
- Periodicidade
  - Atuação em tempo real desejável
- Tipo de Resposta
  - A maior parte dos sistemas proporcionam uma resposta puramente informativa,
  - Ativação automática de respostas defensivas em alguns casos
  - Problemas legais para utilização de sistemas que realizam contra-ataque



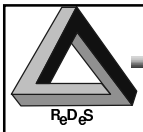
TCP/IP - GERÊNCIA DA SEGURANÇA E AUDITORIA

- análise das condições de segurança da rede
  - COPS - ftp://info.cert.org/pub/tools/cops/
    - senhas ruins e arquivo de senhas
    - acesso a diretórios e arquivos, arquivos exportados
    - arquivos de configuração, comandos
  - SATAN - ftp://ftp.win.tue.nl/pub/security/
    - vulnerabilidades de acesso via rede
- verificação sistemática de eventos
  - ativar registro de logins, registro de operações, registro de arquivos acessados, etc
  - SWATCH - ftp://soe.stanford.edu/pub/sources/
    - análise de registros de eventos
    - execução de ações apropriadas determinadas pelo adminstrador



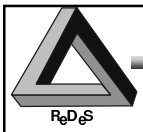
TCP/IP - GERÊNCIA DA SEGURANÇA E AUDITORIA

- coleta de dados e operações de gerência em tempo real
  - SNMP - *Simple Network Management Protocol* (Internet Standard RFC 1067, RFC 1157) é o protocolo padrão de fato na gerência de redes TCP/IP
  - Informações de gerência definidas na MIB - *Management Information Base*, referente aos objetos (recursos de rede) gerenciados
  - Modelo gerente-agentes
    - simplicidade estrutural e operacional
    - baixa sobrecarga de memória, de processamento e de rede
    - utilizável em vários equipamentos e fácil de adaptar



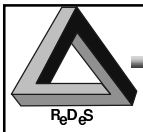
SNMP - MODELO DE GERÊNCIA PADRÃO INTERNET

- Natureza das Informações de Gerência
  - interfaces entre os equipamentos e o meio
  - tipo e configuração das interfaces
  - status operacional das interfaces e equipamentos: *up*, *down*, teste
  - estatísticas das interfaces e equipamentos: número de quadros recebidos, enviados, descartados devido a erros...
  - dados específicos dos protocolos TCP/IP
    - tradução endereço IP - endereço físico
    - contagens de pacotes IP de entrada e saída
    - tabelas de conexão TCP
  - eventos na redes e nos sistemas
  - dados dos computadores/sistemas: memória, CPU, discos, aplicações...



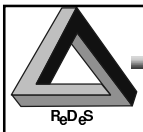
SNMP - MODELO DE GERÊNCIA PADRÃO INTERNET

- Modelo Gerente-Agente, capacita os gerentes de rede para
  - exame dos dados dos dispositivos da rede
  - atualizaçào de informações de configuração e status
  - acionamento (limitado) de funções nos dispositivos da rede
- Entidades do modelo
  - software AGENTE e AGENTE PROCURADOR
  - software GERENTE
  - ESTAÇÃO DE GERÊNCIA
  - APLICAÇÕES DE GERÊNCIA
  - BASE DE DADOS DE GERÊNCIA e DEPÓSITO DE DADOS
  - PROTOCOLO GERENTE-AGENTE



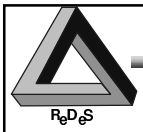
SNMP - MODELO DE GERÊNCIA PADRÃO INTERNET

- Softwares Agente
  - instalados nos dispositivos de rede
  - recebem mensagens de um GERENTE
  - mensagens são requerimentos de READ ou WRITE dos dados dos dispositivos
  - se possível, o AGENTE realiza o que é requerido e envia RESPOSTAS ao GERENTE
  - um AGENTE pode enviar uma NOTIFICAÇÃO (*trap*) ao GERENTE sem que tenha havido um requerimento: isso quando ocorrem eventos significativos ou problemas no AGENTE
- Software Gerente
  - funciona em uma ESTAÇÃO DE GERÊNCIA
  - envia MENSAGENS aos AGENTES
  - recebe RESPOSTAS dos AGENTES
  - recebe NOTIFICAÇÕES espontâneas (*traps*) dos AGENTES



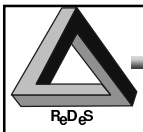
SNMP - MODELO DE GERÊNCIA PADRÃO INTERNET

- Estações de Gerência
  - hospedam o software GERENTE
  - armazenam informações coletadas dos AGENTES
  - hospedam APLICAÇÕES DE GERÊNCIA
- Aplicações de Gerência
  - permitem ao usuário (operador/gerente da rede) controlar o software de gerência
  - visualização de informações sobre a rede
  - não são submetidos à padronização: GUI, módulos de software, bancos de dados, etc



SNMP - MODELO DE GERÊNCIA PADRÃO INTERNET

- Aplicações de Gerência
  - Mapeamento automático da rede
  - Coleta e apresentaçào de dados operacionais
  - Seleção e apresentação de eventos significativos
  - Relatórios espontâneos de eventos
  - Avisos sobre rompimento de limites
  - Apresentação de mensagens de outras aplicações
  - Divisão do trabalho de gerência
  - Ferramentas para construção de aplicações customizadas
  - Aplicações para encontrar, examinar e armazenar informaçòes de gerência



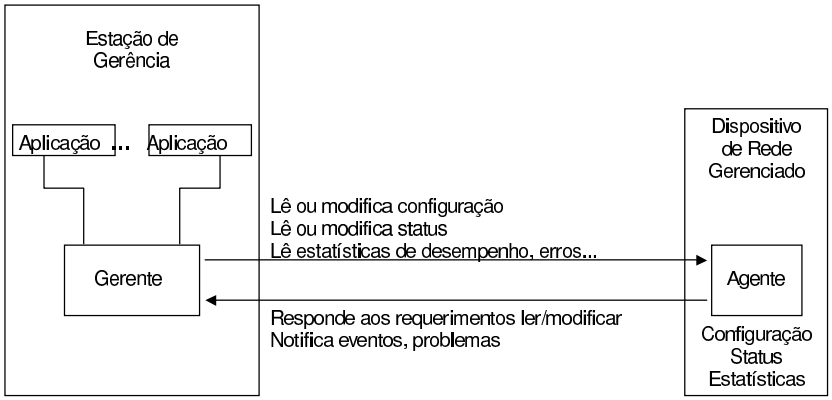
SNMP - MODELO DE GERÊNCIA PADRÃO INTERNET

- Protocolo de Gerência
  - tipos de mensagens entre o GERENTE e o AGENTE
  - formatos das mensagens

    version, community, command, requestID, error status, error index, {object value}
  - protocolos de comunicaçào a serem utilizados
- Base de Dados de Gerência
  - informaçòes armazenadas nos agentes e copiadas para os gerentes
  - descritas de forma abstrata nos gerentes

    SysDescr, SysObjectID, SysUpTime, SysContact, SysName, SysLocation, SysServices, ifNumber, ifTable (ifIndex, ifDescr, ifType, ifMTU, ifSpeed)...
- Depósito de Dados
  - armazenado nas estações de gerência
  - contém os dados coletados de todos os agentes

SNMP - MODELO - ENTIDADES/INTERAÇÕES



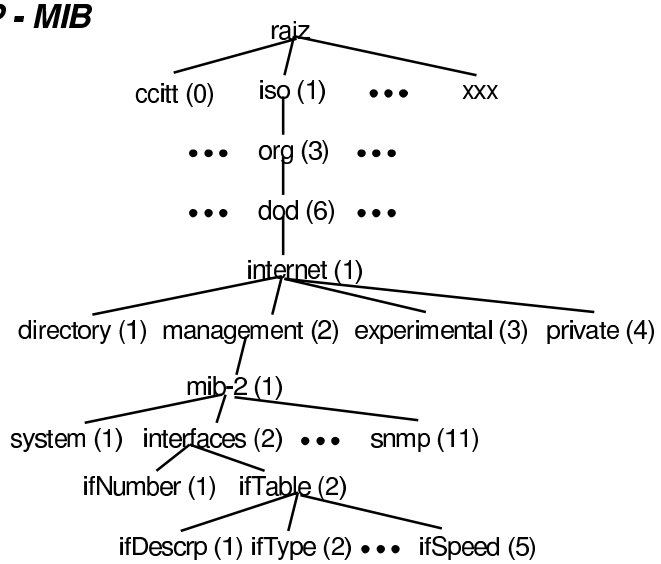
SNMP - MIB /MANAGEMENT INFORMATION BASE

- Informações sobre os Objetos Gerenciados
  - Todo elemento/recurso gerenciado é considerado como um objeto
  - MIB: Conjunto estruturado de objetos
  - Cada agende possui sua MIB
  - O NMS monitora e controla a rede lendo e alterando a MIB dos agentes
- MIB - Base de Informações de Gerência
  - definição precisa da informação acessível através do protocolo de gerência de rede
  - formato estruturado, hierárquico, definido na RFC 1065 - SMI - *Structure of Management Information* (Estrutura da Informação de gerência)
- MIB existentes:
  - MIB-I para TCP/IP (RFC 1066)
  - MIB-II: extensão da MIB-I (RFC 1213)
  - várias extensões de fornecedores de equipamentos
  - RMON - *Remote Network Monitoring*

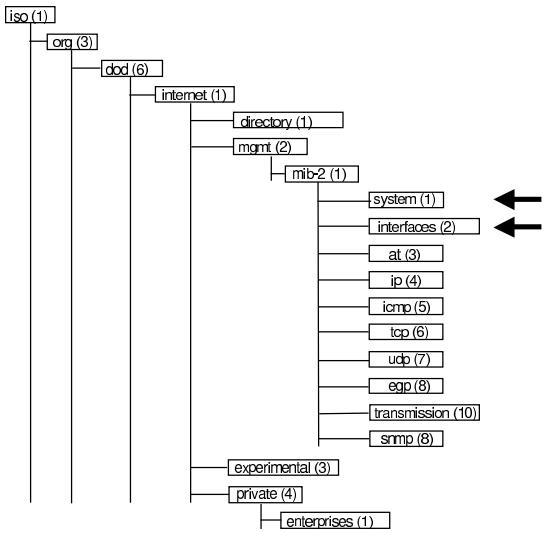
SNMP - MIB/MANAGEMENT INFORMATION BASE

- RFC 1155 - SMI - regras gerais para montagem de MIB
  - Estrutura de uma MIB
  - Objetos individuais: sintaxe e valores
  - Codificação de valores para os objetos
- Arquitetura da MIB:
  - Síntaxe OSI ASN.1 (TLV)
  - Arborescência:
    - Nós da árvore: identificador numérico + descrição textual
    - Folhas da árvore: objetos que cotêm valores
- Especificação de objetos
  - Nome Textual
  - Identificação Númérica (ASN.1)
  - Definição Semântica
  - Tipo de Acesso - RO, RW, WO, NA
  - Status: obrigatório, opcional, obsoleto

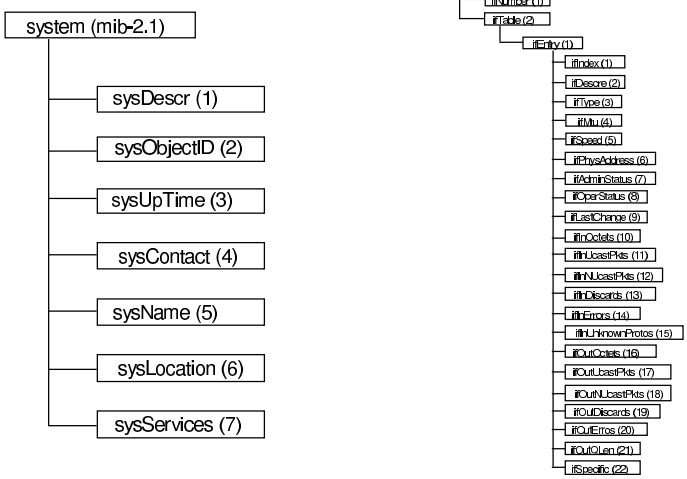
SNMP - MIB

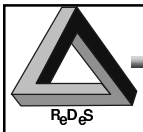


SNMP - ESTRUTURA DA MIB



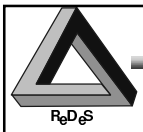
SNMP - MIB II - RFC 1156





SNMP/MIB - SINTAXE DOS OBJETOS

- Utiliza ASN.1, mas por simplicidade é usado um conjunto restrito de elementos e características
- Tipo de dados universais usados
  - INTEGER (Universal 2)
  - OCTET STRING (Universal 4)
  - NULL (Universal 5)
  - OBJECT IDENTIFIER (Universal 6)
  - SEQUENCE, SEQUENCE OF (Universal 16)
- Alguns tipos de objetos definidos pela SMI
  - Network Address
  - IpAddress
  - Counter
  - Gauge
  - Time Ticks
  - Opaque



SNMP/MIB - SINTAXE DOS OBJETOS - EXEMPLO

sysDescr OBJECT-TYPE
SYNTAX DisplayString (SIZE(0.255))
ACCESS read-only
STATUS mandatory
DESCRIPTION

"A textual description of the entity. This value should include the full name and version identification of the system's hardware type, software operating-system, and networking software. It is mandatory that this only contain printable ASCII characters."

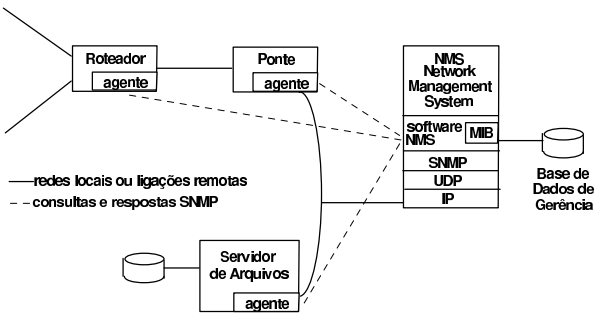
::= { system 1 }

SNMP - PROTOCOLO

- Dois modos de Operação
  - Síncrono: Comando do Gerente/Resposta do Agente
  - Assíncrono: Notificações dos Agentes
- Tipos de Operação/Mensagens
  - NMS obtém valor de variável do agente:
    - Get-request
    - Get-next-request
    - Get-response
  - NMS atualiza valor de variável no agente
    - Set-request
  - Agente envia informação não solicitada
    - Trap
- Simplicidade e limitações
  - SNMP permite apenas verificar e alterar variáveis
  - Não há comandos de ação
  - Não é possível aumentar ou diminuir MIB

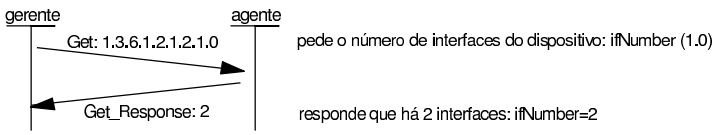
SNMP - PROTOCOLO - OPERAÇÃO

- Comunicação gerente-agentes:
  - *Polling*: a entidade central de gerência regularmente consulta os agentes para verificar se estes têm alguma informação a relatar
  - Agentes procuradores (*proxy*) permitem fazer interface com outros protocolos de gerência
  - Autentificação através de *community string*, não criptografada



SNMP - PROTOCOLO - MENSAGENS

- Protocolo SNMPv1:
  - Mensagens:
    - Get_Request (elemento MIB)
    - Get_Response (elemento MIB, valor)
    - Get_Next_ Request (elemento MIB)
    - Set_Request (elemento MIB, valor)
    - Trap (elemento MIB, evento)
  - Forma de Interação:



SNMP - PROTOCOLO - POSIÇÃO NA PILHA TCP/IP

SNMP
UDP
IP + ICMP
Sub-rede

SNMP - PROTOCOLO - MENSAGENS - FORMATOS

Formato Geral

Versão	Comunidade	PDU

Formatos Específicos de PDU

- Get-request, Get-next-request, Set-request

Tipo	ind-req	0	0	Variáveis

- Get-response

Tipo	ind-req	status de erro	índice de erro	Variáveis

- Trap

Tipo	empresa	endereço agente	trap específico	Tempo	Variáveis

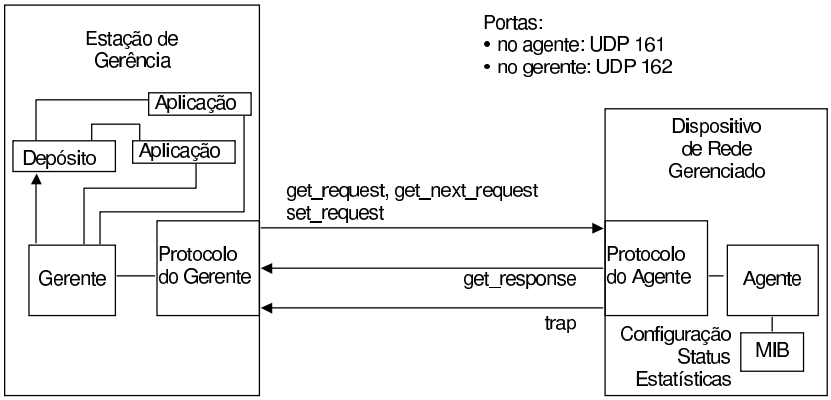
Formato das Variáveis

Nome 1	Valor 1	Nome 2	Valor 2	Nome 3	Valor 3

SNMP - PROTOCOLO - MENSAGENS - CAMPOS

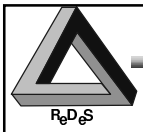
Versão: Versão do SNMP (0 ou 1)
Comunidade: Nome da Comunidade (funciona como senha)
Tipo: Tipo de PDU
Id-req: Número da requisição (para associar respostas a comandos)
Status de erro: Indica alguma exceção de
(0) no-error (1) tooBig
(2) no Such Name (3) bad Value
(4) read Only (5) genericError
Índice de erro: Informação adicional sobre exceções
Empresa: Tipo de objeto gerador do trap
Trap-genérico: Informação genérica sobre o erro
(c) cold Start (1) warm Star
(2) link Down (3) link Up
(4) authentication Failure (5) EGP Neighbour Loss
(6) enterprise Specific
Trap específico: Informação adicional a critério do fabricante
Time-stamp: Tempo desde última reinicialização

SNMP - MODELO - ENTIDADES/INTERAÇÕES



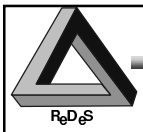
SNMP - COMUNIDADE DE GERÊNCIA

- Várias Estações Gerentes podem acessar um Agente
- Um agente usa o parâmetro *community* do protocolo para realizar controle de acesso
  - autenticação de gerentes
  - reforço de uma política de acesso
- O parâmetro *community* é veiculado nas mensagens SNMP sem nenhuma proteção particular
  - vulnerável à escuta clandestina e ataque por repetição



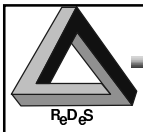
SNMP - v1 - SÍNTESE

- Benefícios:
  - Simplicidade: facilidade de implantação e pouca sobrecarga nos agentes
  - Distribuição dos agentes:
    - separa o sistema de gerência dos elementos gerenciados
    - se há problemas com os elementos gerenciados, a capacidade de gerência permanece intacta
    - diferente dos tradicionais sistemas centralizados que, ao sair do ar, paralizavam também as atividades críticas de gerência
  - Gerência integrada: evita o uso de ferramentas de gerência separadas para cada plataforma ou segmento
- Problemas:
  - Agentes não inteligentes + protocolo por *polling*:
    - iduzem muito tráfego de gerência na rede
    - geram muitos alarmas referentes ao mesmo evento
    - não se adaptam a grandes redes
  - Mecanismo de autentificação muito fraco
- Solução: SNMPv2, RMON ou OSI



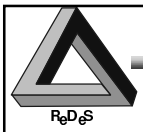
GERÊNCIA DE REDES SNMP - SNMPv2

- Segurança:
  - autentificação:
    - gerente e agente compartilham chave secreta
    - usam tal chave para calcular código de autentificação associado a cada mensagem, usando algoritmo MD5
  - confidencialidade (segredo):
    - gerente e agente compartilham outra chave secreta
    - usam esta chave para criptografar as mensagens com algoritmo DES
  - controle de acesso:
    - agentes possuem diferentes níveis de acesso para gerentes
    - acessos autorizados em função dos comandos solicitados ou partes da MIB acessadas (MIB views)
  - MIB segurança



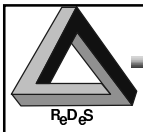
GERÊNCIA DE REDES SNMP - SNMPv2

- Transferência de informações de gerência:
  - nova mensagem GetBulk_Request: versão melhorada de Get_Request para coleta de dados em grandes volumes
  - Set_request executado em duas fases: validação de variáveis, atualização
  - Get_request executado para cada objeto onde for possível
  - Trap simplificado: mesmo formato das outras PDU com informações adicionais na MIB SNMP v2
- Cooperação Gerente-Gerente:
  - nova mensagem Inform_Request para comunicação de notificações entre gerentes
  - MIB Gerente-Gerente: especifica eventos que geram notificações, informações contidas em notificações, gerentes destinatários de notificações...



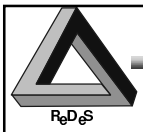
GERÊNCIA DE REDES SNMP - RMON

- RFC 1271, RFC 1213
- Objetivos
  - reduzir a quantidade de informações trocadas para efeito de gerência
  - permitir a gerência proativa da rede, registrando e diagnosticando eventos que possibilitem prever falhas e mau funcionamento
  - detectar e registrar eventos significativos e informar a ocorrência dos mesmos a multiplas estações de gerência
- Estrutura
  - nas redes remotas, coloca-se MONITORES de rede 'promíscuos': escutam todos os pacotes que passam
  - no MONITOR existe uma base de informaçòes especial, a RMON-MIB que é uma extensão da MIB-II
  - não há modificações no protocolo SNMPv1
  - não há modificações nos outros elementos do modelo SNMP: estações de gerência, aplicações, MIB, depósitos de dados...



GERÊNCIA DE REDES SNMP - RMON

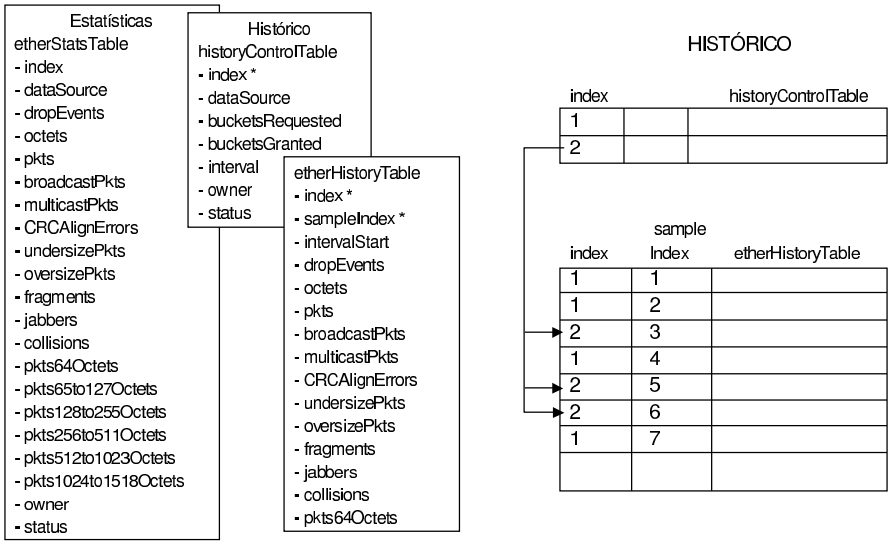
- Monitor Remoto
  - operação *off-line*
    - representa uma distribuição do processamento para efeito de gerência, exigência decorrente da existência de redes muito complexas
    - não precisa haver comunicação constante entre gerente e agente
    - assemelha-se a um agente procurador (proxy)
  - previsão e detecção de falhas
    - coleta de informações para antecipação de erros
    - notificação (*trap*)
  - funções de valor agregado: estatísticas, histórico, filtragem...
  - suporte à invocação de ações remotas
  - suporte ao acesso por várias estações gerentes: o ID de uma estação gerente fica associado aos recursos do monitor alocados a tal estação



GERÊNCIA DE REDES SNMP - RMON

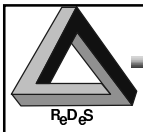
- RMON-MIB
  - Configuração interna
    - Tabela de controle: especifica como funciona o dispositivo monitor
    - Tabela de dados: cotém os próprios dados coletados
    - 9 grupos de informações de monitoração remota de implemetação opcional
  - Grupos de informações/Funções
    - Estatísticas: pacotes (número/tamanho), colisões, erros, pacotes descartados
    - Histórico: intervalos de amostragem e registro de dados históricos do grupo estatísticas de modo a permitir a análise de tendências
    - Alarmes: condições limites de funcionamento da rede para notificação (*trap*), com mecanismo para não inundar o gerente de alarmes
    - Hosts: contagem de tráfego entrante/sainte nos computadores da rede remota
    - HostTopN: classificação dos host segundo certo critério, ex: tráfego sainte
    - Matriz: matriz de tráfego ou de erros nas comunicações entre pares de hosts
    - Filtro: condições de captura de pacotes para registrar estatísticas da rede remota
    - Captura de Pacotes: alocação e controle de *buffers* para armazenar pacotes
    - Eventos: especificação de eventos que devem provocar envio de notificações aos gerentes ou registro em uma tabela (logTable) interna do Monitor

SNMP - RMON - GRUPOS - EXEMPLO



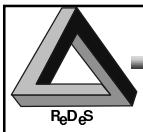
SEGURANÇA EM REDES LOCAIS

- Mecanismos de segurança dos Sistemas Operacionais de LAN
  - segurança de acesso à rede
    - senha e as restrições de acesso por estação
    - contas disponibilizadas com data de expiração
    - detecção de tentativas de penetração ou uso indevido dos recursos pelos próprios usuários
    - rastreamento das conexões e desconexões de usuários, com registros dos horários e locais
    - estabelecimento de limites de utilização de recursos
    - bloqueio de *login*
  - direitos de operação sobre arquivos e diretórios e atributos de arquivos e diretórios
    - lista de diretório e arquivos acessíveis
    - direitos de uso: ler, escrever, copiar, criar, apagar, etc
    - proteções específicas de arquivos e diretórios



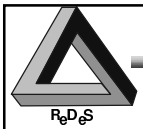
SEGURANÇA EM REDES LOCAIS

- Mecanismos de segurança dos Sistemas Operacionais de LAN
  - controle de acesso a servidores, por exemplo ao Servidor de Arquivos
    - uso de aplicativos de monitoração
    - direitos de administração
    - desativação do servidor
    - desconexão de usuário suspeito
    - difusão de avisos de emergência
    - uso de aplicativos de auditoria e controle: verificação de direitos, verificação de violações, visualização de módulos ativos
  - funcionalidades de tolerância a falhas
    - uso de FATs redundantes
    - verificação de escrita e leitura
    - controle de atualizações incompletas em bancos de dados
    - espelhamento e duplicação de disco
    - no-break



SEGURANÇA EM REDES LOCAIS

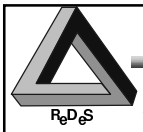
- Mecanismos de segurança dos Sistemas Operacionais de LAN
  - Procedimentos genéricos básicos
    - não devem ser instalados programas executáveis em quaisquer diretórios onde usuários possam criar, escrever, apagar
    - o servidor deve ser instalado em sala com trincos e fechaduras e com ventilação adequada, e a sala deve ser mantida fechada durante a ausência do supervisor autorizado
    - o teclado do servidor deve ser sempre trancado quando não estiver em uso pelo supervisor;
    - quando o ambiente onde residem as estações for de difícil controle, onde circulem pessoas estranhas à empresa por exemplo, devem ser adotadas estações disk-less
    - para evitar a intrusão através dos cabos das redes locais, quando possível, em ambientes sujeitos a riscos, deve ser utilizada fibra óptica
    - os dados sensíveis (por exemplo, senhas) que trafegam na rede devem, sempre que possível, ser criptografados



IV - CONCLUSÃO

CONCLUSÃO

- Medidas de proteção para os diversos componentes dos SI
  - Pode-se alcançar níveis de segurança tão altos quanto se deseje, em termos de robustez, eficácia e cobertura das medidas de proteção
  - Medidas de proteção representam custos adicionais e acarretam restrições de uso dos sistemas de informação
- Necessidades fundamentais
  - Elaborar a Política de Segurança
  - Preparar os recursos humanos e organizacionais
  - Avaliar ameaças, vulnerabilidades e riscos e comparar ao custo das proteções
  - Convecer os usuários a USAR EFETIVAMENTE as medidas de proteção
  - Convecer os administradores a APLICAR EFETIVAMENTE as medidas de proteção
  - Manter o estado de vigilância permanente



FONTES

- Livros
  - Chapman. Zwicky. Building Internet Firewalls. O'Reilly & Associates, Inc. 1995
  - Garfinkel. Spafford. Practical UNIX Security. O'Reilly & Associates, Inc. 1994
  - Pfleeger. Security in Computing, 2a. Ed. Prentice-Hall. 1997
  - http://www.ora.com
- Endereços
  - ftp://info.cert.org/pub/cert_advisories/
  - ftp://rtfm.mit.edu/pub/usenet/news.answers/firewalls-faq
  - http://www.rsa.com
  - http://www.tis.com