Tópicos em Redes de Computadores

Aula de Hoje:

Segurança – Aula 1

Prof. Elias P. Duarte Jr.
Universidade Federal do Paraná (UFPR)
Departamento de Informática
www.inf.ufpr.br/elias/topredes

Contextualização

- Acabamos de terminar o 1º pilar da nossa disciplina – Redes Celulares
- Os dois próximos pilares são:
  - BlockChain
  - Sistemas Tolerantes a Intrusão
- Ambos os pilares são fortemente calcados na área de Segurança Computacional
- Assim vamos ter algumas aulas de segurança & criptografia

Sumário da Aula de Hoje

- Por que preocupar com segurança?
- Ataques & Vulnerabilidades
- Medidas de segurança: definições
- Sigilo & Privacidade, Integridade, Autenticidade e Disponibilidade
- Passwords, Hashing e Assinaturas Digitais
- Criptografia: chaves secreta & pública
- Panorama de ferramentas de segurança TCP/IP

Uma Necessidade

- Perigo!
- As redes de empresas e organizações têm sido atacadas constantemente
- Roubos: bancos, cias aéreas, informação
- Vandalismo
- Ignorância
- Os ataques vêm de dentro e de fora
- Além de vulnerabilidades físicas e naturais

Problemas Diversos

- Entre os muitos, muitos casos reportados quase todo dia:
  - Recentemente: hackers roubaram US$600 milhões em criptomoedas
    - Um dos [auto-alegados] criminosos afirmou que fizeram “por diversão” e para “expor uma vulnerabilidade”
  - Não são apenas ataques: um bug de software alterou as contas de um banco de tal forma que foi necessário pedir um empréstimo de bilhoes de dólares até a situação se resolver
  - Antigamente, um caso “curioso” (apesar de trágico): vírus que alteram a taxa de refrescamento de um monitor de vídeo levam a sua explosão → mudou a indústria!
  - Sites vandalizados incluem: UFPR, CIA (EUA) e governos ao redor do mundo

The Worm: O "Verme"

- Na Internet, os problemas de segurança começaram com data e hora: o *worm*, de 1988
- O programa afetou 6000 computadores
- Após se instalar em uma máquina, o verme se reproduzia, consumindo recursos locais, e se expandindo para máquinas vizinhas
- Alvo: servidores BSD-UNIX de e-mail e finger
- Mostrou que a rede, na época eminentemente acadêmica, não era segura

O que é segurança?

- O objetivo é proteger o sistema computacional – hardware inc. computadores e rede, software de todas as naturezas e dados de acessos e alterações não autorizadas
- Os *invasores* e *impostores* querem obter informações ou bens ou auto-afirmação; mas NÃO são as únicas ameaças
- Medidas de segurança: sigilo & privacidade, autenticidade, integridade e disponibilidade

Sigilo & Privacidade

- Sigilo
  - Somente pessoas & processos *autorizados* devem ter acesso aos diversos recursos do computador e da rede
  - É necessário controlar os níveis de acesso e o que cada um pode fazer
  - Deve ser possível manter e transmitir *informações secretas*
  - Criptografia é a chave do sucesso
- Privacidade: o direito de reservar o acesso aos dados, recursos, condições e atos de uma entidade – indivíduo ou organização

Integridade & Autenticidade

- As informações armazenadas e em trânsito não podem ser corrompidas, alteradas de forma acidental ou maliciosa
- Deve ser garantida a integridade das informações armazenadas e transmitidas
- Devem haver meios de pessoas & processos garantirem a autenticidade de sua identidade

Disponibilidade

- Também é parte da segurança: a rede deve funcionar ininterruptamente
- Deve estar disponível para você quando precisar
- Capacidade de recuperação rápida (idealmente imediata) após falhas, desastres e ataques
- Inclusive: garantir que usuários ignorantes ou maliciosos impeçam o trabalho de outros esgotando os recursos disponíveis

Para que serve a segurança?

- Vulnerabilidades: pontos do sistema suscetíveis ao ataque
- Ameaça: um perigo potencial, pode ser pessoa, processo, desastre, falha
- Medidas de segurança: visam proteger o sistema

Vulnerabilidades

- Comunicação - mensagens podem ser forjadas, interceptadas, desviadas, repetidas
- Falhas e vulnerabilidades de hardware & software
- Vulnerabilidades Físicas (cabeamento da rede...)
- Naturais (incêndio...)
- A mais desafiadora: *pessoas*
  - Em particular: administradores do sistema

Sistema Seguro: Componentes

- Controle de acesso ao sistema
- Controle de permissões, acesso de pessoas e programas às informações armazenadas
- Sistema de *logs*: quem acessou fez o que?
- Administração de segurança: incluindo monitoramento contínuo, treinamento de usuários

Controle de Acesso

- Quem pode entrar no sistema?
- Indentificação + Autenticação
- Métodos de Autenticação incluem:
  - passwords
  - chaves, cartões magnéticos, smart cards
  - impressão digital, reconhecimento de voz, retina, assinatura, padrões de digitação

Passwords

Passwords: A Verdade

"A password should be like a toothbrush. Use it everyday; change it regularly; and DON'T share it with friends"

- A alternativa de autenticação mais prática e mais comum
- Para serem efetivas, é necessário:
  - escolher boas passwords
  - elas devem ser protegidas
- Sempre sujeitas a um ataque de força bruta
  - o invasor tenta todas as combinações, uma de cada vez

Ataques a Passwords

- Existem 2.800.000.000.000 combinações possíveis de 8 caracteres
- Checando 1 milhão de combinações por segundo: demora 45 anos checar todas as possibilidades
  - problema computacionalmente inviável
- O problema é que muitos usuários não escolhem boas passwords...

Passwords Fáceis de Descobrir

- Estudos mostram que grande quantidade de usuários escolhem passwords extremamente simples de descobrir
- Os invasores podem usar um dicionário de passwords comuns
- Entretanto se a password for bem escolhida, fica muito difícil ela ser descoberta, com ou sem um dicionário

Dicas para escolher uma boa password

- Não selecionar palavras da língua portuguesa, inglesa, espanhola...
- Misturar caracteres alfabéticos com numéricos e especiais (&%@...)
- Misturar letras maiúsculas e minúsculas
- Melhor escolher passwords mais longas - mínimo de 8 caracteres
- Escolha passwords diferentes para sistemas diferentes
- Não escreva sua password num papel ou arquivo!

Ainda sobre passwords:

- Uma boa alternativa é escolher as iniciais de uma frase que faça algum sentido F@$Sntd0
  - crie seu próprio alfabeto secreto ;-)
- Nunca mandar a password por e-mail
  - possivelmente a aplicação mais insegura de todas
- Qualquer suspeita: mude a password imediatamente
- O sistema deve incluir providências para diminuir a probabilidade de sucesso de ataque

Armazenando Passwords

- Em geral, os sistemas armazenam passwords criptografadas
- Nunca é necessário descriptografar, basta checar se a versão criptograda está certa
- Por isso é usado hash: "*one way encryption*"
  - um dos 3 tipos de criptografia, "resumo digital"
- O arquivo de passwords deve ter a maior restrição de acesso que o sistema puder oferecer (*shadow password files*)

Programas Perigosos

Virus

- Fragmento de código que invade um sistema, que faz cópias de si próprio, e invade outros programas
- A Internet é o meio perfeito para propagação de virus
- Todos os dias novos vírus são criados, descobertos...

Virus: Estrutura Básica

- Trocar uma instrução numa posição x, por um jump para a posição y
- O código do vírus começa nesta posição
- A instrução originalmente na posição x deve seguir o código do vírus, com jump x+1

Vírus: Antídotos

- Como podemos descobrir a existência de um vírus?
- Os antídotos mais comuns conhecem o código dos vírus, e fazem a busca por padrões dos códigos
- É necessário atualizar tais checadores constantemente, pois novos vírus surgem a todo momento

Para Driblar os Antídotos...

- Foram criados os vírus *polimórficos*
- A cada vez que tais virus criam cópias de si próprios, eles alteram a ordem de suas instruções, ou alteram algumas instruções para outras com funcionalidade similar
- Existem antídotos para estes também, mas a busca de padrões tem que ser mais sofisticada...

Para Driblar os Novos Virus...

- Foram criados antídotos que tiram “fotografias” dos diretórios e, tomando como base parâmetros como o tamanho de arquivos podem descobrir contaminação
- Aí surgiram os vírus que comprimem parte do programa, para que o tamanho total permaneça inalterado!
- Outros antídotos checam a autenticidade de cada arquivo

Trojan Horses

- Disfarce para programas invasores
- O usuário pensa que se trata de um programa, mas a verdade é diferente
- Mais comum: para capturar passwords
- Outras classificações de pestes incluem: bactérias (vírus que é um programa independente), bombas lógicas (vírus com data-hora para atacar) anjos, etc...

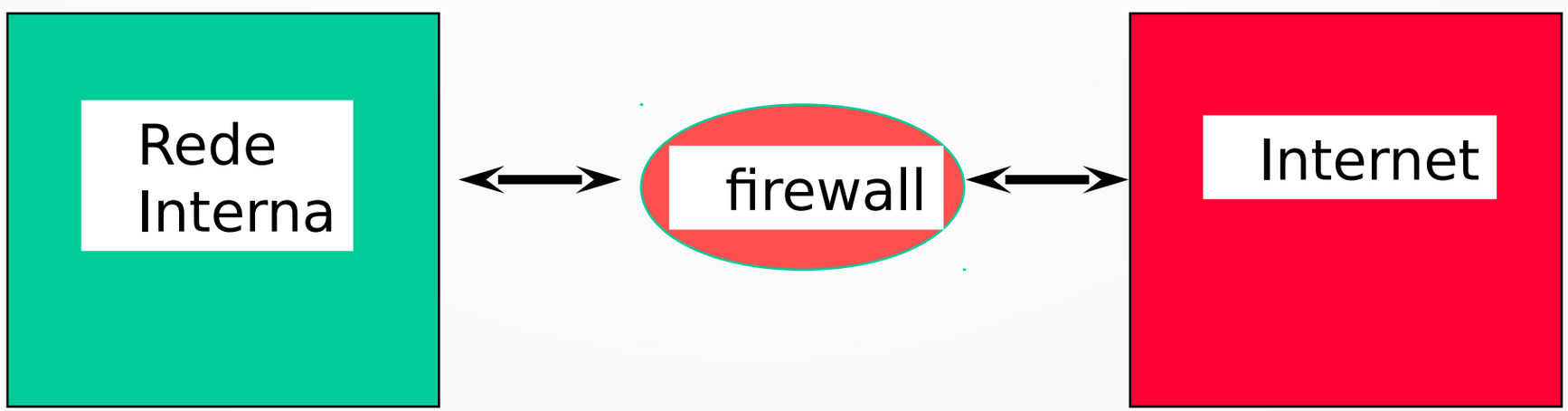
Medidas Preventivas

- Não executar programas vindos de fontes suspeitas: em especial por e-mail
- Fazer backups periódicos
- Delimitar ambientes (jogos, trabalho, ...)

Ferramentas de Segurança

Firewall

- É um filtro de pacotes, que fica entre a rede interna de uma organização & a Internet

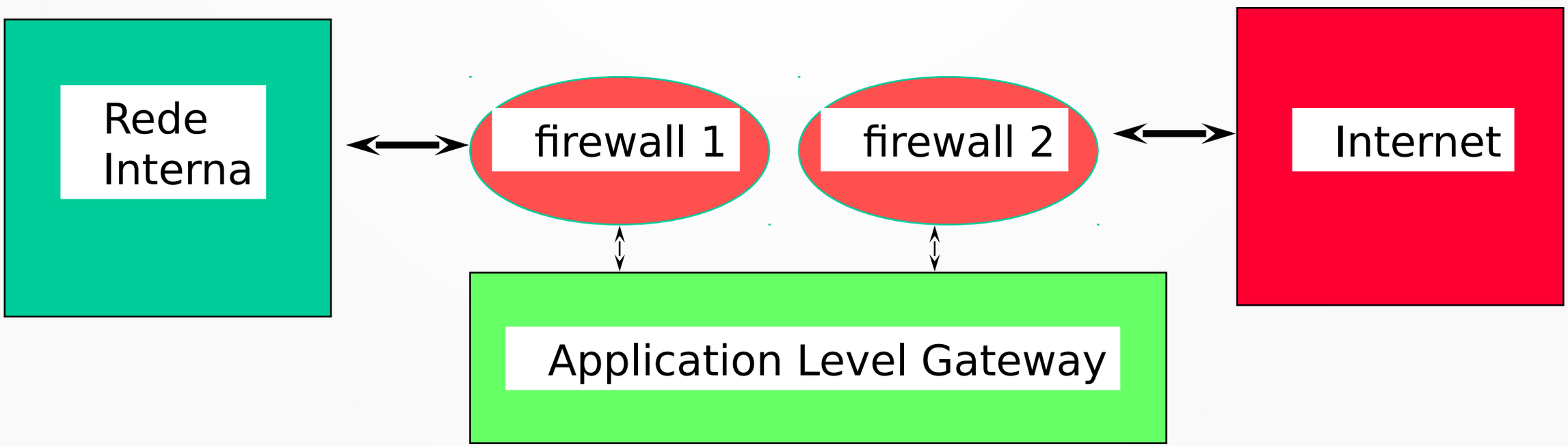


Firewall: Funcionamento

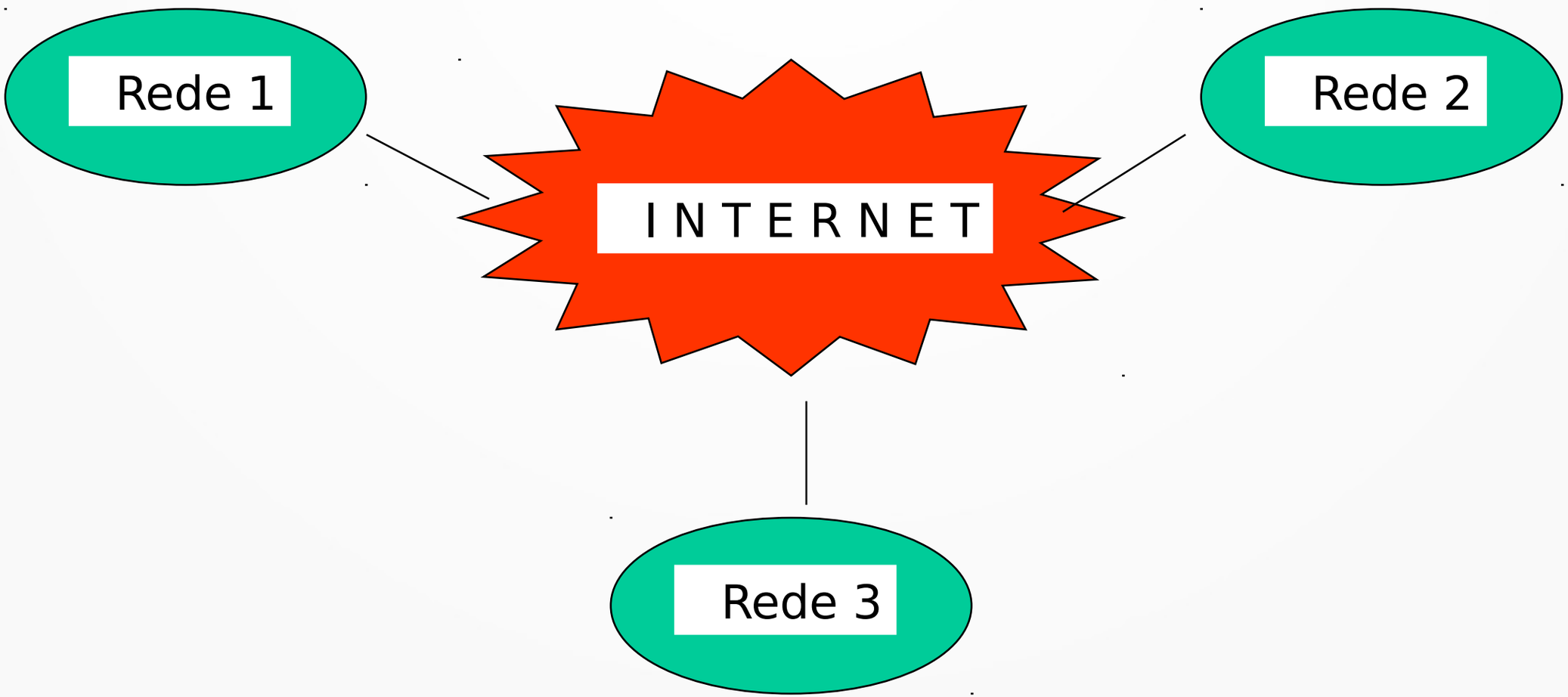
- Um firewall deve ser configurado com um conjunto de regras que permitem a passagem de alguns pacotes e impedem a passagem de outros
- Critérios diferentes podem ser escolhidos
- Exemplos incluem: endereços de rede, portas, protocolos de aplicação específicos
- Veja: que sem autenticidade do header IP é fácil forjar um endereço falso de origem (*IP Spoofing*)

Firewall em Nível de Aplicação

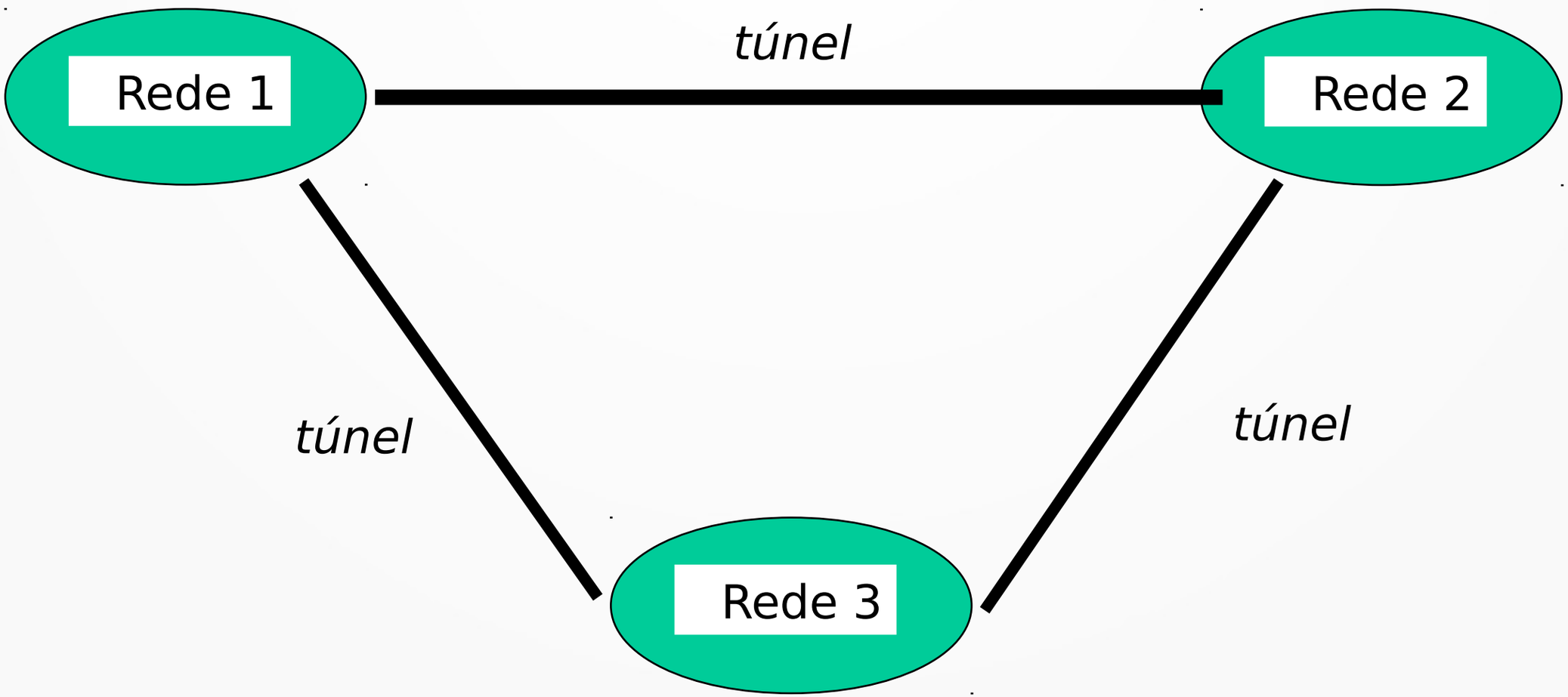
- É possível filtrar também na camada de aplicação, além da camada de rede



Túneis de Segurança



Túneis de Segurança



Virtual Private Network: VPN

- Tecnologia WAN, que permite a comunicação segura através da Internet
- Os dados são transmitidos através de “túneis”, que tem gateways de segurança na suas pontas
- O conteúdo de todas as mensagens é criptografado
- Mecanismos de autenticação e certificação são usados para validar mensagens/usuários

Criptografia

- A base de toda a segurança
- Consiste em codificar uma mensagem de forma que apenas quem tem a *chave* adequada é capaz de decodificar
- São três tipos de criptografia:
  - Criptografia de Chave Secreta
  - Criptografia de Chave Pública
  - Hash (Resumo Digital)
- Explicar como fazer *assinatura digital*

Autoridade Certificadora

- *Public Key Infrastructure*
- Como é que o usuário vai ter certeza de quem são as chaves públicas?
- Uma autoridade independente, idônea, deve emitir um certificado de autenticidade
- Como funciona?
- A autoridade assina o certificado digital do usuário

Segurança em Todas as Camadas

Segurança nas Camadas

- Segurança Física
- Segurança de Enlace
- Segurança no Nível de Rede:
  - Firewalls
  - VPN
- Segurança de Transporte: SSL & TLS (*Secure Socket Layer & Transport Layer Security*)
- Segurança das Aplicações

Aplicações Seguras

- Segurança da Aplicação
- Aplicações de Segurança
- Sistemas Cliente-Servidor
- Na Internet:
  - PGP: Ferramenta para segurança de e-mail
  - DNS seguro
  - etc etc etc...

Sistemas de Gerência de Rede

- Ferramentas automatizadas para monitoração e controle de redes;
- Sua funcionalidade inclui a gerência de
  - Falhas
  - Desempenho
  - Configuração
  - Contabilização
  - Segurança
- Protocolo de Gerência da Internet: SNMP

Aspectos Legais e Importação

- Governos consideram criptografia uma tecnologia perigosa
- Nos EUA, diversas tecnologias de segurança são patenteadas e...
- existem restrições quanto à exportação de diversos produtos (criptg. = munição)
- Leis específicas têm sido desenvolvidas, desde copyright até crimes digitais

Conclusão

- Segurança: uma necessidade
- Sigilo & Privacidade, Autenticidade, Integridade e Disponibilidade
- Vulnerabilidades, Ataques
- Programas perigosos; passwords perigosas
- Segurança em todas as camadas!
- Aspectos Legais
- Próxima aula: criptografia!

Obrigado!

Lembrando: a página da disciplina é:
https://www.inf.ufpr.br/elias/topredes

Obrigado!

Lembrando: a página da disciplina é:
https://www.inf.ufpr.br/elias/topredes