



# Segurança Informática em Redes



**António Costa**  
Departamento de  
Engenharia Informática  
ISEP/IPP


28-11-1999 António Costa - DEI/ISEP 1



## Visão

- **Computação omnipresente**
  - Quase não se nota
  - Altamente adaptável às pessoas
- **Objectos interligados**
  - Habitação
  - Trabalho
  - Sociedade
  - Cultura e Lazer
- **Novamente simples e fácil!**

28-11-1999 António Costa - DEI/ISEP 2



## Objectivos Abstractos

- **Confidencialidade**
  - Informação vai apenas para quem deve receber
- **Autenticação**
  - Origem da informação é correctamente identificada
- **Integridade**
  - Informação modificada apenas por quem está autorizado
- **Não-repudição**
  - Confirmação inegável do envio e recepção da informação
- **Controlo de acesso**
  - Recursos de informação controlados por quem está autorizado
- **Disponibilidade**

28-11-1999 António Costa - DEI/ISEP 3

## Objectivos Práticos

- **Segurança da informação**
  - 2 Grandes mudanças recentes
    - Antes: através de meios físicos e administrativos
    - Computador: **necessidade de ferramentas de protecção de informação armazenada**
    - Sistemas distribuídos: **necessidade de ferramentas de protecção de informação em trânsito**
- **Segurança informática em redes**
  - Meios para **impedir, prevenir, detectar e corrigir** violações de segurança no trânsito da informação

28-11-1999 António Costa - DEI/ISEP 4

## Objectivos Práticos

- **Assunto complexo mas interessante**
  - Em teoria é fácil; a prática mostra o contrário
  - Pode haver modos de contornar os mecanismos de segurança (não há esquemas infalíveis)
  - As violações dos mecanismos de segurança tendem a ser simples mas devastadoras
  - Muitos mecanismos de segurança são “esquisitos”
  - Os mecanismos de segurança exigem a sua própria segurança (quem os controla, de que modo, etc)

28-11-1999 António Costa - DEI/ISEP 5

## Ataques à Segurança

- **Genericamente “fingir”**
  - Obter acesso indevido a informação de outros
  - Simular outra pessoa para imputar responsabilidade
  - Validar informação maliciosamente produzida
  - Afirmar ter recebido informação
  - Afirmar ter enviado informação
  - Modificar indevidamente os direitos dos outros
  - Esconder a existência de certa informação
  - Escutar indevidamente o trânsito de informação
  - Alterar indevidamente uma função de software
  - Causar falhas aparentes no funcionamento normal

28-11-1999 António Costa - DEI/ISEP 6

## Ataques Informáticos

- **Interrupção**
  - Alguma coisa é destruída

~~disponibilidade~~
- **Intercepção**
  - Acesso indevido

~~confidencialidade~~
- **Modificação**
  - Alteração indevida

~~integridade~~
- **Fabricação**
  - Criação indevida de informação

~~autenticidade~~

28-11-1999 António Costa - DEI/ISEP 7

## Ataques Informáticos Passivos

- **Intercepção**
  - Difusão da informação
  - Análise de tráfego
- **Muito difíceis de detectar**
  - Não há alteração de informação
- **A solução é**

**Prevenção!**

28-11-1999 António Costa - DEI/ISEP 8

## Ataques Informáticos Activos

- **Alteração de informação**

- **Mascarada**: fazer-se passar por outro
- **Retransmissão**: captura passiva de informação e retransmissão subsequente
- **Modificação de mensagem**: alteração semântica da informação
- **Negação de serviço**: dificultar o funcionamento normal

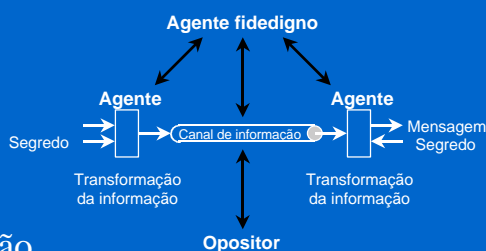
- **Muito difíceis de prevenir**

- **A solução é**

**Detecção e Recuperação!**

28-11-1999 António Costa - DEI/ISEP 9

## Modelo de Segurança em Rede



- **Modelo**

- **Canal** de informação
- **Protocolos** de comunicação
- **Uso cooperativo** pelos agentes
- Como obter segurança:
  - Transformação da informação a enviar
  - Informação secreta partilhada pelos agentes

28-11-1999 António Costa - DEI/ISEP 10

## Modelo de Segurança de Acesso

**Opositor**  
Humano  
Software

Canal de acesso

Porteiro

**Sistema de informação**

- Recursos de computação
- Informação
- Processos
- Software
- Monitorização interna

- **Modelo**
  - **Proteger** de acesso indevido
  - **Fase 1**: porteiro vigilante (*firewall*, etc)
  - **Fase 2**: monitorização interna

28-11-1999   António Costa - DEI/ISEP   11

## Intrusos

- **Hacker ou Cracker**
- **Tipos:**
  - **Mascarado**: usa indevidamente o acesso de outro
  - **Malfeitor**: usa para além dos seus limites
  - **Clandestino**: controla indevidamente o sistema e elimina os seus passos
- **“The Cuckoo’s Egg” - Cliff Stoll**
- **Problema crescente e universal**

28-11-1999   António Costa - DEI/ISEP   12

## Intrusos

- **Técnicas**

- Acesso ao sistema
- Aumento das capacidades

- **Descoberta de *passwords***

- Palavras pequenas, dicionários, siglas, etc
- Escutar informação em trânsito
- Fingir ser um utilizador (engenharia social)

- **Usar “boas” *passwords***

- Educação dos utilizadores

28-11-1999 António Costa - DEI/ISEP 13

## Intrusos

- **Detecção**

- Rapidez
- Desencorajador
- Recolha de informação para melhorar

- **Auditoria**

- Programas de *recolha de dados para auditoria*
- Detecção por *análise estatística*
- Detecção por *inferência, regras, etc*
- Detecção *distribuída (des)centralizada*

28-11-1999 António Costa - DEI/ISEP 14

## Vírus

- **Programas maliciosos**

- **Bactéria**: consome recursos replicando-se
- **Bomba lógica**: função activada por certo contexto (sexta feira 13, etc)
- **Porta secreta**: acesso não-documentado a um programa (filme “War Games”)
- **Cavalo de Troia**: função inserida num programa (utilitário “modificado”)
- **Vírus**: código inserido num programa que se replica
- **Verme**: programa auto-replicante que se espalha sózinho

- **Sistemas sem administrador!**

28-11-1999 António Costa - DEI/ISEP 15

## Crime Informático

- **Falhas de segurança física**

- “Vasculhar lixo”
- Escuta telefónica
- Emissões electromagnéticas
- **Degradação ou negação de serviço**
  - Destuição ou desactivação de material
  - Inundação lógica (*flooding*)
  - Muitas vezes é acidental!
    - Erros de software
    - Trabalhos de impressão

28-11-1999 António Costa - DEI/ISEP 16



## Crime Informático

### • Falhas de segurança pessoal

#### – Mascarada

- Obtenção de *passwords* indevidas

#### – Engenharia social

#### – Assédio

- Cada vez mais frequente na Internet

#### – Pirataria de software

- Deixar copiar software legal
- Instalar cópia ilegal de software
- Modificar software para ultrapassar protecções

28-11-1999 António Costa - DEI/ISEP 17

## Crime Informático

### • Falhas de segurança de informação e comunicação

#### – Ataques à informação

- Cópia ilegal de dados
- Análise de tráfego
- Dissimulação

#### – Ataques a software

- Portas secretas, cavalos de Troia, vírus, etc
- Tomada de sessão
- Trânsito dissimulado de dados (*tunneling*)
- Ataques temporais (deficiências de programas)

28-11-1999 António Costa - DEI/ISEP 18

## Crime Informático

- **Falhas de segurança operacional**

- **Modificação de informação** (analógica)
- **Endereços IP forjados** (*spoofing*)
  - Cada vez mais frequente
- **Captura de passwords** (*sniffing*)
  - Monitorização de tráfego de rede
- **Varrimento** (*scanning*)
  - Telefones, serviços de rede, etc
- **Aumento de capacidades**
  - Privilégios de *superuser* em UNIX, etc

28-11-1999 António Costa - DEI/ISEP 19

## Crime Informático

- **Leis / Regulamentos**

- Institucionais, Departamentais, etc
- Nacionais (109/91 de 17-08-91) e Internacionais

- **Prevenir**

- Ameaça
- Vulnerabilidade
- Contramedida
- Solução

**Análise de Risco**

28-11-1999 António Costa - DEI/ISEP 20

## Crime Informático

- **Antes...**

- Definir um grupo de pessoas para actuar
- Definir níveis de ameaça e ataque
- Activar vários meios de detecção
- Alterar o esquema de vez em quando

- **Depois...**

- Desligar ou continuar ligado?
- Investigar a intrusão ou ignorar?
- Criar uma armadilha?

28-11-1999 António Costa - DEI/ISEP 21

## Crime Informático

- **URL's relevantes**

- **CERT** [www.cert.org](http://www.cert.org)
  - Arquivo de documentos muito completo
- **CIAC** [www.ciac.llnl.gov](http://www.ciac.llnl.gov)
  - Compilação de ferramentas e documentos
- **Hacked.Net** [www.hacked.net](http://www.hacked.net)
  - Tem ligações para quase tudo!
- **L0pht** [www.l0pht.com](http://www.l0pht.com)
  - Tem material interessante para *Windows NT*
- **BugTraq** [www.geek-girl.com/bugtraq](http://www.geek-girl.com/bugtraq)
  - Arquivo da *mailing list* BugTraq

28-11-1999 António Costa - DEI/ISEP 22

## Níveis de Segurança

- **Ideal** (sala fechada e sem ligações!)
- **Livro “Laranja” (DoD, EUA)**
  - **D1**: sem segurança (Windows 3.1X, 95, DOS, Mac)
  - **C1**: controlo e utilizadores (UNIX convencional)
  - **C2**: auditoria (Windows NT, UNIX)
  - **B1**: segurança multi-nível
  - **B2**: protecção estruturada
  - **B3**: domínios de segurança
  - **A**: sistema verificado

28-11-1999 António Costa - DEI/ISEP 23

## Política de Segurança

- **Abordagens**
  - **Por omissão proíbe-se**  
Especifica-se o que é autorizado
  - **Por omissão autoriza-se**  
Especifica-se o que é proibido
- **Documento de política de segurança**
  - Descreve como a segurança é considerada
  - Passo inicial para poder proteger os recursos
  - “Regras de Acesso e Uso” do DEI-ISEP  
[www.dei.isep.ipp.pt/DEI/use.html](http://www.dei.isep.ipp.pt/DEI/use.html)

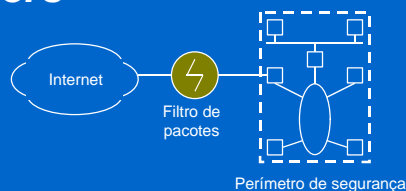
28-11-1999 António Costa - DEI/ISEP 24

## Soluções para Controlo de Acesso

### • Filtragem por routers

#### – Critérios

- Protocolo
- Endereço de origem
- Endereço de destino
- Campos de controlo



#### – Simples mas eficiente

#### – Controlo do tipo de tráfego circulante

#### – Filtro de pacotes (*packet filter*)

28-11-1999 António Costa - DEI/ISEP 25

## Filtro de Pacotes

### • Diverso hardware

- Aplicações comerciais tipo *firewall*
- Aplicações software em PC
- *Routers* comerciais (Cisco, 3COM, etc)

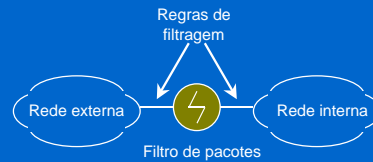
### • Diversas políticas de segurança

- Manter intrusos fora / ~~Policar utilizadores~~
- Definir onde colocar e o que filtrar
- Transparência para os utilizadores de dentro
- Dificultar ataques de dentro

28-11-1999 António Costa - DEI/ISEP 26

## Filtro de Pacotes

- **Modelo Comum**



- **Filtragem**

- Guardam-se regras de filtragem por interface
- Quando chega um pacote, analisa-se o cabeçalho
- Cada regra é aplicada ao pacote sucessivamente
- Se uma regra bloqueia, o pacote é desprezado
- Se uma regra autoriza, o pacote é aceite
- Se não há regra, o pacote é desprezado (aceite)

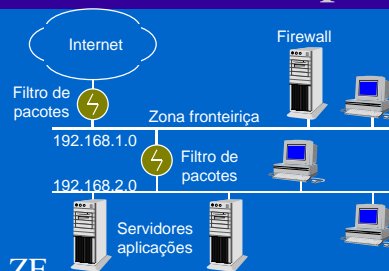
28-11-1999 António Costa - DEI/ISEP 27

## Filtro de Pacotes - Exemplo

- **Rede com 2 subredes**

- Rede 1 como fronteira (ZF)
- Rede 2 protegida
- Regras possíveis:

- Permitir tráfego interno para a ZF
- Permitir que serviços da rede interna cheguem ao *firewall*
- Permitir ligações da ZF de portas TCP entre 1024 e 5000
- Impedir ICMP para a rede interna a partir do exterior (*ping's e traceroute's*)
- Impedir acessos Telnet da rede 10.15.29.0



28-11-1999 António Costa - DEI/ISEP 28

## Filtro de Pacotes - Exemplo

- Política “por omissão aceita”
- Mais de 65 regras TCP, UDP, IP e ICMP

### Pacotes bloqueados - dentro para fora

Origem	Protocolo	Porta	Destino	Comentário
interface interno	ICMP		interface externo	<i>spoofing</i>
interface interno	TCP	25	interface externo	<i>SMTP</i>
interface interno	UDP	67	interface externo	
interface interno	UDP	69	interface externo	
interface interno	TCP	111	interface externo	<i>NFS</i>
interface interno	UDP	111	interface externo	<i>NFS</i>
interface interno	UDP	161	interface externo	
interface interno	UDP	162	interface externo	
interface interno	TCP	177	interface externo	<i>xdmcp</i>
interface interno	TCP	515	interface externo	
interface interno	TCP	1024-65535	interface externo	<i>spoofing</i>
interface interno	UDP	1024-65535	interface externo	<i>spoofing</i>

28-11-1999 António Costa - DEI/ISEP 29

## Firewall

- **Filtro de pacotes**
  - Controla eficientemente tráfego de rede
  - Não exige alterações às aplicações instaladas
  - Sobrecarrega a máquina de filtro de pacotes
  - Não permite implementar segurança elevada
  - Protocolos tipo UDP e RPC são vulneráveis
  - Auditoria tem de ser implementada à parte

- **Solução**

**Firewall**

28-11-1999 António Costa - DEI/ISEP 30

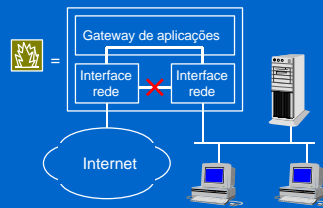
## Firewall

- Proteger uma rede de outra rede
- Filtragem ao nível de aplicação (Filtragem ao nível de rede - pacotes)
- Melhor meio de implementar segurança
  - Mecanismos de autenticação
  - Aumento de confidencialidade
  - Rigor na implementação
- Vários tipos de *firewall*

28-11-1999 António Costa - DEI/ISEP 31

## Firewall - Dual Homed

- *Routing* desactivado
- Isolamento de tráfego
- Transferência entre redes
  - Agentes *gateway de aplicações*  
Software especial para transferir dados de aplicação
  - Acesso ao exterior  
Através de *login* especial no *firewall*
- Política “**por omissão proíbe**”
- *Firewall* é uma zona de risco

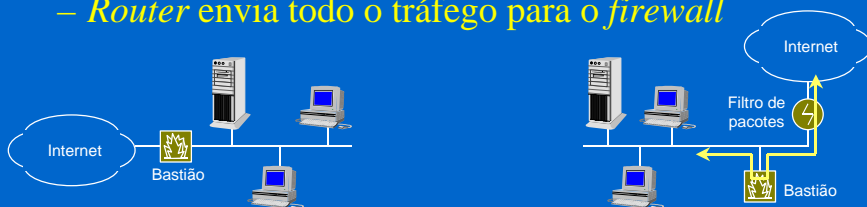


28-11-1999 António Costa - DEI/ISEP 32



## Firewall - Bastião

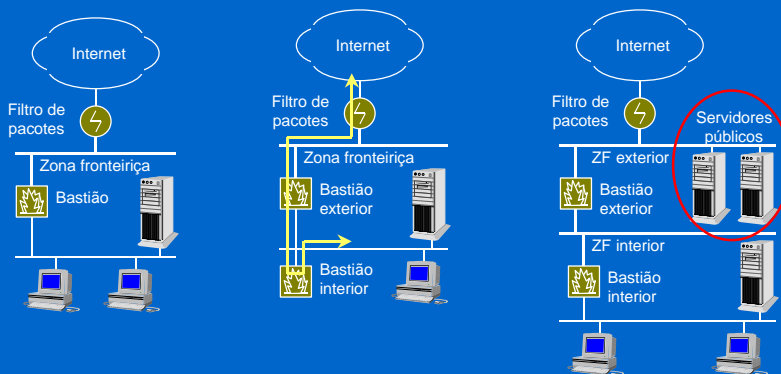
- Essencial para a segurança da rede
- Auditoria permanente
- Adição de Filtro de Pacotes
  - Configuração *Screened Host*
  - Firewall só com um interface de rede
  - Router envia todo o tráfego para o firewall



28-11-1999 António Costa - DEI/ISEP 33

## Firewall - Bastiões

- Maior segurança
- Impossível contornar os bastiões



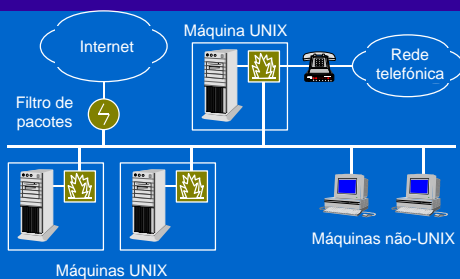
28-11-1999 António Costa - DEI/ISEP 34

## Firewall - Dificuldades

- **Uso de gateways de aplicações**
  - Certos serviços são complicados (FTP)
  - Não há transparência para os utilizadores
  - Exige versões especiais de aplicações
- **Conhecimentos técnicos elevados**
  - Implementação é complicada
  - Verificação é fundamental
- **Firewalls comerciais são caros!**

28-11-1999 António Costa - DEI/ISEP 35

## A rede do DEI



- Filtro de Pacotes com mais de 65 regras
- *Firewalls* software em cada máquina UNIX
- Acesso Telnet exterior através de OTP (*S/Key*)
- Auditoria permanente e redundante
- Monitorização *online* de certas máquinas

28-11-1999 António Costa - DEI/ISEP 36

## Recomendações

- **Essencial ter uma política de segurança**
- **Essencial fazer controlo de acesso**
- **Há muitas soluções baratas**
  - *Router + PC/Linux com mascarada + rede interna*
  - *Router + PC/Windows + software + rede interna*
  - *Boa solução para pequenas organizações*
  - *Rede interna invisível no exterior*
  - *Segurança elevada em ambos os sentidos*
- **Muito software *freeware* disponível**

28-11-1999 António Costa - DEI/ISEP 37