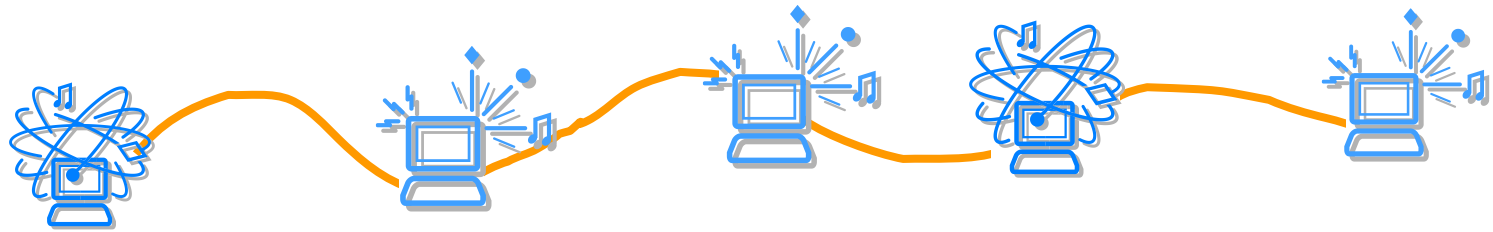
# Segurança em Redes

## Factos sobre segurança



Redes de Comunicação de Dados

Departamento de Engenharia da Eletrónica e das Telecomunicações e de Computadores


**Instituto Superior de Engenharia de Lisboa**

**Polytechnical University of Lisbon (IPL)**

POLITÉCNICO DE LISBOA

# Objectivo

- Abordar de forma estruturada e integrada a arquitetura de redes, os protocolos e respetivo impacto na segurança.

- Fornecer os conceitos essenciais  ao entendimento das tecnologias vigentes e à fácil evolução nas futuras.

- Identificar e estudar, quer do ponto de vista do atacante, quer do utilizador, os pontos críticos e as soluções possíveis para o incremento da segurança através da análise das vulnerabilidades, ameaças e tipos de ataques a sistemas de comunicação.

- Permitir a escolha consciente da politica de segurança mais adequada a cada situação.

# Programa resumido

- Factos sobre segurança.
- Ameaças, vulnerabilidades e ataques.
- Criptografia (cifras simétrica e assimétrica, certificados digitais, assinaturas digitais, distribuição de chaves e autoridades de certificação).
- Segurança em acessos dial-in (controlo de acessos - 802.1x, RADIUS, suporte de VPN - PPTP, L2TP).
- Segurança das comunicações ao nível das várias camadas do modelo OSI (IPsec, IKEv2, SSL/TLS, SSH).
- Segurança nos serviços de *email* e Web.
- Segurança em redes sem fios (WLAN).
- Segurança na gestão de redes.
- Práticas de segurança: *routers*, *firewalls*, IDS e armadilhas.
- Políticas de segurança.

# Boas razões para frequentar esta disciplina

- #1 Pressão do mercado: A segurança em computadores é um negócio em expansão; existe um crescimento constante da necessidade de pessoas que saibam como proteger os recursos vitais em informática.

- #2 Curiosidade intelectual: É um desafio e dá algum "gozo" aprender e praticar segurança em informática. Afinal desde criança que jogamos ao "gato e ao rato" e aos "polícias e aos ladrões".

- #3 Falta de alternativa: Razão "aceitável" - frequentar Segurança em Redes de Computadores devido a não haver alternativa mais interessante nas disciplinas de opção deste semestre.

# Más razões para frequentarem esta disciplina

- Pretende escrever o "último grito" de "*malware*" e testá-lo nos "vizinhos".

- Pretende contribuir activamente de maneira a demonstrar quão inseguro os sistemas operativos e as redes podem ser, praticando em sistemas em exploração que não os seus.

- Pretende testar a segurança da rede do ISEL/IPL e/ou da empresa onde trabalha (ou vai trabalhar) e não pertence à equipa responsável por essa tarefa.

**"Asneirada" nesta área dão normalmente penas de prisão.**

# Princípio a ter em conta

"A arte da guerra ensina-nos a confiar não na probabilidade do inimigo não vir, mas na nossa própria prontidão para o receber; não na possibilidade dele não atacar, mas no facto de termos tornado a nossa posição inatacável."

*"A arte da guerra",* Sun Tzu [general chinês (perito em estratégia militar) que viveu no século 6º antes de Cristo]

# Segurança: É um assunto assim tão importante?

- Não é um problema novo.
- Não é apenas um invenção dos jornais.
- Não é assunto apenas para “cientistas de foguetões”.
- É um assunto que muitos afirmam praticar, mas que poucos dominam.
- No entanto, como profissionais, a falha no entendimento e na implementação de um política de segurança adequada pode “assombrar” a reputação profissional e levar à responsabilização por danos e perdas.

# Há muita gente a dedicar-se à segurança

- Existem muitas entidades a preocuparem-se com a segurança. Destas um grande número são **entidades governamentais**, muitas delas norte-americanas, ou subsidiadas pelo governo americano:
  - http://www.nist.gov/
  - http://www.nsa.gov
  - http://www.cert.org/
- Mas também existem muita **empresas** interessadas na $egurança:
  - http://www.verisign.com/
  - http://www.sans.org/
  - http://www.mcafee.com/us/default.asp
  - www.rsa.com
  - http://informationsecurity.techtarget.com/
  - http://www.cisecurity.org/index.html

# Há muita gente a dedicar-se à segurança (cont.)

- Existem, sobretudo, cada vez mais **universidades e outras instituições de ensino e investigação** envolvidas ou a envolverem-se nestes assuntos. Umas pelo desafio académico envolvido, outras porque, para além deste, é um assunto cada mais intere$$ante; afinal os alunos precisam de empregos motivadore$:

  - http://www.cs.auckland.ac.nz/~pgut001/
  - http://www.deetc.isel.ipl.pt (a semente está lançada, espero que germine e cresça... ;-) )
  - Muitas outras (a minha lista de favoritos no *browser* está cada vez maior ....)

- E muitos **privados** que se interessam pelo assunto:

  - http://www.hak5.org/

# As vítimas habituais

Quem são as vítimas “habituais”?

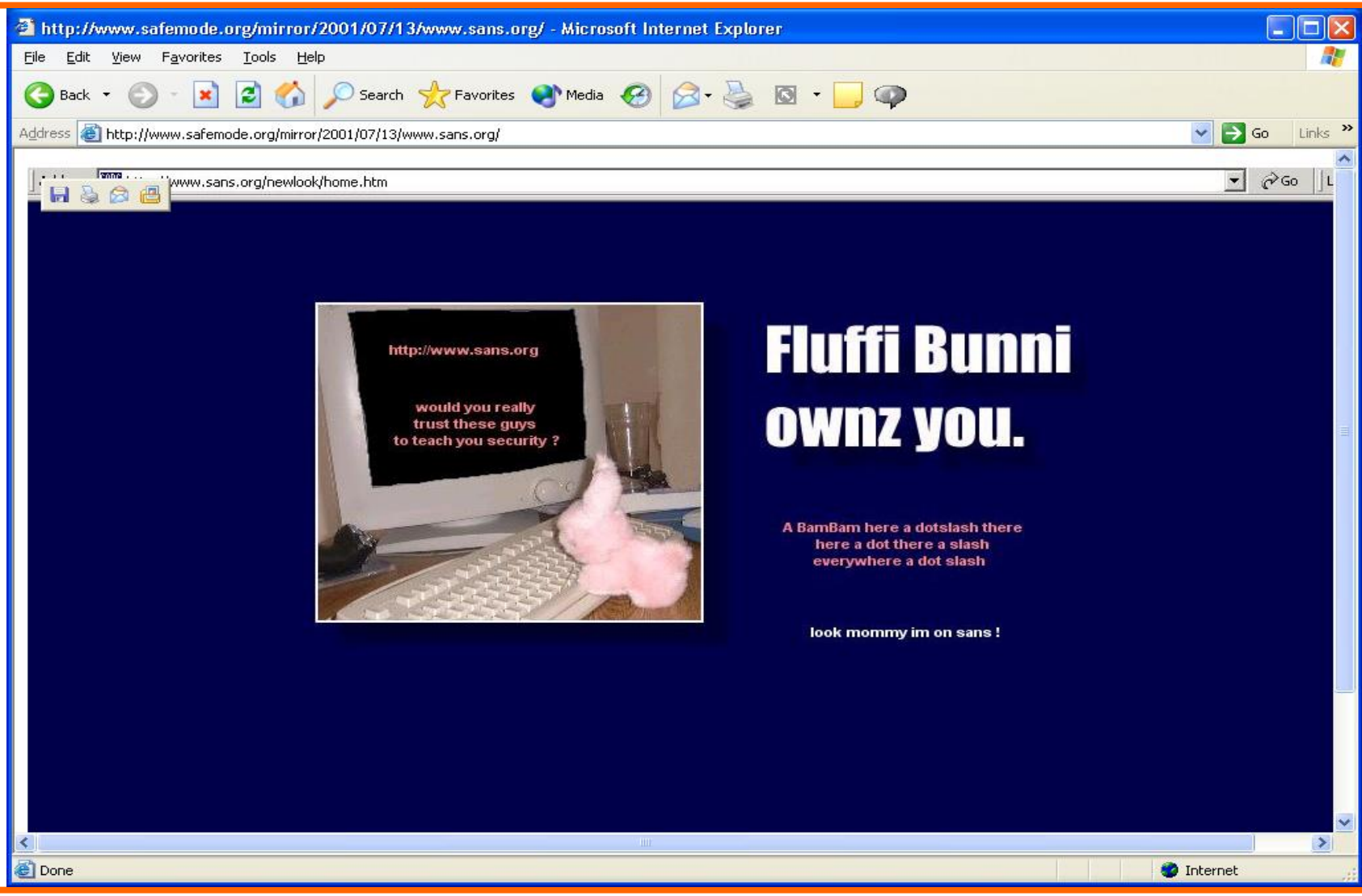
- Nós;
- O banco no qual temos algum do nosso “*plim plim*”, ou não;
- A empresa onde trabalhamos (o caso é ainda mais negro se formos nós os responsáveis pela segurança e a coisa der mesmo para o torto);
- Qualquer um.

Exemplo:

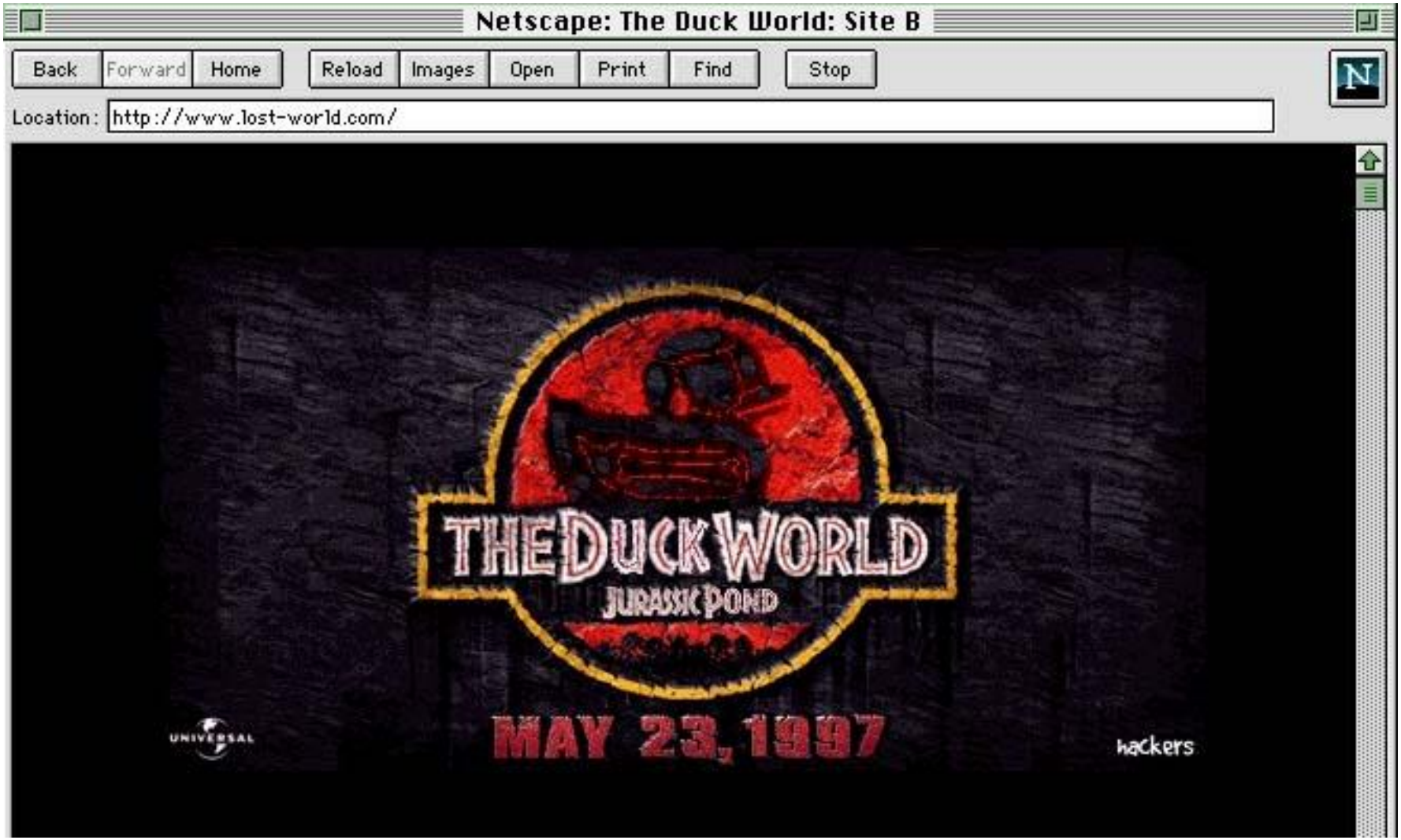
millenniumbcp.pt/site/conteudos/segur/article.jhtml?articleID=351112

Neste caso as vítimas foram os clientes duma instituição bancária a qual, numa atitude inteligente, denunciou e publicitou o caso quando teve conhecimento dele.

# Mas, mesmo os ditos "especialistas" são "infiltrados"
# Instituto SANS – *hacked* !



# E os não especialistas também…
# Universal Studios - *Hacked*



# “Banha da cobra” nos Media

- Os artigos das revistas não são o melhor para se aferir da qualidade da segurança do software, por exemplo o “**WinXFiles**” (programa de cifrar ficheiros facilmente “quebrado”, com um algoritmo fraco):
  - “*PC Answers*”: Listado nos “10 programas com segurança comprovada”
  - “*Windows News*”: Listado nos “75 melhores utilidades para Windows”
  - “*FileMine*”: Cotado como um “Featured Jewel”
  - “*Shareware Junkies*”: 5 estrêlas, “*a must have for anyone sharing a computer with files they want to keep private*”
  - “*PC Format*”: “*Unbeatable and excellent file encryption*”
  - “*TUCOWS*”: Cotado com “4 vacas”
  - “*Ziff-Davis Interactive*”: 5 estrêlas, “*keeps files and data on your PC as safe as if they were under lock and key*”

# “Banha da cobra” nos Media (cont.)

  - “*The Windows95 Application List*”: “*an excellent application for protecting your personal files*”
  - “*RocketDownload*”: Quatro sorrisos
  - “*Simply the Best*”: Prémio

- Uma revista importante classificou um conjunto de programas de cifra pela qualidade da interface com os utilizadores (!!!!!!) ☺.

# O que é Segurança?

- **Segurança**
  - Manter qualquer coisa (informação no nosso caso) segura contra:

    roubo | alteração | destruição | falsificação

# Quatro passos para melhorar a segurança

| | Description |
|---|---|
| 1 | **Prevention**<br>To avoid a security problem in the first place by removing possible vulnerabilities and reducing resource visibility. |
| 2 | **Detection**<br>Comparing what has been deemed acceptable by an organization's policy guidelines with what is actually observed, and executing a notification process so that security personnel realize the inconsistency exists. |
| 3 | **Forensics**<br>Gathering information after a security violation has been detected to form the basis for a response. |
| 4 | **Response**<br>Responding to a detected security breach in a manner which is consistent with the organizational guidelines. |

# “O segredo é a alma do negócio”

Em segurança informática **não é bem assim**.

- Em criptografia assume-se que o que torna um cifra boa não é ocultar o algoritmo utilizado, mas apenas as chaves utilizadas na cifra, ou algumas delas. A confiança numa cifra nasce da sua exposição à comunidade em geral e do seu estudo e teste generalizado.

[Principio de **Kerckhoffs**]

# Principio de Kerckhoffs

**“Um criptosistema deve manter-se seguro mesmo que tudo acerca do sistema, exceto a chave, seja do conhecimento público”.**

- Claude Shannon e Bruce Schneier refinaram o principio de Kerckhoffs com o objetivo de promover a “segurança através da transparência”. Pode-se resumir assim: **“Quanto menor e mais simples forem as coisas que são necessárias manter secretas de forma a garantir a segurança de um sistema, mais fácil será garantir essa segurança.”**

  – A chave é a coisa mais simples num sistema de garantir o secretismo.

# Segurança de informação

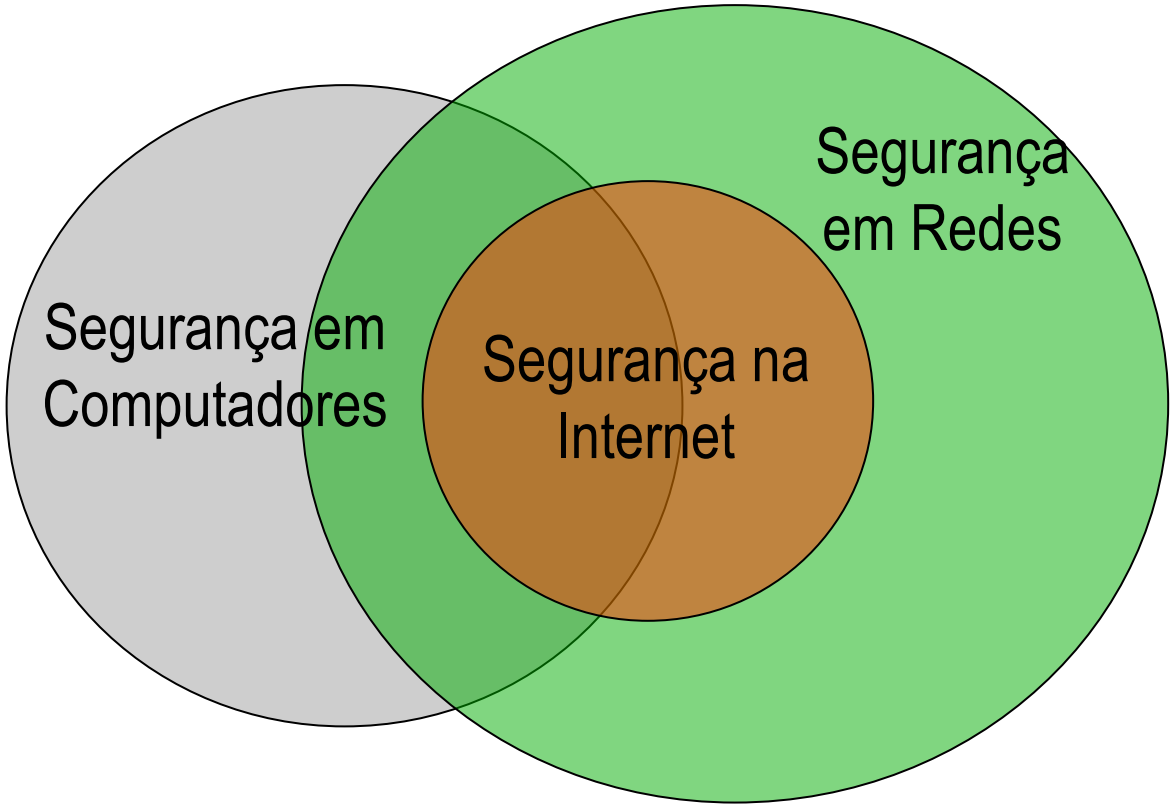
- **Segurança em computadores** envolve prevenir, detectar e responder a acções não autorizadas num sistema de computadores.

- **Segurança em redes** significa a mesma coisa para um grupo de computadores interligados em rede.

- **Segurança na Internet** significa … "maior confusão com os termos anteriores".

Para se perceber sobre Segurança em Redes há necessidade de se investir também na Segurança em Computadores. Não existem "atalhos" que permitam contornar esta necessidade.

# Áreas da Segurança



# Segurança absoluta (???)

**Toda a segurança é relativa**, deve ser implementada por níveis e deve ser um equilíbrio entre:

- Custo da segurança **vs** valor do património a proteger
- Ameaças prováveis **vs** ameaças possíveis
- Necessidade de segurança **vs** necessidades do negócio

# Arquitectura de Segurança OSI

- A recomendação **X.800**, "*Security Architecture for OSI*", define uma aproximação sistemática possível para os gestores organizarem a segurança. Define muitos dos conceitos abstractos que utilizamos em Segurança.
- Mas existem muitas outras fontes que se complementam, como, por exemplo, os **RFC 2196 e 2828**:

**Ameaça**

**Um potencial para a violação da segurança, o qual existe quando se dá uma circunstância, capacidade, ação ou evento que possa quebrar a segurança e causar danos. Isto é, uma ameaça é um perigo possível que pode explorar uma vulnerabilidade.**

**Ataque**

**Um assalto à segurança dum sistema que derive duma ameaça inteligente; isto é, um acto inteligente que seja uma tentativa deliberada (especialmente no sentido dum método ou duma técnica) para contornar os serviços de segurança e violar a política de segurança dum sistema.**

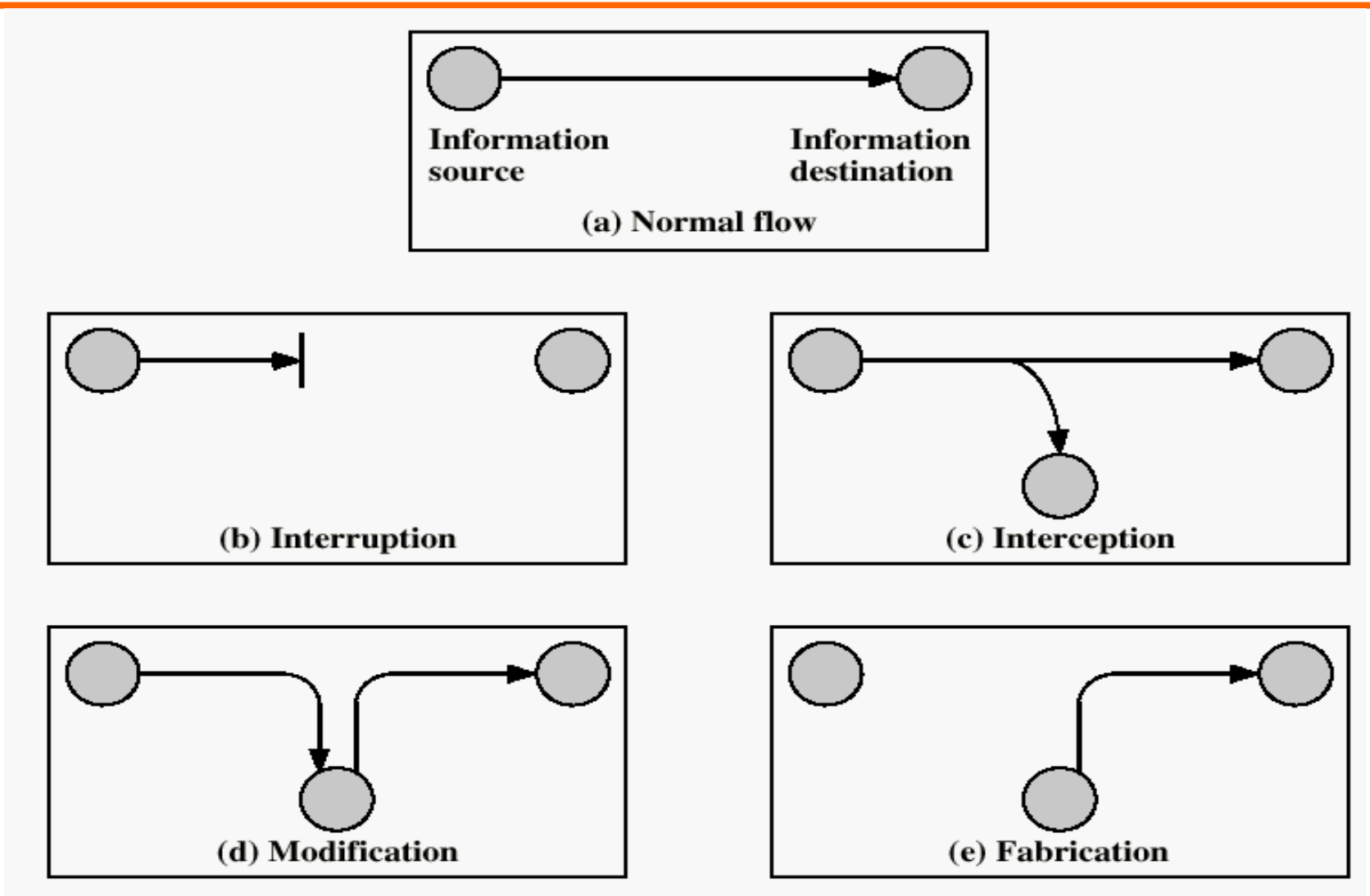
# Arquitectura de segurança

- **Ataque à segurança** (Ameaça)
  - Qualquer acção que comprometa a segurança da informação ou do sistema.

- **Mecanismo de segurança**
  - Um mecanismo projectado para detectar, prevenir ou recuperar de um ataque à segurança.

- **Serviço de segurança**
  - Serviço destinado a melhorar a segurança dos sistemas de processamento de dados e da transferência de informação de uma organização. Os serviços têm como intenção melhorar a resistência a ataques através da utilização de um ou mais mecanismos de segurança para providenciarem o serviço.

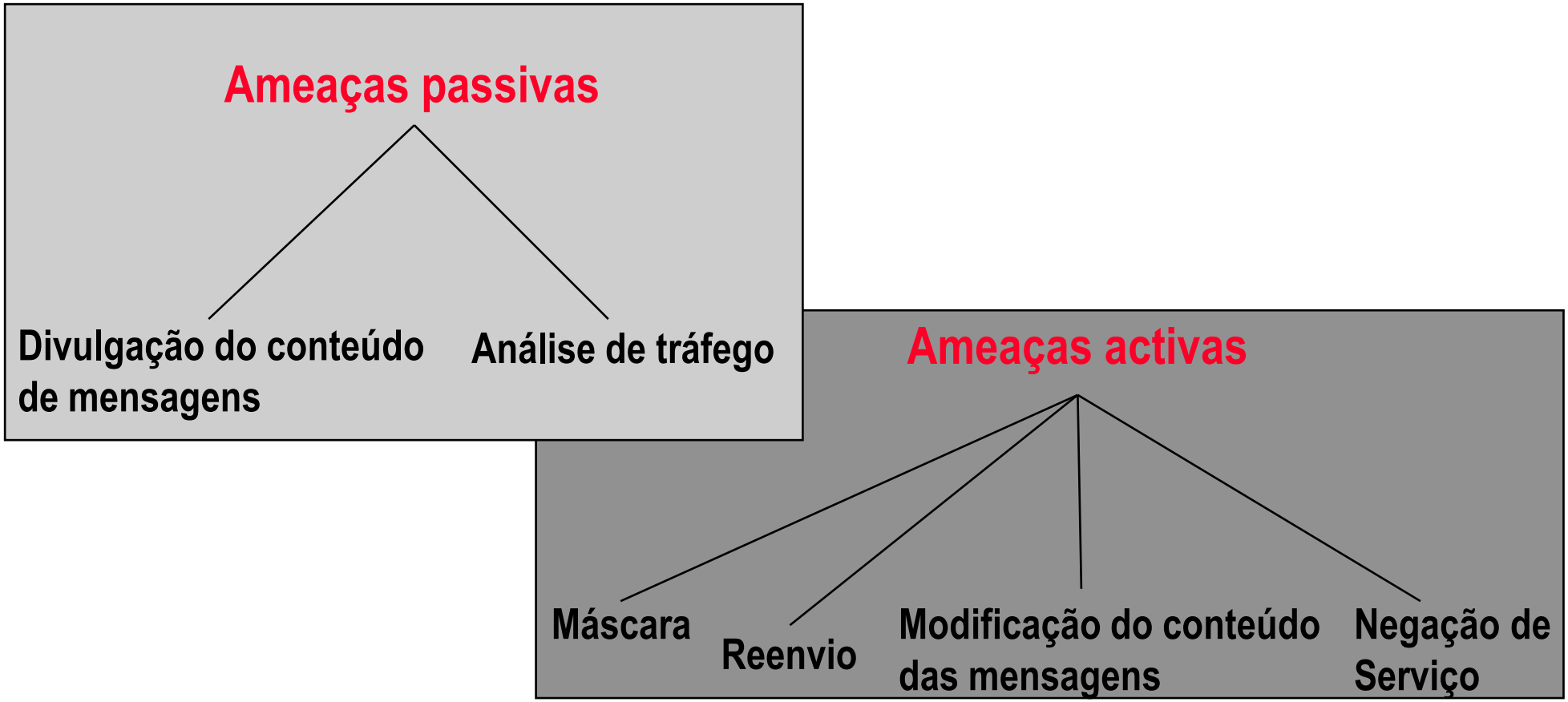
# Ataques à Segurança



# Ataques à Segurança

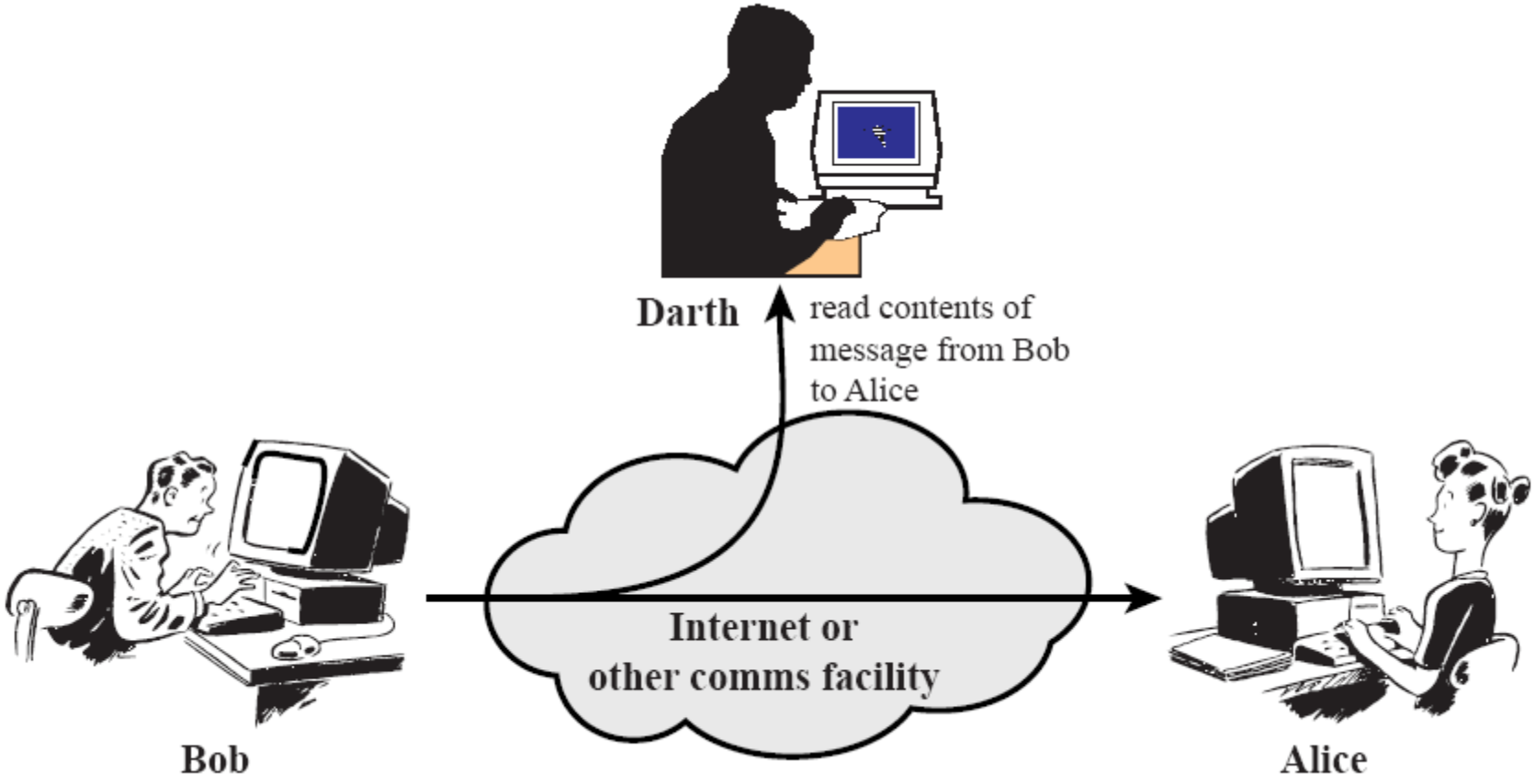
- **Interrupção:** Ataque à disponibilidade
- **Intercepção:** Ataque à confidencialidade.
- **Modificação:** Ataque à integridade.
- **Fabricação:** Ataque à autenticidade.

# Ameaças passivas e ativas à segurança



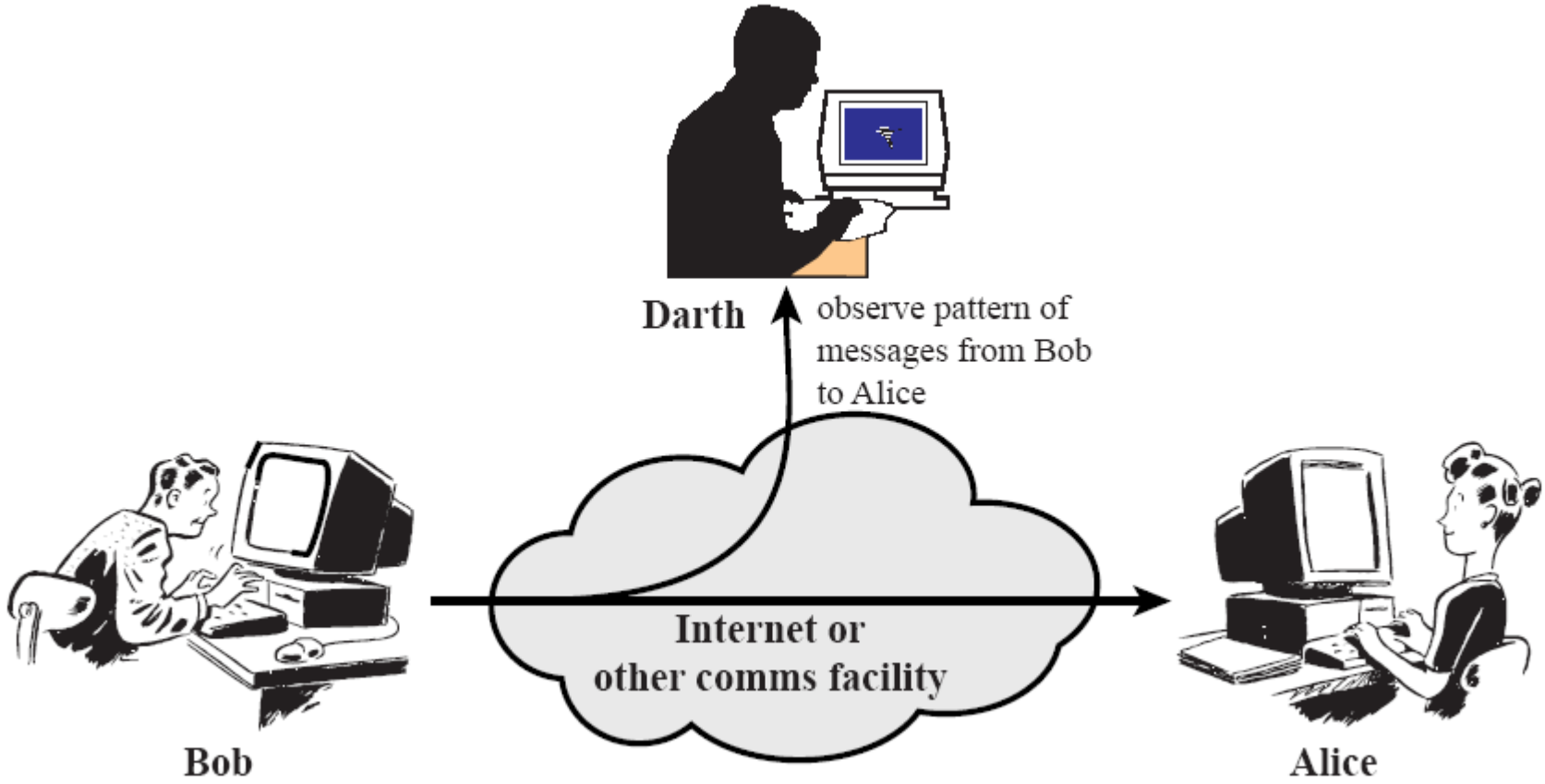
# Ameaças passivas

## (Divulgação do conteúdo de mensagens)

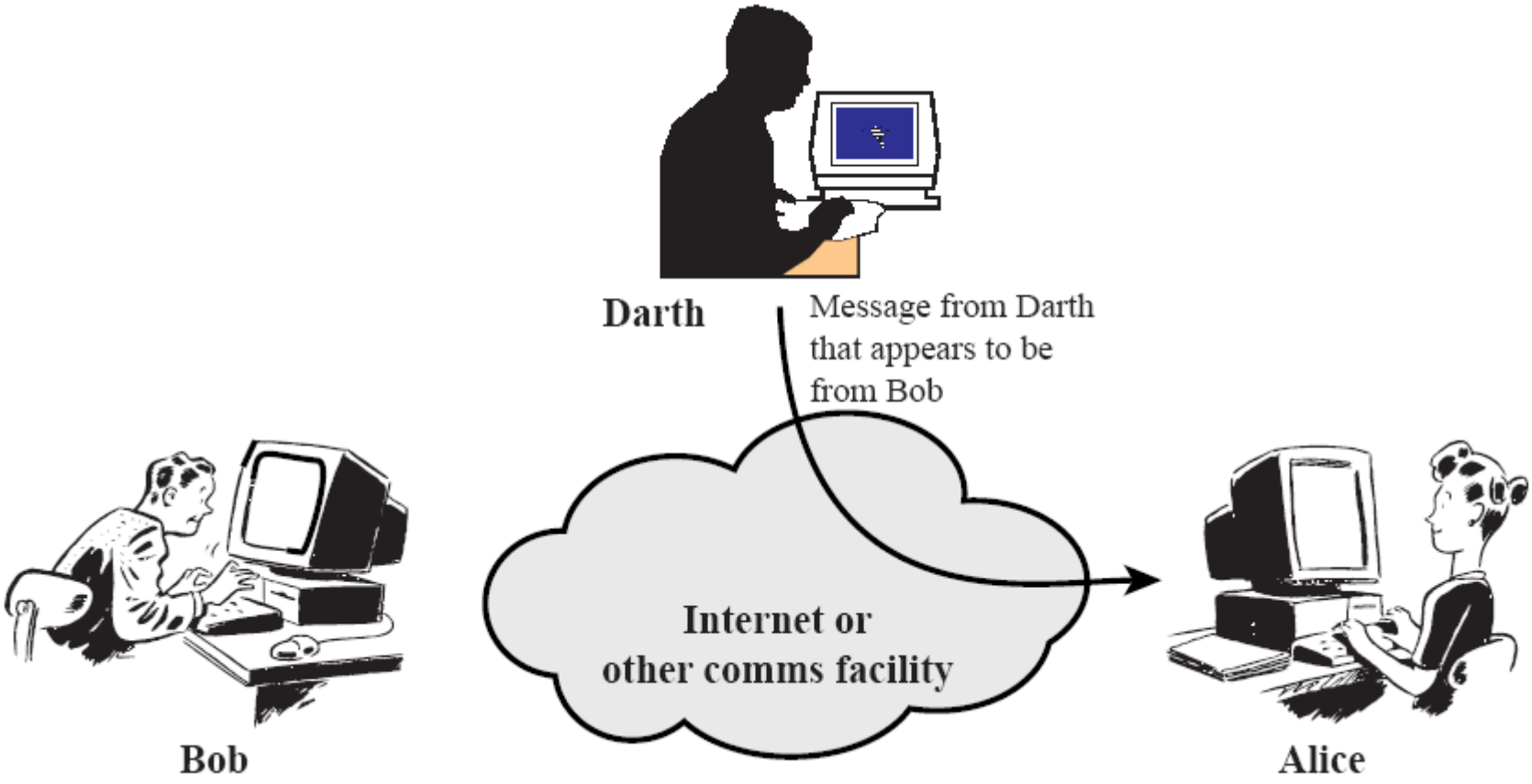


# Ameaças passivas

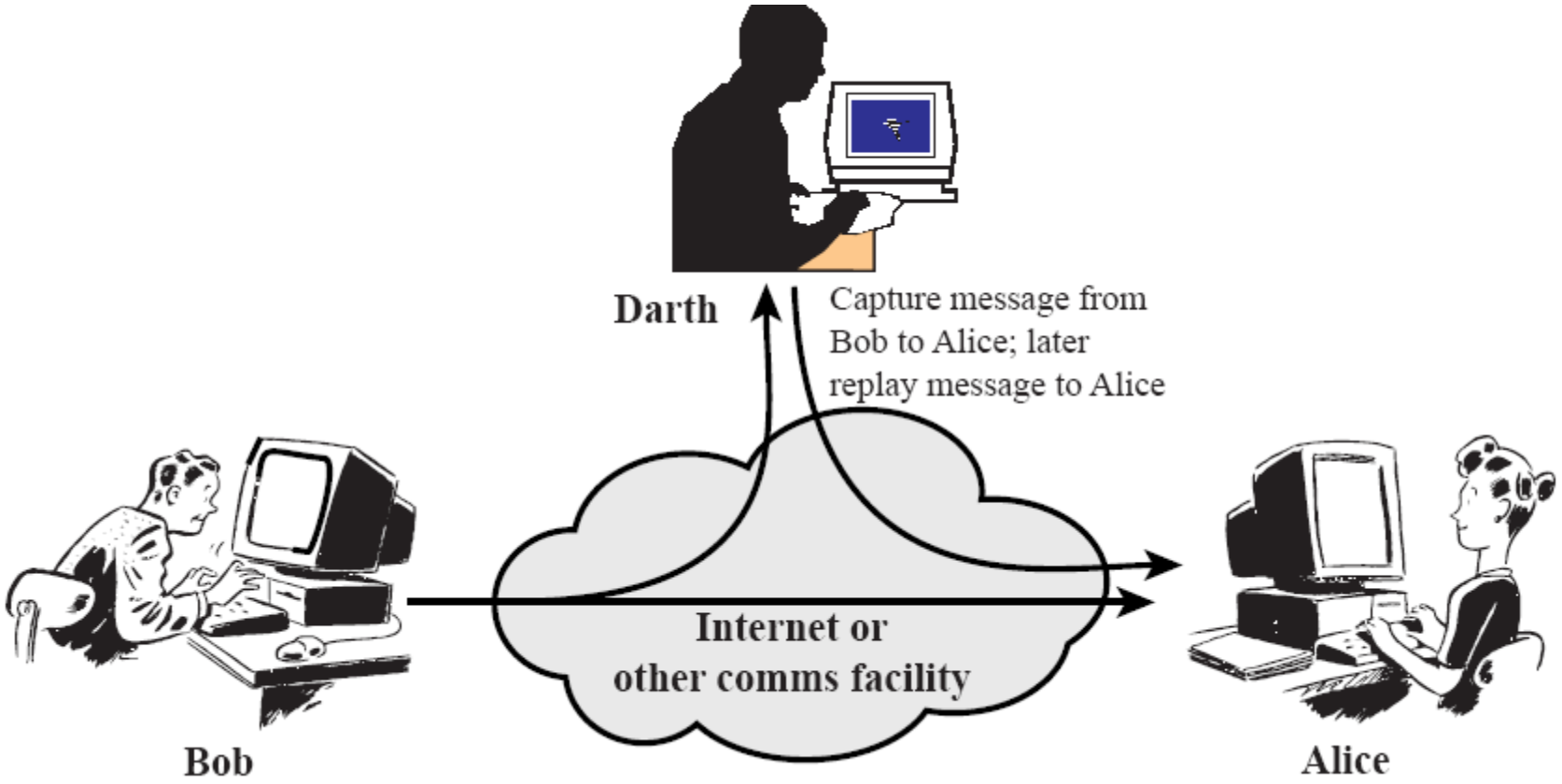
## (Análise de tráfego)



# Ameaças ativas
## (Máscara)

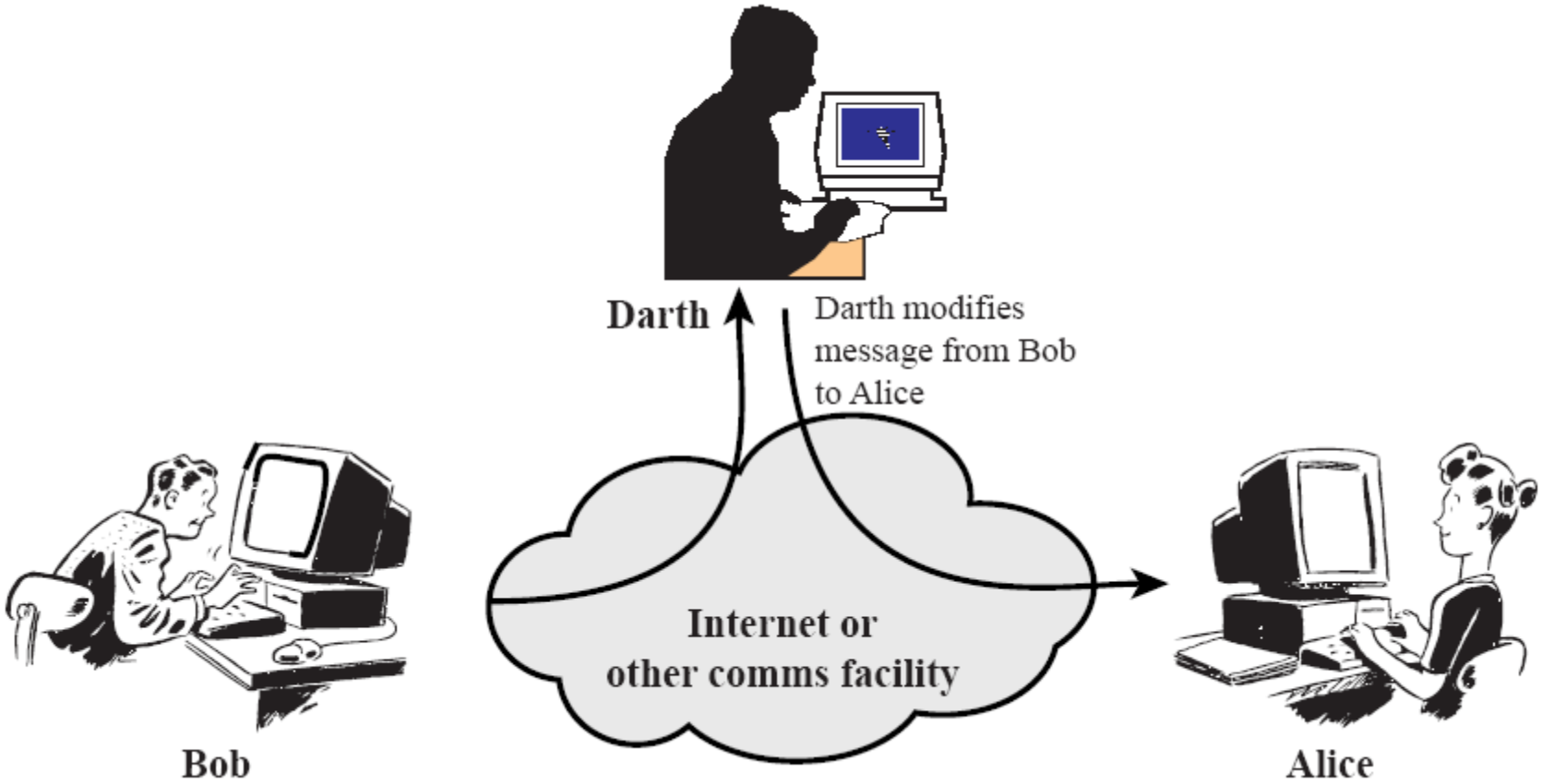


# Ameaças ativas
## (Reenvio)

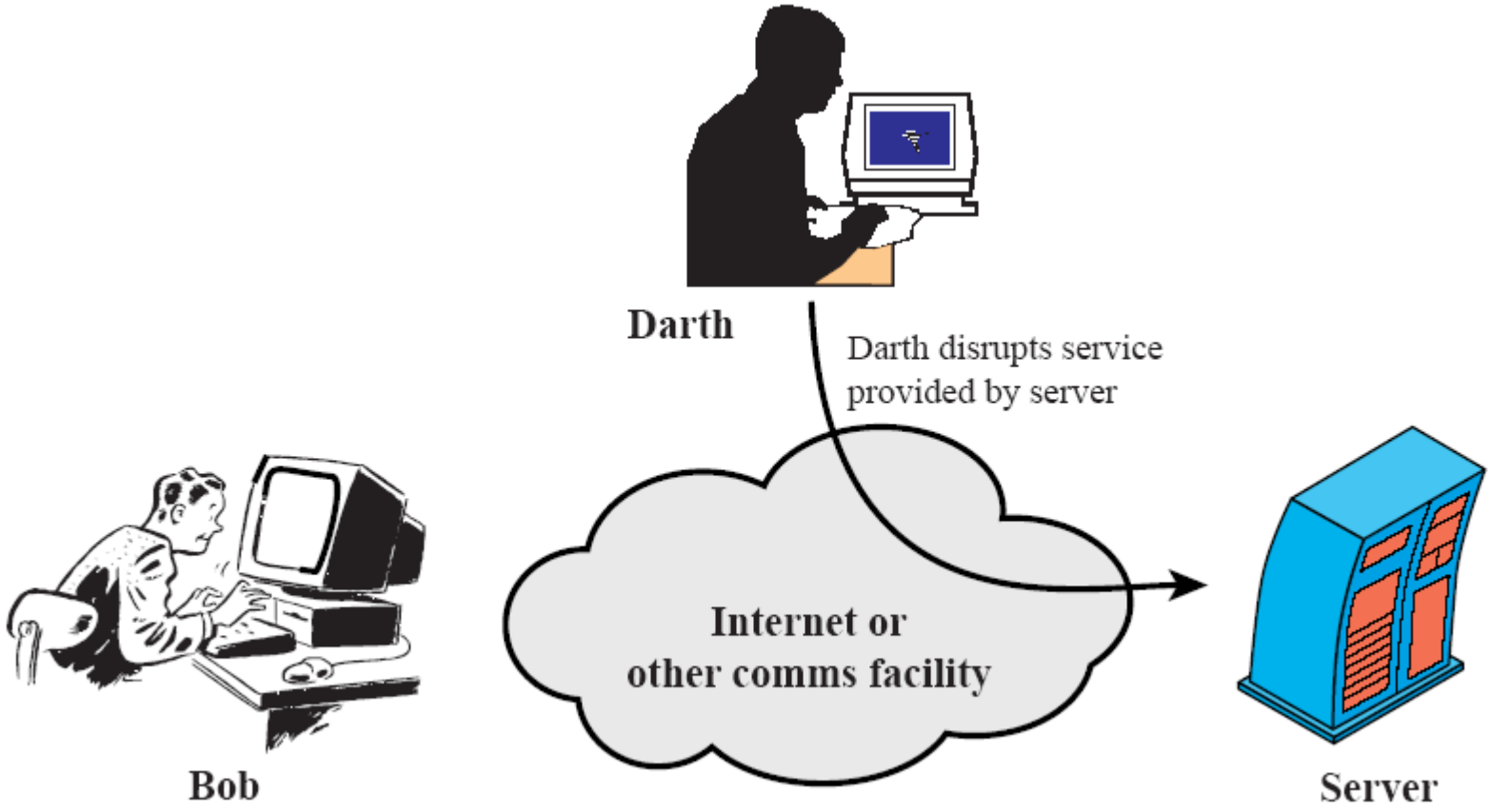


# Ameaças ativas

## (Modificação do conteúdo das mensagens)



# Ameaças ativas
## (Negação de serviço)



# Mecanismos de segurança (X.800)

- **Mecanismos de segurança específicos**

  Podem ser incorporados na camada de protocolo apropriada de maneira a fornecer alguns dos serviços de segurança OSI

  - **Cifragem/encriptação**
  - **Assinatura digital**
  - **Controlo de acessos**
  - **Integridade de dados**
  - **Troca de autenticação/certificação**
  - ***Traffic padding***
  - **Controlo de encaminhamento**
  - **"Notarização"** (Integrity, origin and/or destination of data can be guaranteed by using a 3rd party trusted notary.
    - Notary typically applies a cryptographic transformation to the data.)

# Mecanismos de segurança

- **Cifra**
  - Transformação reversível dos dados por forma a torná-los confusos
  - Desencriptação (ou decifragem) - operação inversa da encriptação

- **Assinatura digital**
  - Bloco de texto gerado através de um algoritmo de cifra / *Hash* aplicado ao documento e enviado cifrado com a chave privada do emissor.
  - O receptor verifica a validade da assinatura aplicando o mesmo algoritmo com a chave pública do emissor.

# Mecanismos de segurança

- **Controlo de acessos**
  - Conjunto muito variado de mecanismos de autenticação e controlo de acesso a recursos (*passwords, smart cards,* sistemas biométricos, listas de acesso, *firewalls)*

- **Garantia de integridade**
  - Adição pelo emissor de dados redundantes à informação (ex. *checksum*) por forma a possibilitar a verificação da sua integridade pelo receptor

# Mecanismos de segurança

- **Certificação**
  - Envolvimento de uma terceira entidade (Autoridade de Certificação) da confiança do emissor e do receptor na certificação da informação (*trusted third-party*)
  - Usado na garantia de integridade de documentos e na autenticação de utilizadores

# Mecanismos de segurança (X.800)

- **Outros mecanismos de segurança**

  Mecanismos que não são específicos de qualquer serviço de segurança OSI em particular ou camada de protocolos

  - **Funcionalidade de confiança**
  - **Etiqueta de segurança**
  - **Deteção de eventos**
  - **Dados de auditorias de segurança**
  - **Recuperação de segurança**

# Pervasive Mechanisms

- Trusted functionality
  - Any functionality providing or accessing security mechanisms should be trustworthy.
  - May involve combination of software and hardware.
- Security labels
  - Any resource (e.g. stored data, processing power, communications bandwidth) may have security label associated with it to indicate security sensitivity.
  - Similarly labels may be associated with users. Labels may need to be securely bound to transferred data.

# Pervasive Mechanisms

- Event detection
  - Includes detection of
    - attempted security violations,
    - legitimate security-related activity.
  - Can be used to trigger event reporting (alarms), event logging, automated recovery.
- Security audit trail
  - Log of past security-related events.
  - Permits detection and investigation of past security breaches.
- Security recovery
  - Includes mechanisms to handle requests to recover from security failures.
  - May include immediate abort of operations, temporary invalidation of an entity, addition of entity to a blacklist

# Services versus mechanisms

- ISO 7498-2 indicates which mechanisms can be used to provide which services.
- Illustrative NOT definitive.
- Omissions include:
  - use of integrity mechanisms to help provide authentication services,
  - use of encipherment to help provide non-repudiation service (as part of notarisation).

# Serviços de segurança

- Existem várias definições do que se entende por “Serviços de segurança”. Quer o X.800 quer o RFC 2828 têm as suas próprias definições de serviço de segurança:

**X.800**
**“Serviço fornecido por uma camada dum protocolo OSI o qual assegura uma adequada segurança do sistema ou da transferência de dados.”**

**RFC 2828**
**“Um serviço de processamento ou de comunicações fornecido por um sistema para garantir um tipo especifico de protecção aos recursos do sistema; serviços de segurança implementam politicas de segurança e são implementadas por mecanismos de segurança.”**

# Security service classification

- ISO 7498-2 defines 5 main categories of security service:
  - Authentication (including entity authentication and origin authentication),
  - Access control,
  - Data confidentiality,
  - Data integrity,
  - Non-repudiation.

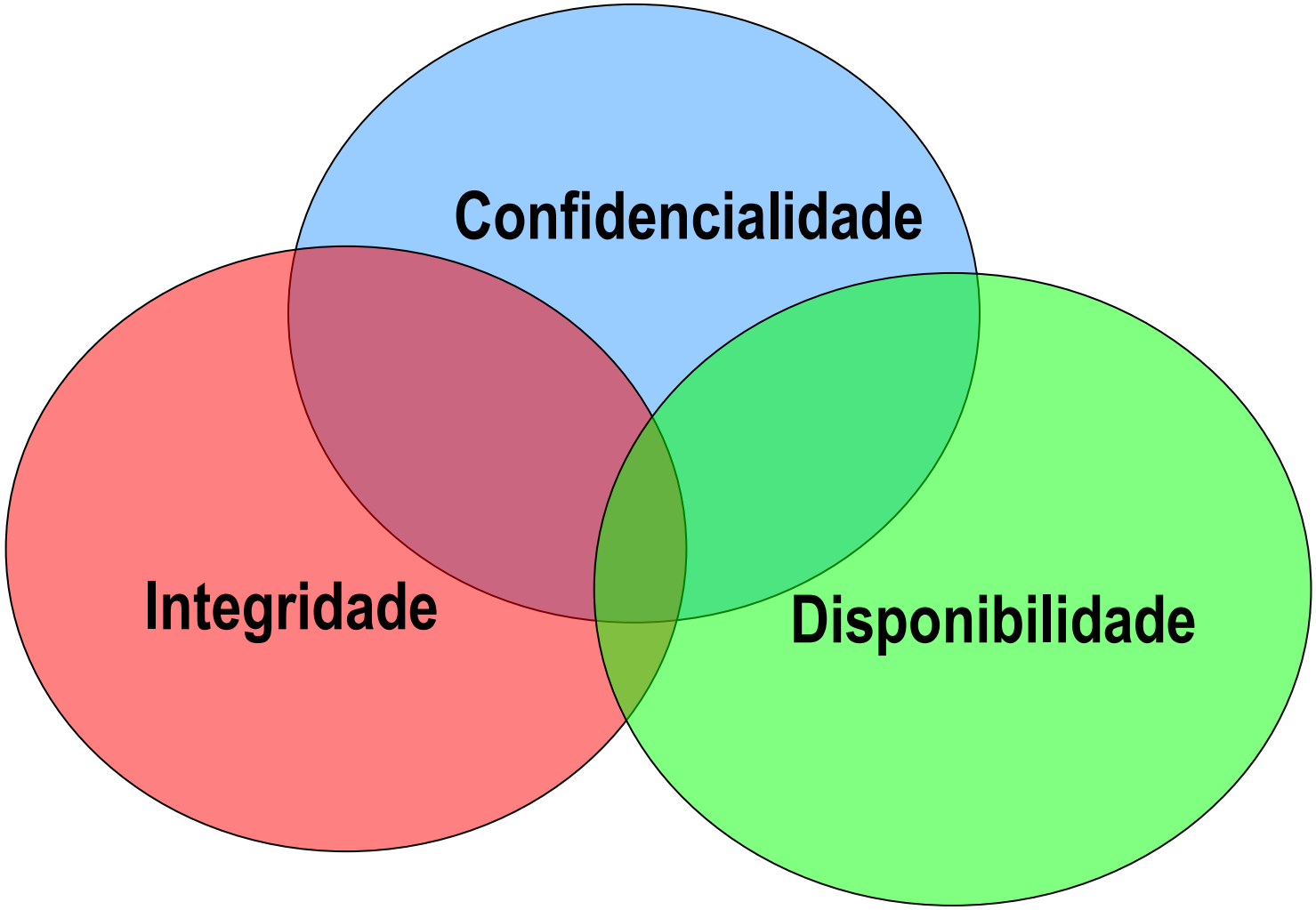
# Serviços de segurança

- **Confidencialidade**
  - A informação deve estar disponível apenas a quem tem direito de lhe aceder.
    - Ocultação da informação e dos recursos; “necessidade de saber”
    - Não dar a conhecer o conteúdo ou mesmo a existência
    - Controlo de acessos, criptografia
- **Integridade**
  - A informação deve ser modificada apenas por aqueles que a isso estão autorizados.
    - Prevenção de alterações impróprias ou não autorizadas
    - Integridade dos dados, autenticação (integridade da origem)
    - Prevenção: Bloqueio dos acessos não autorizados; Detecção: relatar o grau de confiança na integridade dos dados.

# Serviços de segurança

- **Disponibilidade**
  - A informação deve estar acessível àqueles a quem pertence quando dela necessitam.
    - Possibilidade de usar a informação ou o recurso desejado
    - Ataques de Negação de Serviço (*Denial of Service* (DoS))

# Serviços de segurança



# Serviços de segurança

- Além dos serviços definidos anteriormente podemos ainda considerar outros:
  - **Confidencialidade (privacidade)**
  - **Integridade (não foi alterado)**
  - **Autenticação (certeza sobre quem criou ou enviou os dados)**
  - **Não-repudiação (quem fez não pode dizer que não fez)**
  - **Controlo de acessos (prevenir o mau uso dos recursos)**
  - **Disponibilidade (permanência, não-apagamento)**
    - Ataques de negação de serviço
    - Vírus que apagam ficheiros

# Serviços de segurança – Confidencialidade dos dados

**Protecção dos dados contra revelação não autorizada**.

- **Confidencialidade da ligação**
  - Proteção dos dados dos utilizadores de uma ligação
- **Confidencialidade numa ligação não-orientada à ligação**
  - Proteção de todos os dados num simples do bloco de dados
- **Confidencialidade em campos selecionados**
  - Confidencialidade de alguns campos escolhidos nos dados do utilizador numa ligação ou num bloco de dados
- **Confidencialidade do fluxo de dados**
  - Protecção da informação que pode ser obtida pela observação dos fluxos de dados

# Serviços de segurança – Integridade dos dados

Assegurar que os dados recebidos estão exactamente como enviados pela outra parte (não foram modificados, inseridos, apagados ou reenviados)

- **Integridade da ligação com recuperação**
- **Integridade da ligação sem recuperação**
- **Integridade de campos seleccionados da ligação**
- **Integridade de uma ligação não-orientada à ligação**
- **Integridade de campos seleccionados numa ligação não-orientada à ligação**

# Serviços de segurança - Autenticação

Assegura que a entidade que comunica é mesmo quem diz ser.

- **Autenticação das entidades pares (*peer*)**
  - Utilizado em associação com uma ligação lógica para fornecer confiança na identidade das entidades ligadas.
- **Autenticação da origem dos dados**
  - Numa transferência não-orientada à ligação fornece a certeza da origem dos dados ser quem diz que é.

# Serviços de segurança – Não-repudiação

Fornece protecção contra a repudiação por parte de uma das entidades envolvidas numa comunicação, independentemente de ter participado em toda ou em parte da comunicação.

- **Não repudiação, origem**
- **Não repudiação, destino**

# Serviços de segurança – Controlo de acessos

**Prevenção do uso de recursos sem autorização** (controla quem pode ter acesso a um determinado recurso, em que condições o acesso pode ocorrer e o que é que aqueles que têm autorização para aceder aos recursos podem fazer).

# Serviços de segurança – Disponibilidade

**Garantir que os recursos estão disponíveis** para aqueles a quem pertencem sempre que são necessários.

O X.800 trata a disponibilidade como uma propriedade que pode ser associada a vários outros serviços de segurança.

# Relação entre serviços e mecanismos de segurança

| | Mechanism | | | | | | | |
|---|---|---|---|---|---|---|---|---|
| Service | Enciph-erment | Digital signature | Access control | Data integrity | Authenti-cation exchange | Traffic padding | Routing control | Notari-zation |
| Peer entity authentication | Y | Y | | | Y | | | |
| Data origin authentication | Y | Y | | | | | | |
| Access control | | | Y | | | | | |
| Confidentiality | Y | | | | | | Y | |
| Traffic flow confidentiality | Y | | | | | Y | Y | |
| Data integrity | Y | Y | | Y | | | | |
| Non-repudiation | | Y | | Y | | | | Y |
| Availability | | | | Y | Y | | | |

# Relação entre serviços de segurança e ataques

| | Attack | | | | | |
|---|---|---|---|---|---|---|
| Service | Release of message contents | Traffic analysis | Masquerade | Replay | Modification of messages | Denial of service |
| Peer entity authentication | | | Y | | | |
| Data origin authentication | | | Y | | | |
| Access control | | | Y | | | |
| Confidentiality | Y | | | | | |
| Traffic flow confidentiality | | Y | | | | |
| Data integrity | | | | Y | Y | |
| Non-repudiation | | | | | | |
| Availability | | | | | | Y |

# Services versus layers

- ISO 7498-2 lays down which security services can be provided in which of the 7 layers.
- Layers 1 and 2 may only provide confidentiality services.
- Layers 3/4 may provide many services.
- Layer 7 may provide all services.

# Service/layer table

| Service \ Layer | Layer 1 | Layer 2 | Layer 3 | Layer 4 | Layer 5/6 | Layer 7 |
|---|---|---|---|---|---|---|
| Entity authentication | | | Y | Y | | Y |
| Origin authentication | | | Y | Y | | Y |
| Access control | | | Y | Y | | Y |
| Connection confidentiality | Y | Y | Y | Y | | Y |
| Connectionless confidentiality | | Y | Y | Y | | Y |
| Selective field confidentiality | | | | | | Y |
| Traffic flow confidentiality | Y | | Y | | | Y |
| Connection integrity with recovery | | | | Y | | Y |
| Connection integrity without recovery | | | Y | Y | | Y |
| Selective field connection integrity | | | | | | Y |
| Connectionless integrity | | | Y | Y | | Y |
| Selective field connectionless integrity | | | | | | Y |
| Non-repudiation of origin | | | | | | Y |
| Non-repudiation of delivery | | | | | | Y |

# Tarefas básicas a ter em conta no projecto dum serviço de segurança

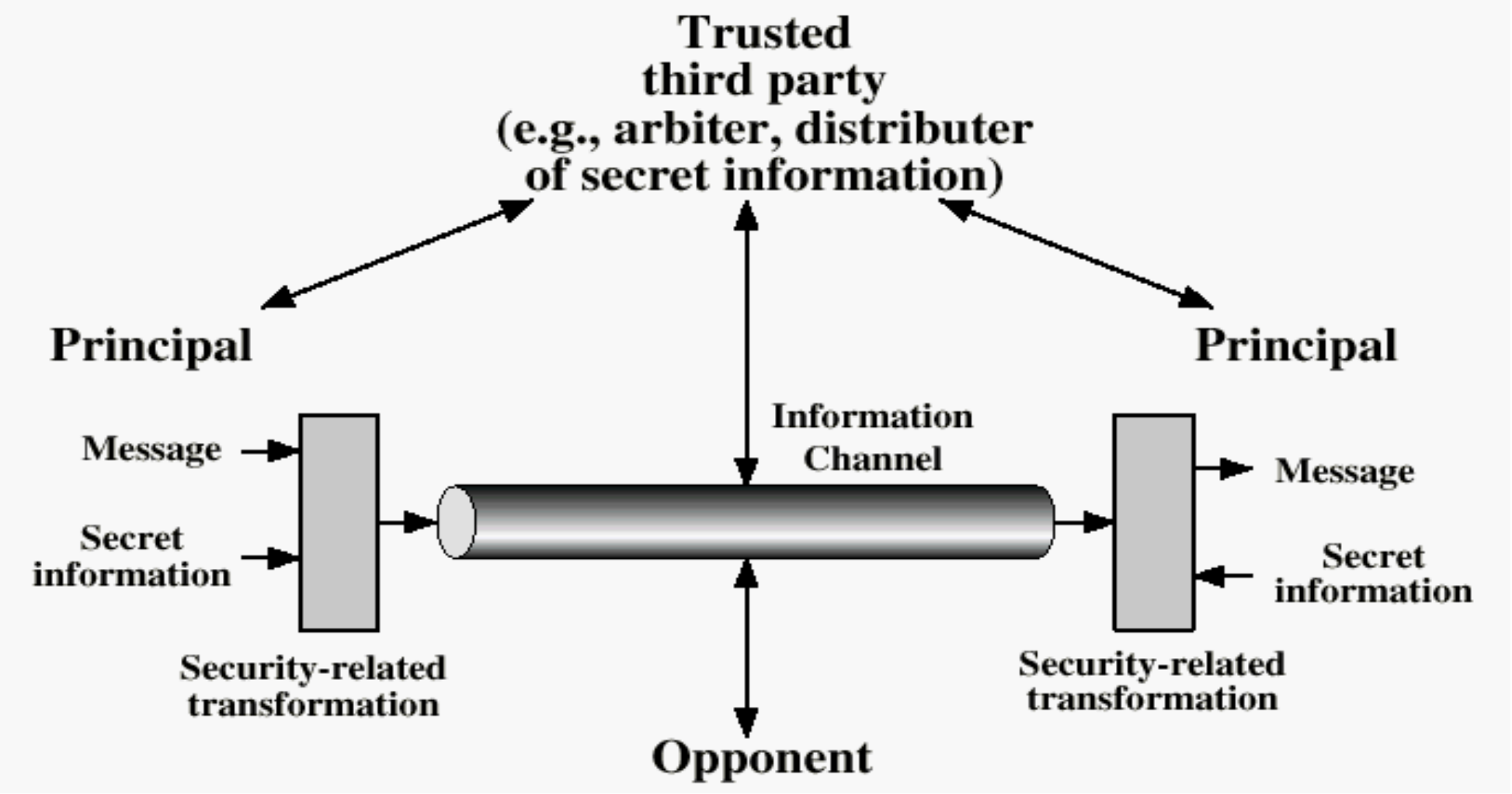
1. Projecto dum algoritmo para efectuar as transformações relacionadas com segurança. O algoritmo deve ser tal que os oponentes não consigam contrariar o seu objectivo.

2. Gerar a informação secreta a ser utilizada com o algoritmo.

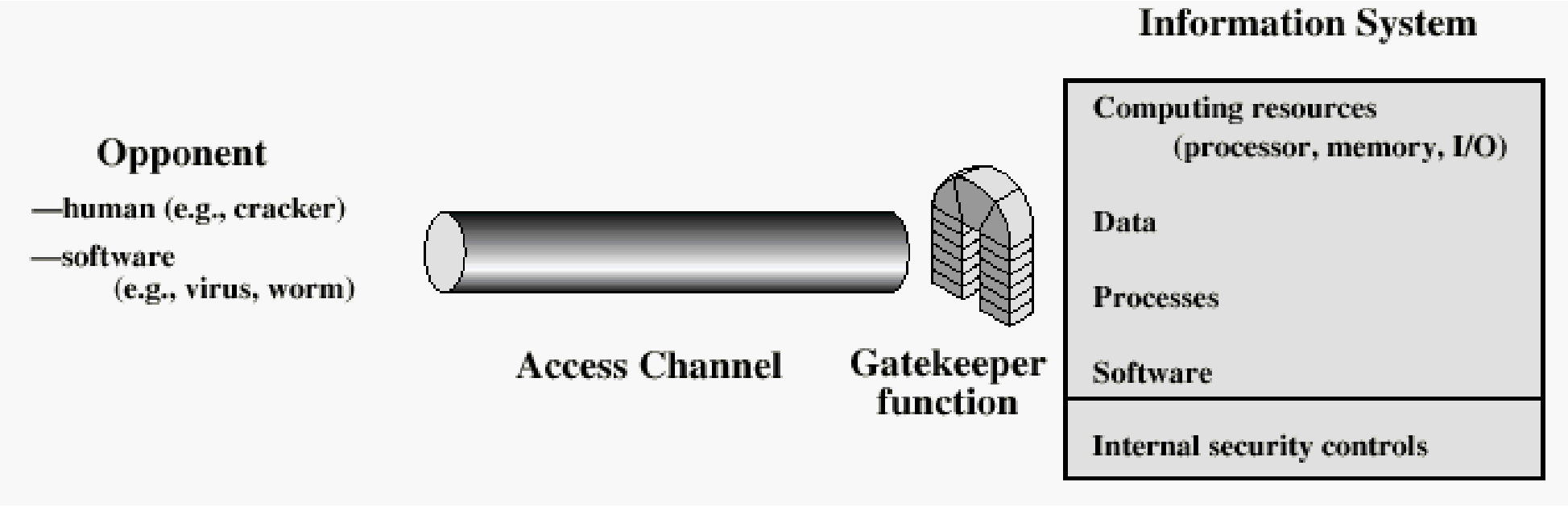
3. Desenvolver métodos para a distribuição e partilha da informação secreta.

4. Especificar um protocolo a ser utilizado pelos “principais” que utilizam o algoritmo de segurança e a informação secreta para conseguir um serviço de segurança em particular.

# Modelo de segurança de redes



# Modelo de segurança de acesso a redes



# Métodos de defesa

- Encriptação
- Controlo de Software (limitações no acesso a base de dados, num sistema operativo protege cada utilizador dos outros utilizadores)
- Controlo de Hardware (*smartcard*)
- Políticas (alteração frequente de *passwords*)
- Controlos físicos

# O que é que se pode fazer para melhorar a segurança?

1. Implementar uma política de segurança
2. Realizar uma análise dos riscos
3. Implementar tecnologias de segurança
4. Realizar auditorias de segurança periódicas

# Perguntas para a definição da política de segurança

- O que proteger?
- Contra quem ou o quê?
- Quais as ameaças mais prováveis?
- Qual a importância de cada recurso?
- Qual o grau de protecção desejado?
- Quanto tempo, recursos humanos e financeiros se pretende gastar para atingir os objectivos de segurança desejados?
- Quais as expectativas dos utilizadores e clientes em relação à segurança de informações?
- Quais as consequências para a instituição se os seus sistemas e informações forem violados ou roubados?

# Política de segurança

- A política de segurança é utilizada como referência básica para:
  - Definir controlos de utilização para serviços e aplicações.
  - Estabelecer direitos e restrições de acesso a recursos.
  - Definir medidas preventivas e correctivas das violações da segurança.
  - Orientar análise de riscos.
  - Conduzir processos de auditoria.
  - Definir medidas preventivas e correctivas das violações da segurança.

# Política de segurança

- A política de segurança deve reflectir as características da instituição ou empresa em beneficio da qual foi criada, considerando, além das metas e objectivos, o ambiente institucional e a cultura da organização.

- A elaboração de uma política de segurança deve ser orientada em níveis estratégico, táctico e operacional. A cada um destes níveis corresponderá uma classe de disposições, com diferentes graus de exigências e detalhe.

# Política de segurança

- **Normas como, por exemplo, a BS7799/ISO17799/ISO27001**
  - Temos de começar de alguma forma. O melhor é começar por seguir as ideias de quem já pensou durante algum tempo no assunto.

    Resumindo: “Evitar inventar a roda de novo”.
- **Deve ter a “benção” da Administração**
  - Se a Administração não for convencida das vantagens de implementar uma politica de segurança nunca se disporá a investir e, sem o “*cacau*” necessário para investir a segurança .....
- **Necessita ser explicada a todos os utilizadores**
  - Sem a participação destes não há implementação de medidas de segurança com possibilidade de ter sucesso.
- **Uma empresa pode ser certificada em termos de segurança dos sistemas de informação através das norma ISO 27000.**

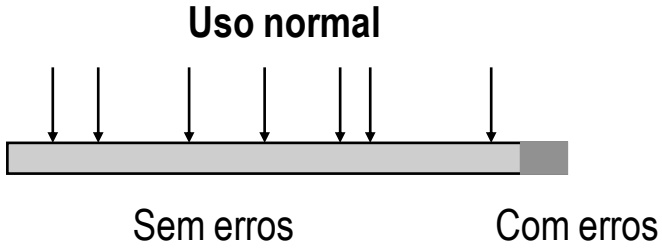
# Política de segurança

- A norma **ISO 17799** inclui dez secções principais:
  - *Security Policy*
  - *System Access Control*
  - *Computer & Operations Management*
  - *System Development and Maintenance*
  - *Physical and Environmental Security*
  - *Compliance*
  - *Personnel Security*
  - *Security Organization Asset*
  - *Classification and Control Business*
  - *Continuity Management (BCM)*

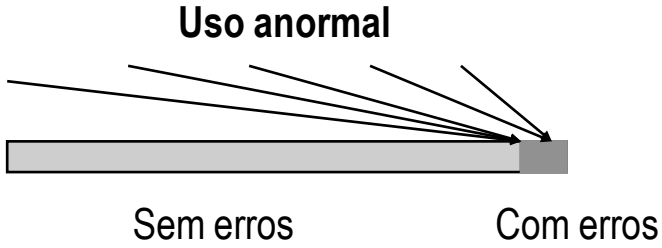
# Porque é que a Segurança é mais dificil de implementar do que parece?

Todo o software tem *bugs*

Em condições normais um programa 99,99% livre de *bugs* raramente causa problemas




Um programa de segurança livre de erros em 99,99% pode ser explorado sendo seguro que os 0,01% de erros serão sempre encontrados




**Isto converte uma falha de 0,01% numa de 100%**

# Porque é que a Segurança é mais dificil de implementar do que parece?

- Os clientes já assumem que todo o software tem *bugs*
  - A correcção não é um ponto considerado para a venda
  - A validação e verificação de software é dispendiosa e consumidora de tempo pelo que é dificil de justificar.
- Solução:
  - Limitar a funcionalidade da segurança a um pequeno subconjunto de funções, o "***trusted computing base*** (**TCB**)"
    - Em teoria o TCB é pequeno e relativamente fácil de analisar
    - Na prática os vendedores acabam por colocar tudo e mais alguma coisa no TCB, tornando-o um UTCB (*universal*)
    - Os consumidores compram o produto de qualquer forma

# Venda de Segurança à Administração da empresa

- A Segurança não se vende bem aos Administradores

- **O gestor de segurança tem direito a "pouco crédito se funcionar bem, a culpa toda se não funcionar". Raramente receberá "palmadinhas nas costas" por uma boa política de segurança.**

- Para assegurar boa segurança deviam existir penalizações monetárias pela sua falha.

# Venda de Segurança à Administração da empresa

- Objecto de regulamentos
  - Processos por negligência (segurança pobre/cifras fracas)
  - Acionistas podem processar a companhia se os preços da acções cairem devido a brechas na Segurança
  - As companhias nos EUA gastam mais em Segurança devido a ameaças de processos
- Requisitos de protecção de dados/privacidade
- Noticias de ataques dos *hackers* a sistemas
- Os que deviam ser os melhores clientes da Segurança
  - Têm sido publicamente embaraçados
  - Sofrem auditorias