
## Cadeira de Tecnologias de Informação

### Ano lectivo 2009/10

# Segurança Informática

# Tópicos

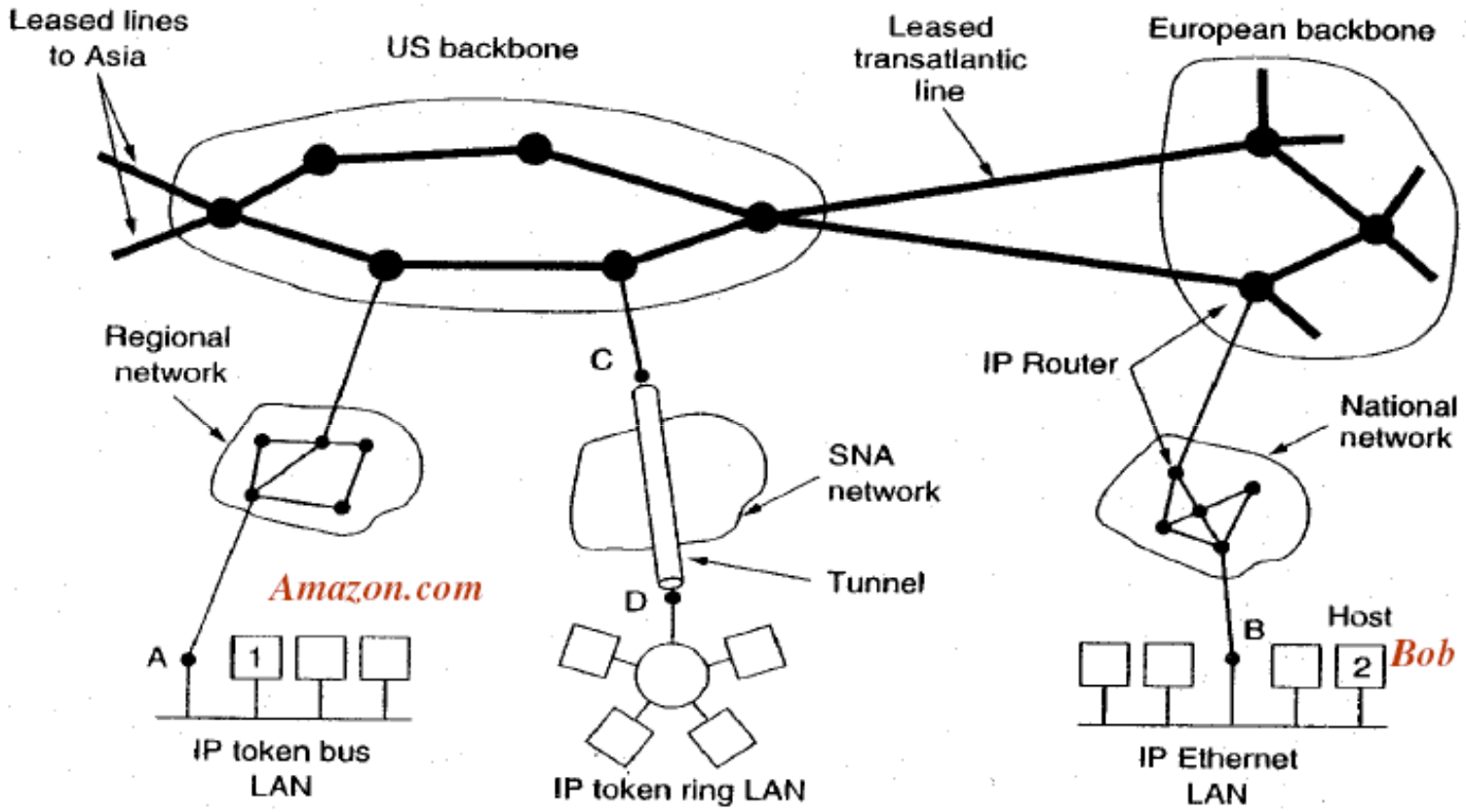
1. O que é segurança?
2. Problemas relacionados com segurança
3. Criptografia
4. Assinatura digital
5. Certificados digitais/ Autoridades de Certificação
6. VPN
7. *Firewall*
8. *Intrusion Detection Systems* (IDS)

# O que é a segurança informática?

- **Comunicações**
  - **Sigilo**: comunicações interceptadas não podem ser entendidas ou traduzidas
  - **Autenticação**: estabelece  a identidade do emissor
  - **Integridade**: garante que a mensagem não foi alterada

- **Acesso a recursos**
  - **Autenticação**: estabelece a identidade de quem pede acesso ao recurso
  - **Autorização**: dá ou nega acesso ao recurso

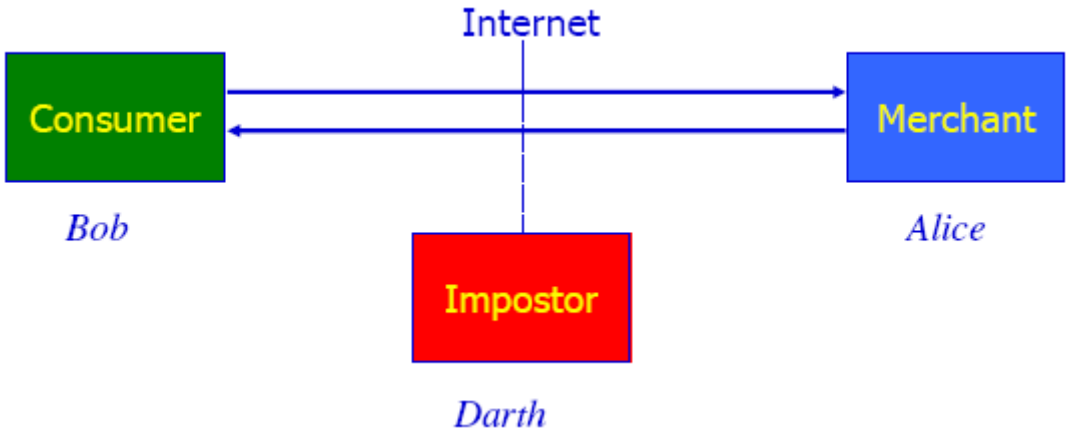
# O que pode correr mal ???



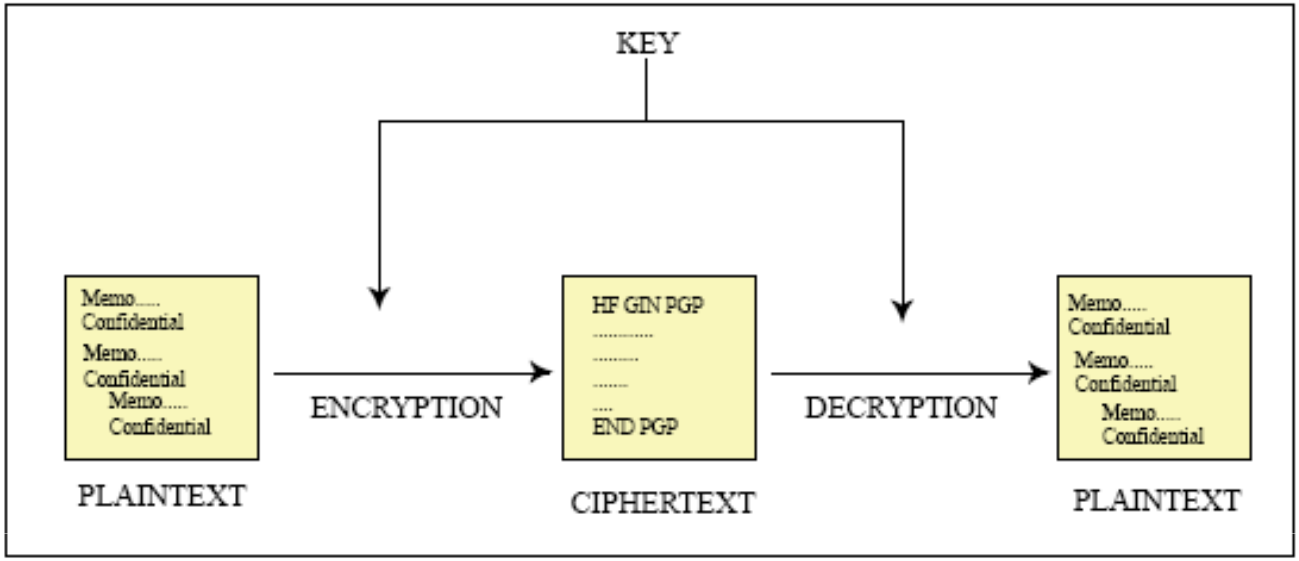

"*A birds eye view of the internet*"

# Problemas relacionados com segurança

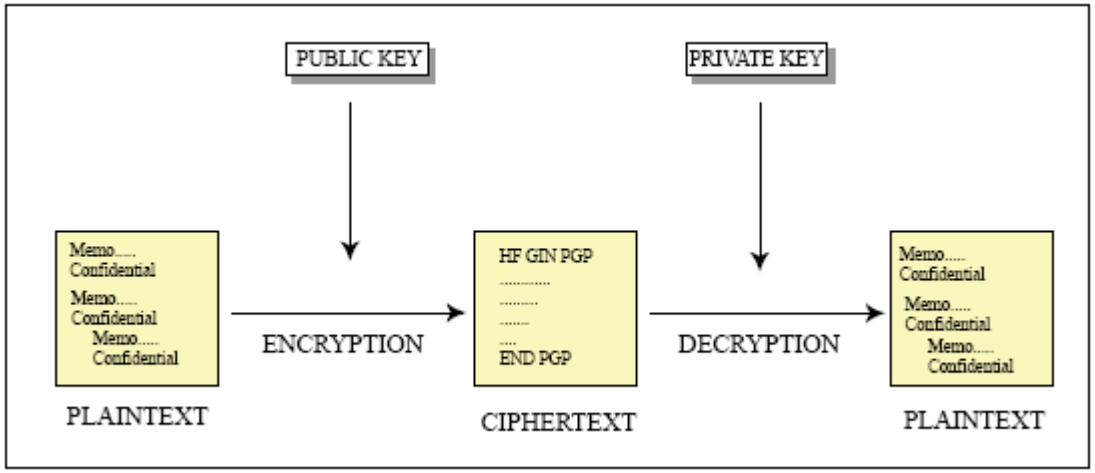
- **Encriptação** – Como asseguro o sigilo das minhas transacções ?
- **Autenticação** – Como valido a verdadeira identidade dos envolvidos numa transacção ?
- **Integridade** - Como tenho garantias que uma mensagem não foi alterada?



# Criptografia Tradicional




**Chave Privada**

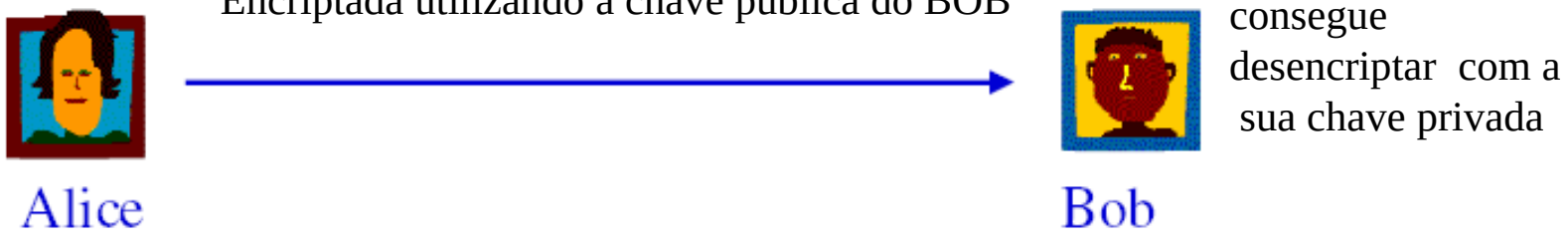



**Chave Pública**
**Chave Privada**

# Criptografia baseada em chave pública

- **Criptografia baseada numa chave privada**
  - A mesma chave é utilizada para encriptação e desencriptação.
  - Problema: como transmitir a chave de forma segura!!???

- **Criptografia baseada numa chave pública, duas chaves utilizadas**
  - **Chave pública** conhecida por todos, utilizada para encriptação.
  - **Chave privada** conhecida apenas pelo dono, utilizada para desencriptação.



# A criptografia baseada em chave pública funciona se ...

- **A chave privada permanece secreta**
  - Nunca abandona o computador do dono.
  - Normalmente encriptada e protegida por *password.*
- **Dificuldade em adivinhar a chave privada a partir da pública**
  - Tentar todas as combinações
  - A quebra do código cresce exponencialmente com o tamanho binário da chave.
  - As chaves de 1024 bits levam mais tempo que a vida do universo a serem quebradas.
- **Distribuição da chave pública de forma fidedigna**
  - A chave pública  não é secreta e pode ser distribuída livremente

# A Encriptação não é suficiente ...
## *Spoofing*

- **Fazer de conta que é outra pessoa**
- **Enviar comunicações em nome de outra pessoa**

  Exemplo do email

  Exemplo de *sniffing* de pacotes

Donde surge a necessidade de autenticação das mensagens ...
Ou assinatura digital de mensagens ...

# Assinaturas digitais

- **Utilização do principio chave pública / chave privada**

- **A Alice envia uma mensagem M**
  - aplica a sua **chave privada**
  - envia a mensagem encriptada para o Bob

- **O Bob desencripta-a com a chave pública da Alice**
  - Obtém a mensagem enviada
  - Infere que de facto o emissor é a Alice (pelo *match* das chaves)

- **Desta forma, encriptando uma mensagem com a chave privada de alguém funciona como assinatura digital!**

# Como é gerido o processo de distribuição das chaves?

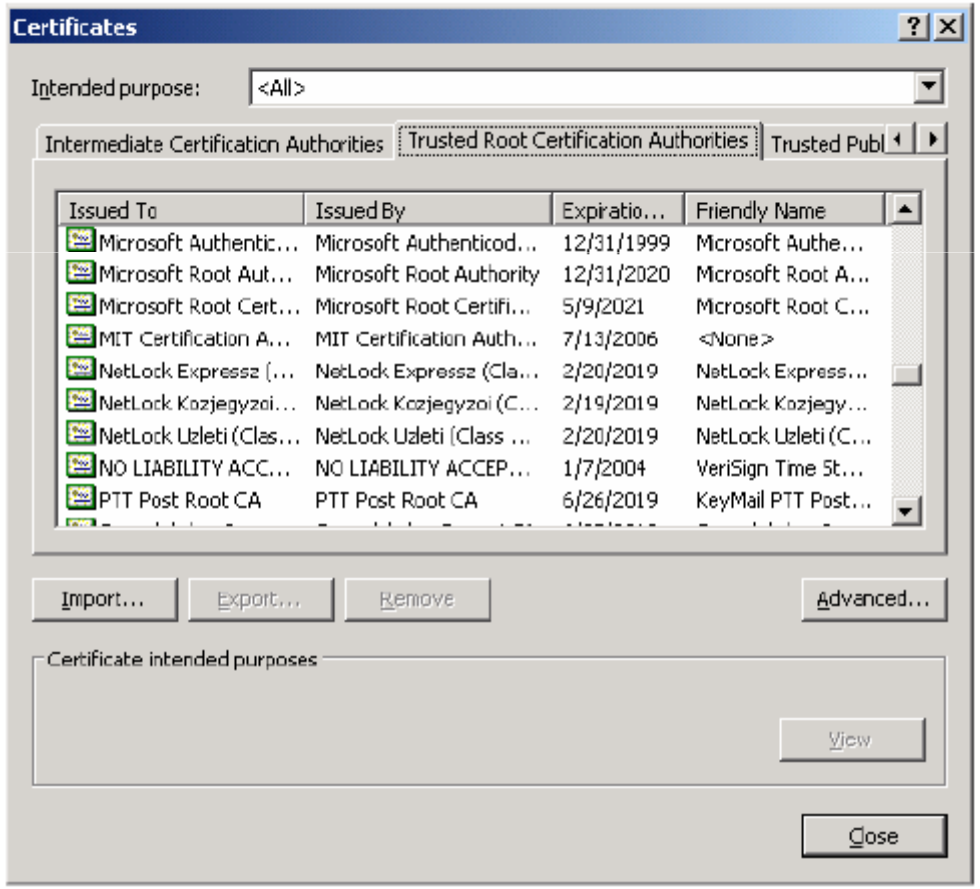
- **PKI - *Public Key Infrastructure***
  - **Autoridades de Certificação** com responsabilidade de emitir certificados credíveis.
  - Antes de um certificado ser emitido, a entidade certificadora valida a credibilidade da entidade que irá ser dona do certificado.
  - Os certificados públicos são digitalmente assinados pela entidade certificadora.

    ex: Verisign, Entrust, Cybertrust , Multicert (Portugal)

- **Certificados**
  - Utilizados para certificar a identidade de um utilizador perante outro utilizador.
  - Assinados digitalmente pelo emissor.
  - O emissor é uma entidade credível.

# Certificados digitais nos *web browsers*

- Os *web browsers* já trazem vários certificados …
- No Internet Explorer ver em: *Tools-> Internet Options-> Content -> Certificates*



# Aplicações: segurança no *e-commerce*

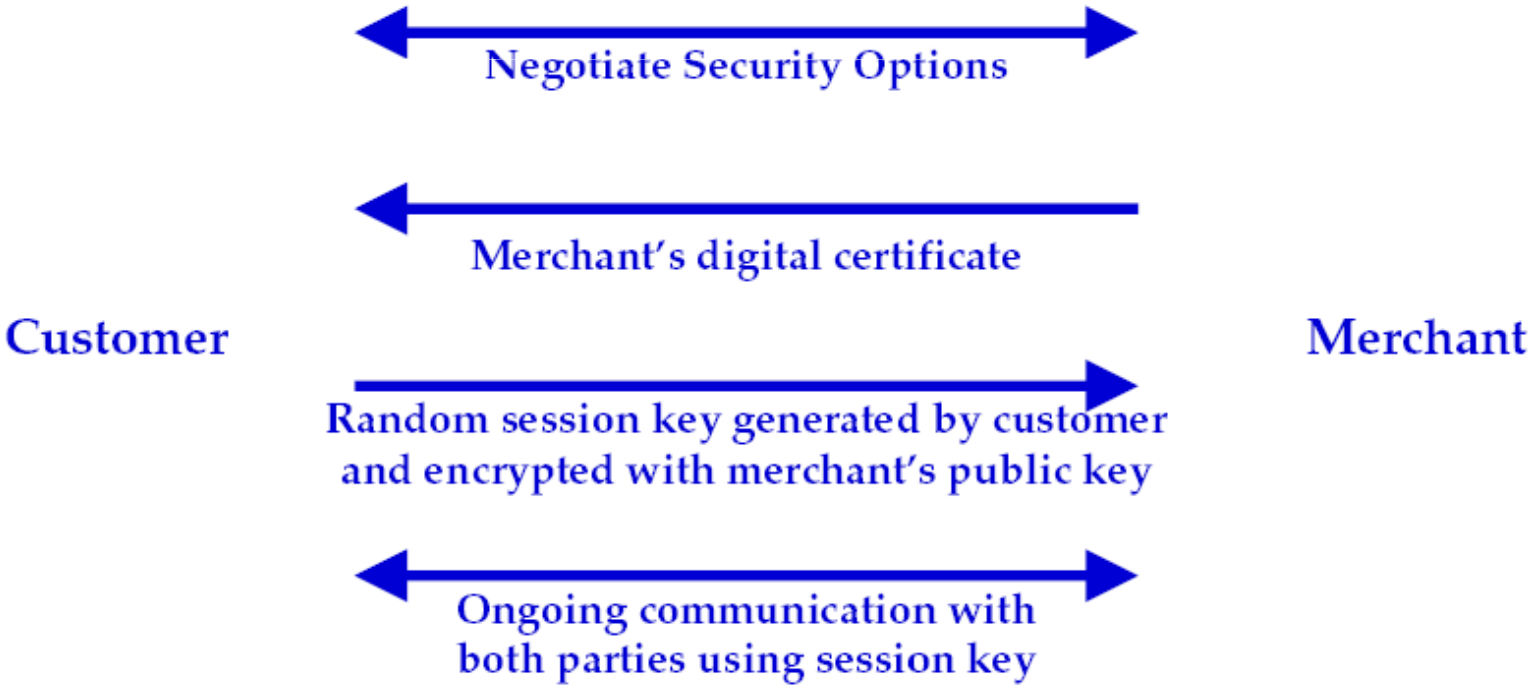
- **A necessidade de transmitir informação sensível na NET**
  - Números cartões de crédito
  - Encomendas de produtos

- **Requisitos**
  - Emissor e receptor têm que se identificar antes de trocarem qualquer informação.
  - Toda a informação trocada, circula encriptada.
  - Qualquer comunicação interceptada, não consegue ser utilizada pelo intruso.
  -

# TLS/SSL

***Transport Layer Security* é o sucessor do *Secure Sockets Layer***

- Providencia um elevado nivel de segurança
- Regularmente utilizado para transacções na WEB
- Encriptação dos **segmentos** ao **nível transporte**



# TLS *(Transport Layer Security)* e a PKI *(Public Key Infrastructure)*

- TLS / SSL utiliza PKI para fornecer autenticação do servidor perante o cliente e, opcionalmente, do cliente perante o servidor.
- O tipo de PKI que o TLS utiliza precisa de ser emitido por uma Autoridades de Certificação

# HTTPS - *Hypertext Transfer Protocol Secure*

- O **HTTPS** é uma combinação do protocolo **HTTP** com o protocolo **TLS** para proporcionar encriptação e identificação segura do Servidor.

- A ideia principal do protocolo HTTPS é a da criação de um canal seguro numa rede insegura. Isso garante uma protecção razoável de intrusos, desde que sejam utilizados códigos apropriados e que o certificado do servidor seja verificado e confiável (emitido por uma Autoridade de Certificação confiável)

# Redes Privadas Virtuais – VPNs

- **Redes privadas seguras, que operam sobre uma rede pública (ex: a Internet)**
  - As mensagens são confidenciais.
  - Só utilizadores autorizados acedem à rede.

- ***Tunneling***
  - Mensagens encriptadas de um protocolo são encapsuladas dentro de outro protocolo.

# Controlo de acesso

- **Que tu tens**
  -*Smartcards* – armazenam os certificados - privado

- **Que tu conheces**
  - Forma de login
  - *Passwords* de acesso (tipos de passwords, muitas *passwords*)

- **Que tu és**
  - Biometria

# Biometria

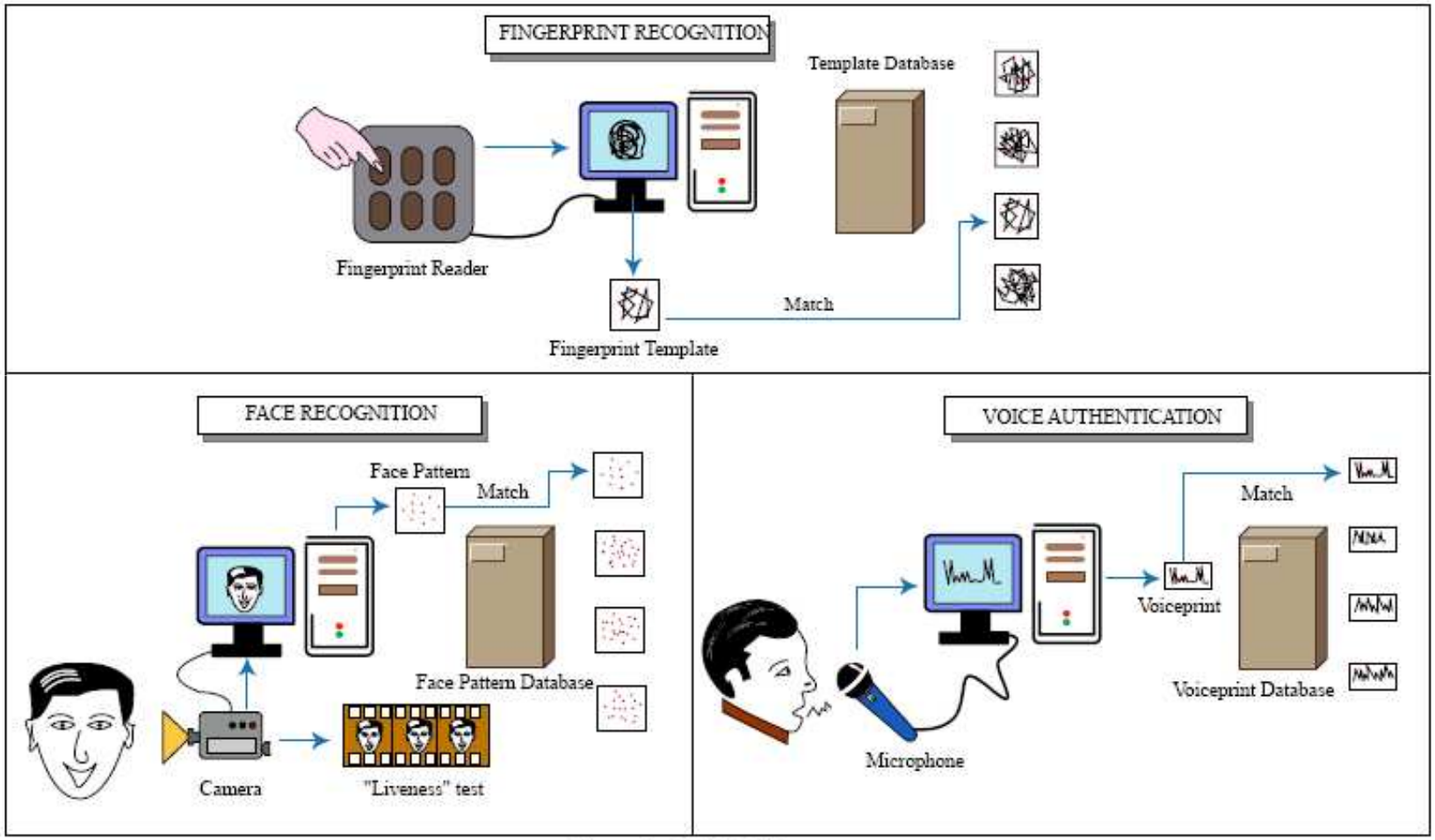



Figure by MIT OCW.

# Quebra da segurança!!!!

- **Mecanismos que exploram falhas aplicacionais acedendo dessa forma à rede e à informação**
  - Virus e *Worms*
  - *Spyware, Adware, Malware* ( cuidado com o que se instala)
  - *Denial of Service Attacks* (não permite que mensagens legítimas cheguem ao destino porque está “cheio” com mensagens inválidas)

- **Medidas de defesa**
  - Anti-Virus, *malware removers*
  - Manter actualizado os *patchs* de segurança da Microsoft (e outros fornecedores) para computadores e *proxys*.
  - *Firewalls, Proxies*
  - Sistemas de Detecção de Intrusões (*Intrusion Detection Systems)*

# *Firewall*

- **O que faz ?**

- Esconde toda a estrutura da rede, fazendo parecer que todas as mensagens são originadas nele.
- Bloqueia mensagens ilegítimas externas.
- Analisa e bloqueia comportamentos “estranhos”.
- Analisa e bloqueia comportamentos “estranhos” e conhecidos.

- **Tipos de *firewalls***

- *Packet filter:* filtra pacotes baseada em regras definidas por utilizador.
- *Proxy server:* filtra efectivamente toda a rede, escondendo-a

# O *trade-off* entre segurança e *performance* do proxy

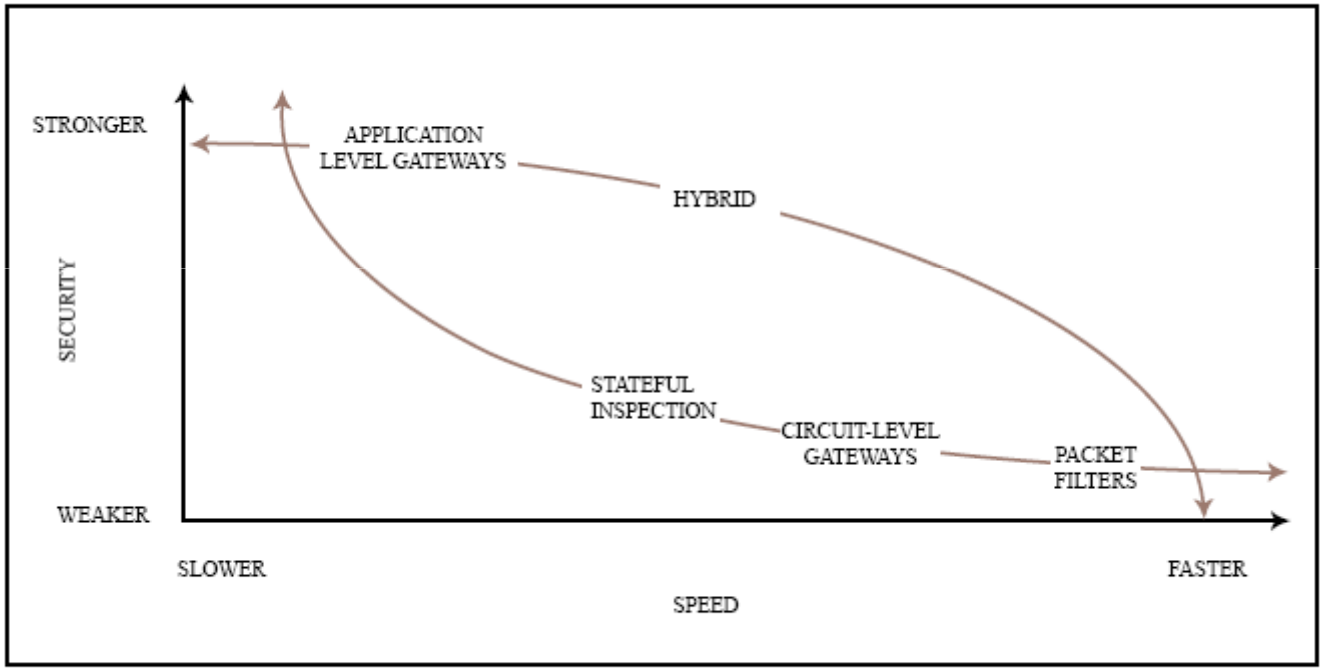



Figure by MIT OCW.

## *Intrusion Detection Systems* (IDS) (1/2)

- Um ***Intrusion Detecting System*** **(**ou **Sistema de Detecção de Intrusões)** pode ser harware e/ou software projectado para detectar tentativas indesejadas de aceder, manipular e/ou tornar inoperantes computadores, principalmente através da Internet.
- Essas tentativas podem assumir a forma de ataques tais como os efectuados por *crackers, malware* e/ou empregados descontentes.
- Um IDS não consegue detectar directamente ataques no tráfego corretamente encriptado.

# *Intrusion Detection Systems* (IDS) (2/2)

- **Um IDS pode ser composto de diversos componentes:**
  - **Sensores** que geram eventos de segurança
  - Uma **consola** para monitorar os eventos e alertas e controlar os sensores
  - Um **"Motor"** central que regista os eventos numa base de dados e usa um sistema de regras para gerar alertas de segurança a partir dos eventos registados
  - Esse **"Motor"** central utiliza, entre outros:
    - Técnicas de *datamining*
    - Reconhecimento de *patterns*
    - Reporte de actividades suspeitas

# Cada vez são mais os ataques e com mais técnica...

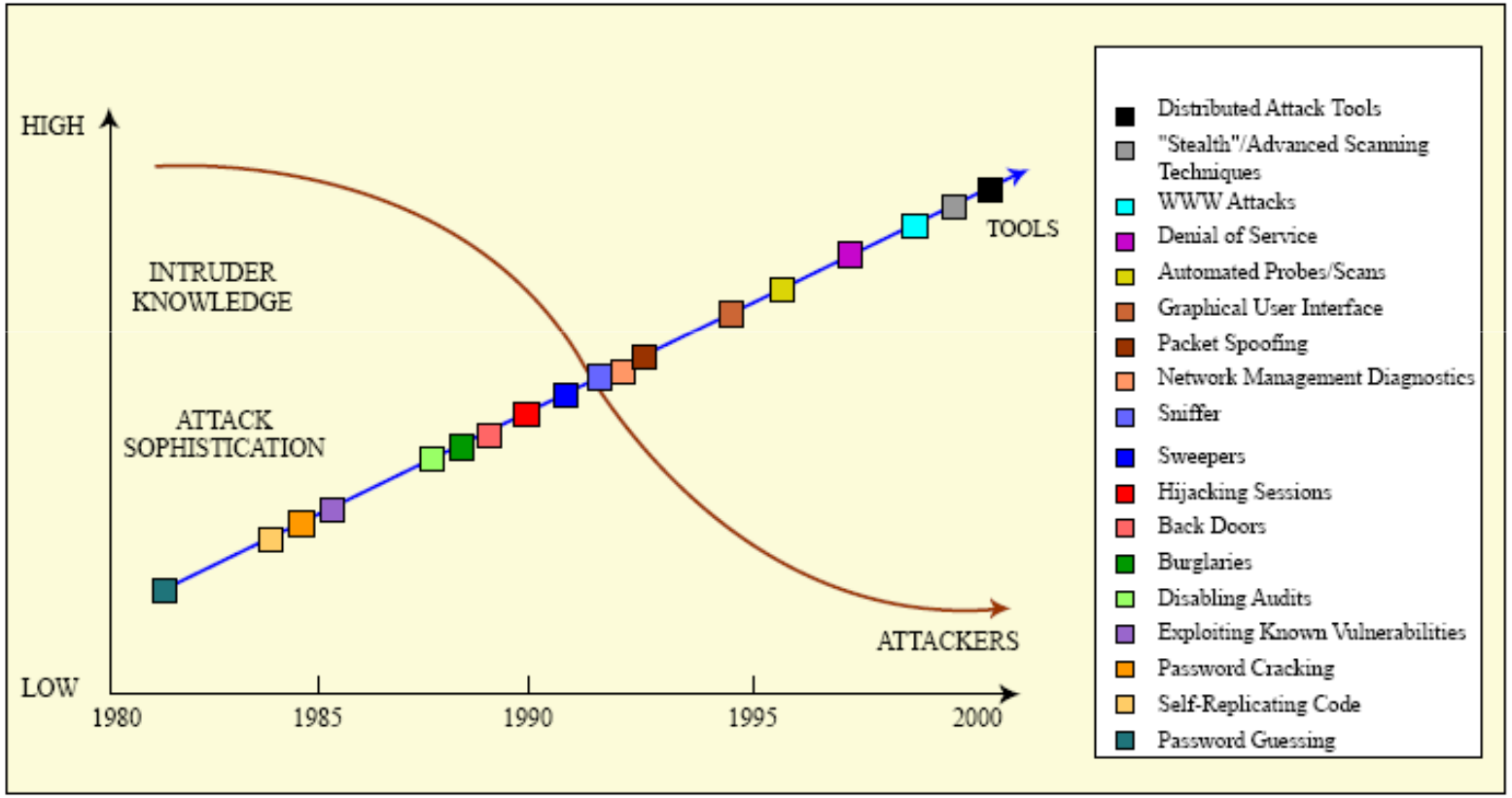



Figure by MIT OCW.

Pretendemos com esta aula sobre conceitos de **segurança** que os alunos compreendessem:

O que é segurança?

**Problemas** relacionados com segurança

Criptografia

*Assinatura digital*

Certificados digitais

**VPN**

*Firewall*

*Intrusion Detection Systems*