

# **Segurança Informática e nas Organizações**

---

Resumos  
2016/2017

João Alegria | 68661

# Capítulo 1

## Introdução

---

Em segurança de sistemas computacionais, podem-se considerar três grandes áreas de atividade, todas relevantes e com as suas especificidades:

- defesa contra catástrofes físicas
- defesa contra faltas / falhas previsíveis
- defesa contra atividades não autorizadas

### Defesa contra catástrofes físicas

Conseguir que um sistema computacional, ou o serviço que esse sistema presta, consiga sobreviver a catástrofes onde existam consequências a nível físico.

<b>Catástrofes ambientais</b>	Tremores de terra, incêndios, inundações, quedas de raios, tempestades magnéticas
<b>Catástrofes políticas</b>	Ataques terroristas, motins
<b>Catástrofes materiais</b>	Degradação irreparável ou perda ou roubo de equipamentos computacionais, como: discos magnéticos, computadores portáteis

Todas estas catástrofes são potenciais causas de dano físico irreparável de equipamentos informáticos e potenciais causas de perda irreparável de informação armazenada.

Para que a sobrevivência seja assegurada, pode-se usar hardware com redundância ou equipamentos redundantes com informação replicada. Isto permite que o sistema afetado continue a prestar o serviço esperado com uma perturbação que será determinada apenas pelo tempo que levarem a entrar em funcionamento efetivo os sistemas alternativos não afetados.

**Solução:** realização periódica de cópias de salvaguarda (backup)  
prevenção realista: para catástrofes mais prováveis  
replicação da informação e dos recursos computacionais

## Defesa contra faltas ou falhas previsíveis

A defesa contra falhas previsíveis visa sobretudo minimizar o impacto de problemas que ocorrem com uma frequência maior, mas cujo impacto global é normalmente menor.

Pode-se considerar:

Falha	Solução
Falta de energia <ul style="list-style-type: none"><li>• Quebra no fornecimento de energia elétrica</li></ul>	Sistemas de alimentação alternativos (baterias, geradores a combustível)
Falha dos sistemas: <ul style="list-style-type: none"><li>• Bloqueio na execução de aplicações ou sistemas operativos (blue-screen)</li></ul>	Sistemas transacionais (garante a transformação da informação guardada se faz de forma coerente através do agrupamento de conjuntos de microalterações em macroalterações atómicas (ex: transferências bancárias))
Falhas de comunicação <ul style="list-style-type: none"><li>• Falhas temporárias de conectividade em troços de rede</li></ul>	Encaminhamento alternativo (em caso de falha de um dos caminhos, pode-se usar outros, garantindo que, mais tarde ou mais cedo, a informação consegue chegar ao destino pretendido).

## Defesa contra atividades não autorizadas

Defesa de sistemas computacionais face a iniciativas tomadas por indivíduos contra o funcionamento normal dos primeiros. Neste caso o desastre não é simplesmente fruto de circunstâncias que podem ocorrer com um dada probabilidade, mas sim fruto da atividades deliberadas que visam a corrupção ou subversão de sistemas computacionais. As atividades não autorizadas podem ter origem em sujeitos que pertencem à organização detentora do sistema computacional que se quer proteger ou que não pertençam a ela. Os primeiros são sempre os mais difíceis de contrariar, uma vez que possuem habitualmente privilégios acrescidos, em relação aos segundos, que podem usar para iniciar atividades não autorizadas.

- ***Tipos de atividades ilícitas***

- Acesso a informação
- Alteração de informação
- Utilização de recursos (CPU, memória, impressora, rede, etc...)
- Impedimento de prestação de serviço (Denial of Service - DoS)
- Vandalismo (interferência com o normal funcionamento do sistema sem qualquer benefício para o sujeito causador)

## Complexidade do problema

Os sistemas computacionais unidos por redes (Internet), são cada vez mais explorados para guardar e manipular informação usada no dia-a-dia das pessoas e das organizações. A segurança nos sistemas computacionais são um problema técnico, porque a multiplicidade de arquiteturas de hardware, sistemas operativos e suas versões, protocolos aplicacionais e requisitos aplicacionais fazem com que a definição e implantação de políticas de segurança em sistemas distribuídos ligados à Internet seja difícil, quer de pôr em prática quer de manter.

A Internet permite um acesso rápido a um número elevado de máquinas e redes, o que torna extremamente eficazes todos os ataques que exploram vulnerabilidades de forma automatizada em todo o espaço de endereçamento da Internet.

<b>Os computadores podem fazer muito estrago em pouco tempo</b>	<b>Existem cada vez mais pontos fracos</b>	<b>As redes permitem:</b>	<b>Regra geral os utentes são incautos</b>
- Gerem muita informação - Processam e comunicam rapidamente	- Porque os sistemas são cada vez mais complexos - Porque o time-to-market é cada vez mais reduzido	- Ataques “anónimos” a partir de qualquer lado - Propagação automática de ciberpragas - A existência e uso de programas e máquinas hostis	- Porque não estão cientes dos problemas e soluções - Porque não se preocupam ou arriscam

## Atitudes realistas

Costuma-se dizer que não existe segurança a 100%, portanto existirão sempre vulnerabilidades, ataques capazes de as explorar, pessoas dispostas a efetuar tais ataques.

<b>Proteção a 100% é impossível</b>	<b>A segurança é dispendiosa</b>	<b>Proteção, valor e punição</b>
- Mau equilíbrio custo-eficácia no retorno do investimento. Cara porque exige pessoas com muito boa formação em tecnologias de segurança e em equipamentos - Problema: Calcular custos e eficácia	- Em material e pessoas - Dispor apenas do necessário	- Proteção suficiente boa para impedir ataques frequentes - Interferir com o trabalho diário menos do que os danos causados por atacantes - Polícia e tribunais para identificar e punir os atacantes

# Segurança: Léxico

## Vulnerabilidades, ataques, riscos e defesas

Uma vulnerabilidade é uma característica de um sistema que o torna sensível a certos ataques. Um ataque é um conjunto de passos executados no âmbito da exploração de vulnerabilidades e que permite concretizar uma ação ilícita.

Um risco, ou uma ameaça, é o dano que pode resultar da execução bem-sucedida de um ataque. A defesa consiste no conjunto de políticas e mecanismos desenhados, concretizados e implantados para:

- diminuir as vulnerabilidades de um sistema
- detetar e contrariar/anular ataques passados ou atuais
- minimizar os riscos de ataques bem-sucedidos



### Resumo de Palavras

#### • Vulnerabilidade:

- Característica de um sistema que o torna sensível a ataques
- Na conceção/ no desenvolvimento/ na instalação

#### • Ataque

- Conjunto de passos que levam à execução de uma ou mais atividades ilícitas (normalmente explorando vulnerabilidades)

#### • Risco/Ameaça

- Possibilidade de dano resultante de um ataque
- Dano material ou imaterial

#### • Defesa

- Conjunto de políticas e mecanismos de segurança que visam:
  - Diminuir as vulnerabilidades de um sistema
  - Detetar o mais rápido possível ataques passados ou atuais
  - Diminuir os riscos de um sistema

### Resumo dos Riscos

#### • Informação, Tempo e Dinheiro

- Eliminação ou alteração de informações

#### • Confidencialidade

- Acesso não autorizado a informação

#### • Privacidade

- Recolha de dados de índole privada

#### • Disponibilidade de recursos

- Ruptura de sistemas informáticos

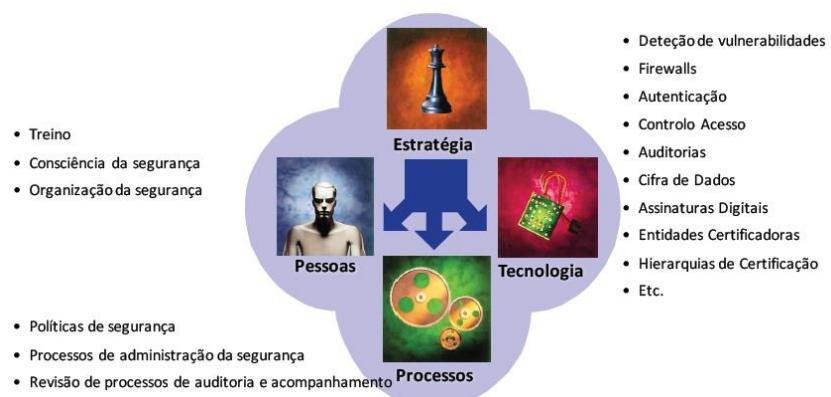
#### • Personificação

- De pessoas ou serviços
- Uso abusivo de sistemas alheios privilegiados

### Fontes de vulnerabilidades

- Aplicações com bugs ou hostis
- Utilizadores
- Má Administração
  - Os sistemas são cada vez mais complexos
  - As configurações por omissão nem sempre são as melhores
  - Medidas restritivas de base vs flexibilidade de operação
- Comunicações sobre redes não controladas
  - Geridas por terceiros independentes das fontes de comunicação.

### Dimensões a considerar



## **Políticas de Segurança**

As políticas de segurança definem fundamentalmente requisitos de segurança que devem ser respeitados para garantir um determinado resultado.

- Definem o poder/privilégio dos sujeitos
  - Princípio do privilégio mínimo
  - Hardening
- Definem procedimentos de segurança
  - Quem deve fazer o quê e em que circunstâncias
- Definem os requisitos de segurança de um domínio
  - Níveis de segurança
  - Autorização necessária (e respetivos requisitos mínimos de autenticação satisfatória)
- Definem estratégias de defesa táticas de contra-ataque
  - Arquitetura defensiva
  - Monitorização de atividades críticas ou de indícios de ataques
  - Reação a ataques ou situações anormais
- Definem o universo de atividades lícitas ou ilícitas
  - Tudo o que não é negado é permitido
  - Tudo o que não é permitido é negado

## **Mecanismos de segurança**

As políticas de segurança são colocadas em prática recorrendo a mecanismos de segurança. Os mecanismos de segurança são a forma prática como as políticas são aplicadas em cenários concretos. Normalmente uma política de segurança pode ser aplicada de diversas formas.

- **Os mecanismos servem para implantação das políticas**

- As políticas definem o que precisa ser feito
- Os mecanismos servem para o fazer

- **Mecanismos de segurança genéricos**

- Confinamento: criam barreiras à difusão de atividades para além de barreiras de segurança.
- Autenticação
- Controlo de acesso: permite aferir se um dado sujeito pode ou não realizar uma terminada ação sobre um determinado objeto.
- Execução privilegiada: estes mecanismos destinam-se a conceber privilégios acrescidos a aplicações especiais que sejam executadas por utentes que normalmente não usufruem desses privilégios.
- Filtragem: servem para realizar certas formas de confinamento ou controlo de acesso, ou seja, servem para identificar atividades não necessárias ou autorizadas e evitar que as mesmas sejam levadas a efeito.
- Registo (logging): produzem relatórios mais ou menos exaustivos/pormenorizados de atividades solicitadas ou realizadas.
- Inspeção: são mecanismos que estão de forma permanente a observar o sistema, de modo a detetar alguma atividade não esperadas, legal ou ilícita.
- Auditória: são normalmente mecanismos de inspeção e análise de registos que permitem tirar conclusões após ter acontecido algo de inesperado.
- Algoritmos criptográficos e afins: mecanismo insubstituível para proteger informação que possa ser fisicamente devassada. Este apenas permite concretizar cifras mais complexas e sofisticadas e agilização da aplicação a conteúdos formados por blocos de bits.
- Protocolos criptográficos: são trocas ordenadas de dados entre entidades em que parte ou a totalidade dos dados úteis trocados são cifrados.

## Segurança em sistemas distribuídos

A defesa dos sistemas computacionais é uma tarefa complexa e árdua, devem ser atribuídas prioridades máximas a técnicas de defesa de perímetro que criem uma primeira barreira aos potenciais atacantes.

Numa primeira fase de concepção de segurança de um sistema distribuído, é preciso subdividir o mesmo em subgrupos de redes e máquinas e enquadrar esses subgrupos de redes e máquinas em domínios de segurança, definindo bem que sujeitos e em que circunstâncias os mesmos podem ter acesso a cada perímetro de segurança, tanto para efeitos de administração como para fins de exploração. Deve ainda ser definido o conjunto de atividades autorizadas e proibidas, quer explicita quer implicitamente. Entre cada domínio de segurança, deverá haver um número mínimo de pontos de contacto que deverão ser estabelecidos por pontes de segurança.

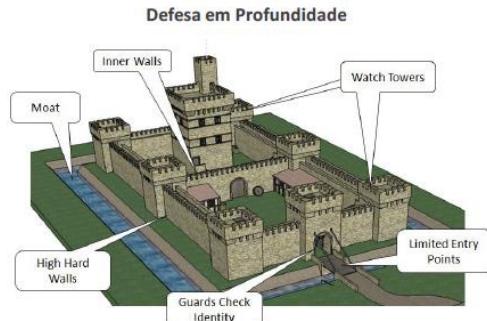
Uma ponte de segurança é uma infra-estrutura intrinsecamente segura por definição e que controla, monitoriza e limita as interações entre domínios de segurança, de forma a evitar interações ilegais ou inesperadas entre sujeitos, aplicações ou máquinas operando em domínios de segurança distintos.  firewall

## Políticas em Sistemas Distribuídos

### Abrangência de várias máquinas e redes

- Domínios de segurança
  - Definição do conjunto de máquinas e redes do domínio
  - Definição do universo de utentes válidos
  - Definição do universo de atividades lícitas
- Security gateways
  - Definição do conjunto de interações permitidas com o exterior
    - De dentro para fora
    - De fora para dentro

Defesa em Perímetro	Defesa em Profundidade
<p>Consiste em definir um perímetro protegido englobando um conjunto de máquinas e redes e em evitar interações indesejáveis entre os dois lados desse perímetro. O perímetro divide o universo de máquinas e redes em dois:</p> <ul style="list-style-type: none"><li>- onde estão os recursos a proteger</li><li>- onde estão os possíveis abusadores desses recursos</li></ul>	<p>A defesa em profundidade é particularmente útil para detetar problemas mais internos em domínios de segurança que foram originados internamente, ou que, por alguma razão, foram originados externamente ao perímetro de segurança e conseguiram passar através do mesmo.</p> <p>A defesa em profundidade é mais complexa de gerir, mas teoricamente, mais eficaz do que a defesa em perímetro.</p>



## Ataques em sistemas distribuídos

Ataques às máquinas	Ataques às redes	Outros
<ul style="list-style-type: none"><li>• Roubo</li><li>• Intrusão</li><li>• Personificação</li><li>• Negação de prestação de serviços (DoS)</li></ul>	<ul style="list-style-type: none"><li>• Inspeção</li><li>• Personificação</li><li>• Interceção</li><li>• Modificação</li><li>• Reprodução</li><li>• Negação de prestação de serviços (DoS)</li></ul>	<ul style="list-style-type: none"><li>• Transferência de informação</li></ul>

## Modelos de Ataque

Ataques específicos	Ataques automatizados
<ul style="list-style-type: none"><li>• Concebidos especificamente para uma máquina ou rede</li><li>• Conduzidos em tempo real por especialistas</li></ul>	<ul style="list-style-type: none"><li>• Concebidos para explorar vulnerabilidades prováveis</li><li>• Pré-codificadores e lançados contra qualquer máquina ou rede</li><li>• Tempo médio de sobrevivência<ul style="list-style-type: none"><li>- Tempo que medeia entre dois ataques automatizados consecutivos</li><li>- Existem máquinas sensores que permitem calcular esse tempo</li></ul></li><li>• Conduzidos por especialistas, iniciantes, curiosos, etc...</li></ul>

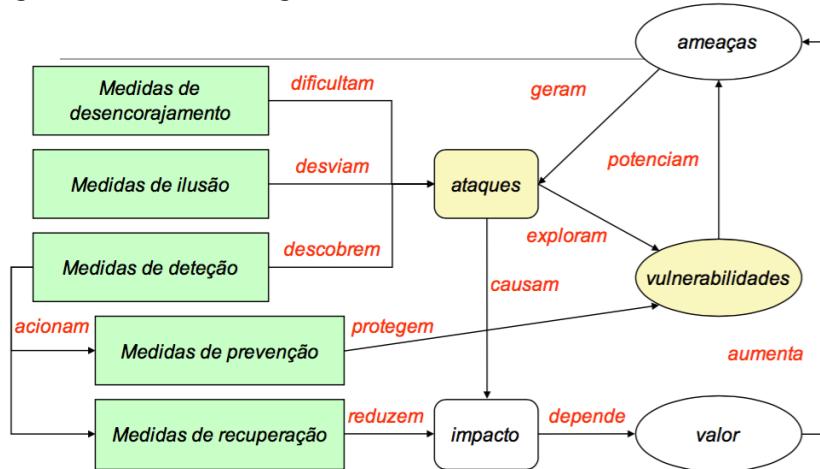
## Mecanismos em sistemas distribuídos

Sistemas operativos confiáveis	Autenticação	Firewalls & Security Appliances
<ul style="list-style-type: none"> <li>• Níveis de segurança, certificação</li> <li>• Ambientes seguros para servidores</li> <li>• Execução confinada (sandboxing)/máquinas virtuais</li> </ul>	<ul style="list-style-type: none"> <li>• Local</li> <li>• Remota</li> <li>• Single Sing-On</li> </ul>	<ul style="list-style-type: none"> <li>• Controlo de tráfego entre duas redes</li> <li>• Monitorização (carga da rede, etc...)</li> </ul>
Autoridades de Certificação/PKI	Cifra de ficheiros e de sessões	Comunicação cifra/VPNs
<ul style="list-style-type: none"> <li>• Gestão de certificados de chaves públicas</li> </ul>	<ul style="list-style-type: none"> <li>• Privacidade de dados que circulam na rede</li> <li>• Privacidade de dados guardados em disco</li> </ul>	<ul style="list-style-type: none"> <li>• Canais seguros sobre redes públicas inseguras</li> <li>• Extensão segura de redes organizacionais</li> </ul>
Monitorização de conteúdos	Deteção de intrusos	Detetores de vulnerabilidades
<ul style="list-style-type: none"> <li>• Deteção de vírus (ciberpragas)</li> </ul>	<ul style="list-style-type: none"> <li>• Deteção de atividades proibidas ou anómalas</li> <li>• Host-based / Network-based</li> </ul>	<ul style="list-style-type: none"> <li>• Procura para efeitos de correção ou exploração</li> <li>• Host-based / Network-based</li> </ul>
Testes de penetração	Administração da Segurança da Empresa	Real-Time Security Awareness / Incident Response
<ul style="list-style-type: none"> <li>• Análise de vulnerabilidades</li> <li>• Tentativas de penetração para demonstração</li> <li>• Teste dos mecanismos de segurança instalados</li> </ul>	<ul style="list-style-type: none"> <li>• Desenvolvimento de políticas</li> <li>• Aplicação distribuída de políticas</li> <li>• Co-administração de serviços de segurança</li> </ul>	<ul style="list-style-type: none"> <li>• Capacidade de aprender corretamente a existência de problemas em tempo real</li> <li>• Meios para reação rápida e correta ao incidente</li> </ul>

# Capítulo 2

## Vulnerabilidades

### Segurança da Informação: Vulnerabilidades e Ataques



### Medidas e Ferramentas

Desencorajamento Dificultam os ataques	Ilusão Desviam os ataques
<ul style="list-style-type: none"><li>• Punição<ul style="list-style-type: none"><li>- Restrições legais</li><li>- Evidências forenses</li></ul></li><li>• Barreiras de Segurança<ul style="list-style-type: none"><li>- Firewalls, autenticação, comunicação segura, sandboxing</li></ul></li></ul>	<ul style="list-style-type: none"><li>• Honeypots / Honeynets</li><li>• Acompanhamento forense</li></ul>
Deteção Descobrem os Ataques	Prevenção Protegem Vulnerabilidades
<ul style="list-style-type: none"><li>• Sistemas de detecção de intrusões (ex: Snort)</li><li>• Auditorias</li><li>• Análise forense de penetrações</li></ul>	<ul style="list-style-type: none"><li>• Políticas restritivas (ex: princípio do privilégio mínimo)</li><li>• Pesquisa de vulnerabilidades (ex: OpenVAS)</li><li>• Eliminação de vulnerabilidades (ex: atualização regular)</li></ul>
Recuperação Reduzem o impacto	

As medidas de prevenção (que protegem vulnerabilidades) estão associadas ao processo de deteção (que descobre ataques), e ambas são controladas pelas medidas de segurança (que desencorajam e ilusão).

## Prontidão

- O desencorajamento, a ilusão e a deteção servem sobretudo para lidar com problemas conhecidos
  - Tentativas de reconhecimento (ex: port scanning)
  - Ataques genéricos (ex: escura de rede)
  - Ataques específicos (ex: buffer overflows)
- As medidas de prevenção protegem de vulnerabilidades conhecidas ou desconhecidas
  - Vulnerabilidades genéricas
    - ex: Reação a mensagens mal formadas (protocol scrubbers)
    - ex: Ataques furtivos (normalmente para formatos canónicos)
  - Vulnerabilidades específicas
    - ex: Um erro de software em particular
- A aplicação das medidas requer conhecimento sobre:
  - Vulnerabilidades conhecidas (problema, forma de exploração, impacto, etc...)
  - Padrões dos ataques que exploram essas vulnerabilidades (modus operandi, assinaturas de ataques)
  - Padrões anormais de atividade (Mas será fácil estabelecer um padrão de normalidade? ; Os ambientes heterogéneos são um problema)
- As ameaças em rede de computadores são diferentes de outros tipos de ameaças
  - Os ataques podem ser lançadas em qualquer hora, de qualquer local e por intermédios inocentes
  - Podem ser facilmente coordenados (ex: Distributed Denial of Service Attacks (DDoS))
  - São baratos e rápidos
  - Podem ser automatizados
- Requerem uma capacidade permanente (24x7) de reação de ataques
  - Equipas de especialistas em segurança
  - Alertas de ataque na hora
  - Teste e avaliação dos níveis de segurança existentes
  - Procedimentos de reação ágeis

## Deteção de Vulnerabilidades

- Ferramentas específicas podem detectar vulnerabilidades em sistemas
  - Implementam ataques usando vulnerabilidades conhecidas
  - Implementam ataques usando padrões de vulnerabilidades
    - Buffer Overflow, SQL Injection, XSS, etc...
- Vitais para a robustez das aplicações e sistemas implementados
  - Serviço frequentemente contratado
- Podem ser aplicados a:
  - Código desenvolvido (Análise Estática): OWASP LAPSE+, RIPS
  - Aplicação a executar (Análise Dinâmica): Valgrind, Rational AppScan
  - Externamente como um sistema remoto: Metasploit, ...
- Não devem ser aplicados de foram cega a sistemas em produção!
  - Potencial perda / corrupção de dados
  - Potencial negação de serviço

## Ataques ou ameaças do dia zero

Este tipo de ataques são chamados de *zero day attacks* uma vez que o autor da aplicação tem zero dias para planejar qualquer forma de evitar esse ataque (como por exemplo: aconselhamento forense). Ou seja, o ataque explora vulnerabilidades desconhecidas e, uma vez que não existe quaisquer soluções conhecidas para por fim, possibilita o acesso dos dados e a informações confidenciais.

Uma medida de resistir a este ataque é apostar na diversidade de sistemas operativos para qual o software pode ser lançado ou bloquear com defesas em profundidade com auxílio de firewalls ou utilizar mecanismos de proteção em análise comportamental (*honeypots*)

- Ataque que ocorre no dia zero do conhecimento de vulnerabilidades que o permitem
  - Para as quais não existem soluções conhecidas
  - Pode explorar mesmo um padrão desconhecido
- Ataque que explora vulnerabilidades que:
  - São desconhecidas das vítimas
  - São desconhecidas dos fabricantes implicados
  - São desconhecidas dos organismos e empresas que apoiam a defesa contra ataques
- Podem existir como “dia zero” durante muito tempo
  - Dias... Meses... Anos...

## CVE - Common Vulnerabilities and Exposures

Um CVE consiste num dicionário público de vulnerabilidades e exposições de segurança para gestão de vulnerabilidades e deteção de intrusões. É um método que fornece uma linguagem comum para referir os problemas e facilita a partilha de dados entre investigadores e base de dados vulneráveis.

Uma vez que as vulnerabilidades se encontram acessíveis publicamente, um dado indivíduo é capaz de realizar um ataque a partir do estudo da vulnerabilidade. Este está sempre associado a um software ou a um sistema operativo e o atacante só precisará de um sistema “compatível” com as especificações declaradas no CVE.

Um mecanismo para a redução da utilização por atacantes é limitar o acesso a este tipo de dicionários, deixando apenas acesso a entidades competentes e validadas para tal.

- **Dicionário público de vulnerabilidades e exposições de segurança**
  - Para gestão de vulnerabilidades
  - Para gestão de correções (*patches*)
  - Para alarmística de vulnerabilidades
  - Para deteção de intrusões
- **Identificadores comuns do CVE**
  - Permite a troca de informações entre produtos de segurança
  - Fornece uma base de indexação para avaliar a abrangência de ferramentas e serviços
- **Detalhes de uma vulnerabilidade podem ser restritos**

## **CVE: Vulnerabilidades**

- **Erro no software**

- Que pode ser usado diretamente por um atacante para ganhar acesso ao sistema ou à rede

- **Um erro só é vulnerabilidade se permitir que o atacante viole uma política de segurança**

- Exclui políticas de segurança “abertas” onde todos os utentes são de confiança ou onde não se considera existência de riscos para o sistema

- **Uma vulnerabilidade é um estado de um sistema computacional (ou conjunto de sistemas) que, alternativamente:**

- Permite que um atacante execute comandos em nome de terceiros
- Permite que um atacante acceda a dados ao arrepio do especificado nas restrições de acesso para esses dados
- Permite que o atacante se apresente como outrem
- Permite que o atacante negue a prestação de serviços

## **CVE: Exposição**

- **Problema de configuração de um sistema ou um erro no software**

- Que permitem aceder a informação ou capacidades que podem auxiliar um atacante

- **O CVE considera um problema de configuração ou um erro como uma exposição se não permitir comprometer diretamente um sistema ou rede**

- Mas for uma componente importante para o sucesso de um ataque e uma violação de uma política de segurança expectável.

- **Uma exposição é um estado de um sistema computacional (ou conjunto de sistemas) que, alternativamente:**

- Permite que um atacante realize recolhas de informação
- Permite a um atacante esconder as suas atividades
- Inclui uma funcionalidade que se comporta como esperado mas que pode ser facilmente comprometida
- É um ponto de entrada frequente para atacantes que tentam obter acesso ao sistema ou a dados
- É considerado problemático por uma política de segurança razoável

## **CVE: Benefícios**

- **Fornece uma linguagem comum para referir problemas**

- **Facilita a partilha de dados entre**

- Sistemas de deteção de intrusões
- Ferramentas de aferição
- Bases de dados de vulnerabilidades
- Investigadores
- Equipas de resposta a incidentes

- **Permite melhorar as ferramentas de segurança**

- Maior abrangência, facilidade de comparação, interoperabilidade
- Sistemas de alarme e reporte

- **Fomenta a inovação**

- Local primordial para discutir conteúdos críticos das BDs

## LIMITAÇÕES

Não ajuda à defesa contra ataques do dia zero!

### CVE: Identificadores

- aka CVE *names*, CVE *numbers*, CVE-IDS, ou CVEs

- **Identificadores únicos para vulnerabilidades conhecidas e públicas da CVE List**

- Estados possíveis: “candidate” ou “entry”
- Candidate: sob revisão para inclusão na CVE List
- Entry: Aceite na CVE List

- **Formato**

- Identificador numérico CVE (CVE-Ano-Índice)
- Estado (candidate ou entry)
- Descrição sumária da vulnerabilidade ou exposição
- Referência para informação adicional

### CVE e ataques

- **Ataques podem ser compostos / possibilitados por várias vulnerabilidades**

- Um CVE para cada vulnerabilidade
- Pode necessitar de uma sequência de vulnerabilidades
- Pode necessitar de uma das vulnerabilidades

## CWE - Common Weakness and Enumeration

- **Linguagem comum para discutir, encontrar e lidar com as causas das vulnerabilidades de segurança**

- De programas, do seu desenho ou da arquitetura de sistemas
- Cada CWE representa um tipo de vulnerabilidade
- Gerida pela MITRE Corporation
  - Uma CWE List é disponibilizada pela MITRE website
  - Esta lista fornece uma definição pormenorizada de cada CWE

- **Os CWEs são catalogados segundo uma estrutura hierárquica**

- CWEs localizados nos níveis superiores fornecem uma descrição genérica sobre o tipo de vulnerabilidades
  - Podem ter vários CWEs filhos associados
- CWEs nos níveis inferiores descrevem problemas de uma forma mais focada
  - Com menos ou sem CWEs filhos

- **Bases de dados de vulnerabilidades**

- NIST NVD (National Vulnerability Database)
- CERT Vulnerability Card Catalog
- US-CERT Vulnerability Notes Database

## CERT - Computer Emergency Readiness Team

- Organização orientada para assegurar que a tecnologia e as práticas de gestão de sistemas adequados são usados para:
  - Resistir a ataques em sistemas em rede
  - Limitar estragos e assegurar a continuidade de operação de sistemas críticos apesar da ocorrência de ataques bem sucedidos, acidentes ou falhas
- CERT / CC (coordination Center) @ CMU
  - Uma componente do vasto CERT Program
  - Centro primordial para questões de segurança na internet
  - Criado em 1988
  - O verme demonstrou a vulnerabilidade crescente da rede a ataques globalizados

## CSIRT - Computer Security Incident Response Team

- Uma organização responsável por fornecer serviços de apoio para problemas de segurança em sistemas computacionais
  - Serviço 24x7 para particulares, empresas, departamentos governamentais e outras organizações
  - Ponto único de contacto para reportar incidentes de segurança computacional
  - Disseminação de informação de incidentes

## Alarmes de segurança

- Vitais para a disseminação rápida do conhecimento sobre novas vulnerabilidades
  - US-CERT: Technical Cyber Security Alerts
  - US-CERT (non-technical): Cyber Security Alerts
  - SANS: Internet Storm Center
  - Microsoft: Security Response Center
  - Cisco: Security Center

Vulnerabilidades na Prática	
SQL Injection	Cross-Site Scripting
<p>É uma ameaça de segurança que se aproveita de falhas em sistemas com BD via SQL.</p> <p>Os possíveis ataques são:</p> <ul style="list-style-type: none"><li>- Exposição da informação</li><li>- Consulta da informação</li><li>- Modificação dos dados contidos na BD (através de Insert, Update, Delete)</li><li>- Falsa autenticação em sistemas de <i>login</i></li></ul> <p>Medidas de prevenção:</p> <ul style="list-style-type: none"><li>- Utilização de stored procedures</li><li>- Parametrização de consultas</li><li>- Limitar privilégios de acesso</li></ul>	<p>É um tipo de vulnerabilidade do sistema de segurança de um computador, encontrado normalmente em aplicações web que ativaram ataques maliciosos ou injectaram client-side script dentro das páginas web vistas por outros utilizadores.</p> <p>Este script pode ser usado pelos atacantes para escaparem aos controlos de acesso que usam a política da mesma origem.</p>

# Capítulo 3

## Criptografia

A **criptografia** é a arte ou ciência que permite escrever de forma a ocultar conteúdos. O objetivo da criptografia é permitir que um conjunto limitado de entidades, tipicamente duas, possam trocar informação que é ininteligível para terceiros. (Serve para garantir a privacidade da informação)

A **criptanálise** é a arte ou ciência de violar sistemas criptográficos ou informação criptografada.

**Criptologia** é o ramo que se dedica ao estudo da criptografia e da criptanálise.

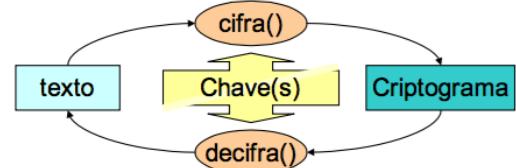
### Cifras

A criptografia baseia-se no uso de cifras. Uma cifra é uma técnica concreta de criptografia, isto é, uma forma específica de ocultar informação. Assim, uma cifra transforma um texto em claro num texto cifrado ou criptograma.

A operação inversa é a decifra, que transforma um criptograma no texto em claro original.

#### Operação de uma cifra

Cifra: texto em claro -> criptograma  
Decifra: criptograma -> texto em claro  
Algoritmo: modo de transformação de dados  
Chave: parâmetro do algoritmo



### Evolução da Tecnologia de Cifra

As primeiras cifras usadas baseavam a sua segurança no secretismo do algoritmo.

<b>Cifras Manuais</b>	Algoritmos de substituição ou transposição (Exemplo: cifra do bastão, cifra de César)
<b>Cifras Mecânicas</b> (séc. XIX)	Algoritmos de substituição ou transposição. As máquinas de cifra usavam fundamentalmente algoritmos de substituição de símbolos, nomeadamente das letras. (Exemplo: máquina Enigma, M-209 Converter)
<b>Cifras Informáticas</b>	Surgiram com o uso dos computadores e a complexidade algorítmica também evoluiu. Assim, os algoritmos de substituição ficaram mais complexos e novos algoritmos baseados em operações matemáticas surgiram.

## Tipos de Cifra

- **Cifra de transposição** - Opera baralhando caracteres do texto original.
- **Cifra de substituição** - Opera substituindo caracteres do alfabeto usado no texto original por caracteres de um alfabeto de substituição.  
Os tipos de cifras de substituição mais vulgares são:
  - 1) **Cifras Monoalfabéticas** - Usam apenas um alfabeto de substituição. Um carácter do alfabeto original é sempre substituído pelo mesmo carácter do alfabeto de substituição numa operação de cifra (e o inverso acontece numa operação de decifra).

<b>Aditiva</b>	A cada letra do alfabeto original é adicionada uma quantidade constante (chave) e o carácter de substituição é o resto da divisão da soma pelo cardinal do alfabeto original. $\text{cripto-letra} = (\text{letra} + \text{chave}) \bmod \#\text{alfabeto}$
<b>Multiplicativa</b>	A cada letra do alfabeto original é multiplicada por uma quantidade constante (chave) e o carácter de substituição é o resto da divisão do produto pelo cardinal do alfabeto original. $\text{cripto-letra} = (\text{letra} \times \text{chave}) \bmod \#\text{alfabeto}$
<b>Frase-Chave</b>	São retirados todos os espaços da frase, caracteres de pontuação e caracteres repetidos e coloca-se o resultado obtido por baixo de um alfabeto corretamente escrito e a partir de uma letra-chave. O resto do alfabeto de substituição obtém-se preenchendo-o com os demais caracteres do alfabeto original, pela ordem correta, que não fazem parte da frase-chave. <div style="border: 1px solid black; padding: 10px; margin-top: 10px;"><p style="text-align: center;">Cálculo do alfabeto de substituição com frase-chave ELES NÃO SABEM NEM SONHAM e a letra-chave H</p><p style="margin-left: 20px;">Alfabeto normal: abcdefghijklmnopqrstuvwxyz</p><p style="margin-left: 20px;">Alfabeto de substituição: tuvwxyzELSNAOBMHcdfgijkper</p></div>

- **Problema:** Reproduzem os padrões estatísticos dos caracteres usados no texto original. Ou seja, se num texto 23% dos caracteres forem um A, então no criptograma 23% dos caracteres serão o substituto de A obtido através do alfabeto de substituição. Da mesma forma, podem-se detetar construções características da linguagem, como diagramas (consoantes dobradas RR e SS em português).
- **Solução:** Usar línguas pouco divulgadas, como fizeram os americanos na Segunda Guerra Mundial.

- 2) **Cifras Polialfabéticas** - Usam um número finito de alfabetos de substituição. Um carácter do alfabeto original pode ser substituído por diferentes caracteres dos alfabetos de substituição numa operação de cifra (e o inverso acontece numa operação de decifra). Os alfabetos são normalmente usados de forma cíclica.

# Cifra de Vigenère

Aplicação de N cifras monoalfabéticas aditivas. A chave de cada uma delas é o valor atribuído a cada letra de uma frase-chave com N letras ( $A=0$ ,  $B=1, \dots$ ,  $Z=26$ ).

	a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z
b	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	
c	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A		
d	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A			
e	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A				
f	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A					
g	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A						
h	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A							
i	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A								
j	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A									
k	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A										
l	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A											
m	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A												
n	O	P	Q	R	S	T	U	V	W	X	Y	Z	A													
o	P	Q	R	S	T	U	V	W	X	Y	Z	A														
p	Q	R	S	T	U	V	W	X	Y	Z	A															
q	R	S	T	U	V	W	X	Y	Z	A																
r	S	T	U	V	W	X	Y	Z	A																	
s	T	U	V	W	X	Y	Z	A																		
t	U	V	W	X	Y	Z	A																			
u	V	W	X	Y	Z	A																				
v	W	X	Y	Z	A																					
w	X	Y	Z	A																						
x	Y	Z	A																							
y	Z	A																								
z	A																									

Cifra de Vigenère e sua aplicação para cifrar um texto com a frase-chave “poema”

Texto original:

eles não sabem que o sonho é uma constante da vida ou uma realidade concreta e definida.

Chave:

поема поема поема поема поема поема поема поема поема

Criptograma:

**tzienpcwmbtaugedqszhdsyyarcretpbxqdpjmpaiosooocgvqtpshqfxbma**

As cifras polialfabéticas escondem melhor a frequência de letras individuais e de conjuntos característicos de letras, como diagramas, do que as monoalfabéticas. Apesar disso, as cifras polialfabéticas podem ser criptanalisisadas tal como as monoalfabéticas se se souber o seu período  $N$ , reduzindo o problema à criptanálise de  $N$  cifras monoalfabéticas normais.

**Teste de Kasiski** - Tem como finalidade procurar padrões comuns no criptograma e posteriormente, calcular a sua posição relativa (posicionamento). Assim, o maior divisor comum de todas as distâncias indica o período da cifra polialfabética.

# Máquina de Rotores

As máquinas de rotores concretizam cifras polialfabéticas complexas

- Cada rotor efetua uma permutação do alfabeto, que consiste num conjunto de substituições
  - A posição do rotor concretiza um alfabeto de substituição
  - A rotação de um rotor concretiza uma cifra polialfabética
  - Acumulando vários rotores em sequência e rodando-os de forma diferenciada consegue-se uma cifra polialfabética complexa

A chave de cifra é:

- O conjunto de rotores usado
  - A ordem relativa dos rotores
  - A posição de avanço do rotor seguinte
  - A posição original dos rotores

### Operação recíproca com um refletor

- O operador emissor carrega em "A" (texto em claro) e obtém Z (criptograma).
  - O operador receptor carrega em "Z" (criptograma) e obtém "A" (texto em claro).
  - Uma letra nunca pode ser cifrada para si própria!

Aproximações Teóricas	Aproximações Práticas
<p><b>Cifra Perfeita</b> - Uma cifra diz-se perfeita quando, dado um criptograma <math>c</math>, a probabilidade de ele corresponder a um dado texto original <math>m</math> e ter sido gerado com uma chave <math>k</math> é igual à probabilidade de ocorrência do texto <math>m</math>.</p> <p><u>Por outras palavras:</u> A cifra é perfeita quando o criptanalista que capturar o criptograma não conseguir de modo algum concluir qual o texto original correspondente, porque para cada texto candidato existe sempre uma chave que pode ter efetuado a transformação.</p> <p><u>Conclusão:</u> O cardinal do espaço de chaves tem de ser igual ou superior ao cardinal do espaço de textos em claro.</p>	<p>Uma cifra diz-se <b>segura na prática</b> se cumprir o objetivo para que é usada. Significa que:</p> <ul style="list-style-type: none"> <li>• As vulnerabilidades da cifra, mesmo quando esta é usada de forma correta, não permitem a sua criptanálise em tempo útil e admitindo um investimento, tendo em conta a relação custo-benefício. (Caso a cifra seja violada para além do período em que é relevante, então o seu objetivo foi cumprido)</li> <li>• A cifra é usada de forma correta, sem aumentar as suas vulnerabilidades intrínsecas.</li> </ul> <p>A segurança é assegurada pela dificuldade computacional de realizar a criptanálise.</p>



## Critérios de avaliação da qualidade das cifras (por Shannon)

Estes critérios abrangem diversos aspectos, como segurança efetiva, usabilidade e facilidade de realização. Os critérios são os seguintes:

- **Quantidade de secretismo oferecida** - Avalia o tempo mínimo de segurança do criptograma face a um determinado esforço e dinheiro envolvido na sua criptanálise. (Ex: Comprimento da Chave)
- **Complexidade das chaves** - Avalia a complexidade inerente à transmissão e salvaguarda de chaves de cifra entre as entidades que cifram e decifram. (Ex: Geração da chave, deteção de chaves fracas)
- **Simplicidade de realização** - Avalia a facilidade de realização e uso da cifra em ambientes de produção.
- **Propagação de erros** - Relevante em ambientes onde podem surgir erros. (Ex: Canais de comunicação ruidosos)
- **Dimensão do criptograma** - Idealmente um criptograma deve ter uma dimensão igual ou menor do que o texto original, de modo a não ter maiores custos de armazenamento ou transmissão de criptogramas do que se tem normalmente com texto em claro.

**Confusão** - Relação entre o texto em claro, uma chave e o criptograma. Esta deve ser o mais complexa possível para ser difícil a descoberta de partes do texto e/ou chaves.

**Difusão** - Cada pedaço de informação do criptograma deverá sempre depender de um pedaço grande de informação do texto original. Assim, qualquer alteração no texto original leva a grandes alterações no criptograma.

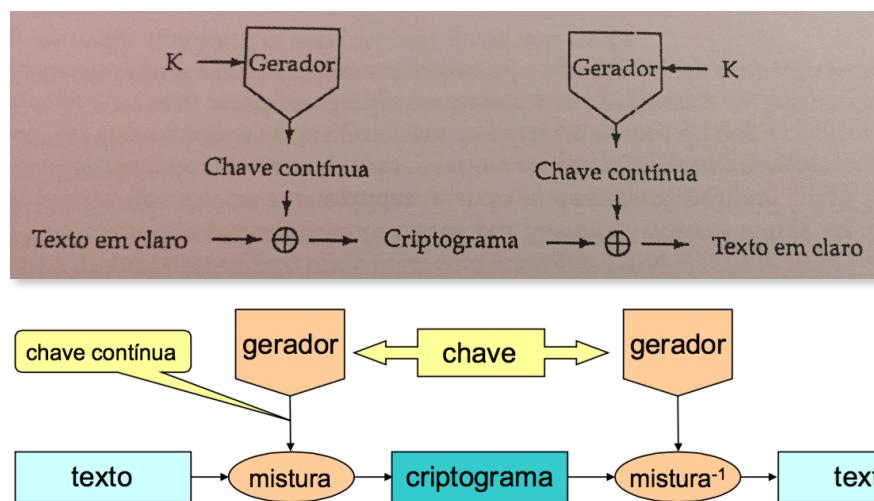
### → Assumir sempre o pior caso (procurar livro p.38)

- O criptanalista conhece o algoritmo - A segurança está na chave
- O criptanalista possui grande número de criptogramas gerados com um algoritmo e chave - Os criptogramas não são secretos
- Os criptanalistas conhecem parte dos textos originais - É normal haver alguma noção do texto original; ataques com texto conhecido ou escolhido

## Cifras Contínuas (stream)

As cifras contínuas surgiram como uma aproximação prática da cifra de Vernam para ambientes digitais. A aproximação consiste em:

- Substituir a chave infinita e aleatória (one-time pad) por uma chave contínua (keystream) produzida por um gerador pseudoaleatório seguro.
- Assim, é misturada a chave contínua produzida com o texto original ou criptograma, usando somas exclusivas (XOR).
- As cifras contínuas usam apenas o princípio da confusão, onde existe uma relação complexa entre a chave do gerador e a chave contínua que o mesmo produz.



- Uma chave contínua pode ser infinita mas periódica, em que o período depende do gerador.
- As chaves contínuas não devem ser reutilizadas, caso contrário, a soma de criptogramas produz a soma de textos.  $C_1 = P_1 \oplus K_s, C_2 = P_2 \oplus K_s \rightarrow C_1 \oplus C_2 = P_1 \oplus P_2$
- O comprimento do texto deverá ser inferior ao período de  $K_s$  - a exposição da chave contínua é total caso se conheça o texto; a repetição de ciclos facilita a criptanálise se se conhecer o período e amostras do texto
- Tem que existir controlo de integridade - não há difusão; é fácil de alterar de forma determinística o texto cifrado

- **Lorenz** - Máquina de cifra contínua com 12 rotores.

- Concretiza uma cifra contínua (cada símbolo de 5 bits é misturado com 5 chaves contínuas)

## Cifras modernas: tipos

A expressão “cifras modernas” refere-se a cifras usadas correntemente em universos computacionais (desktops, portáteis, smartphones, smartcards) que efetuem cifras usando lógica binária.

### Classificação das cifras

- **Modo de Operação**

- **Cifras por blocos** - Cifras por blocos são cifras monoalfabéticas onde cada carácter do alfabeto original e do resultante é formado por conjuntos com imensos bits (64, 128, 256).
- **Cifras contínuas** - Cifras contínuas são cifras polialfabéticas constituídas por um gerador pseudoaleatório onde cada carácter do texto original, independentemente da sua dimensão, será sempre traduzido por outro carácter de igual dimensão, mas dependerá do “alfabeto” que estiver a ser usado nesse momento pela cifra.

- **Tipo de chave**

- **Cifras simétricas** (segredo partilhado) - Chaves secreta partilhada por (tipicamente) dois ou mais interlocutores. Permite a confidencialidade para todos os conhecedores da chave e autenticação de mensagens (cifra por blocos). Apenas os detentores de uma chave secreta podem decifrar a informação cifrada com a mesma.
  - Garantir confidencialidade de dados conhecidos apenas por uma entidade, única detentora da chave secreta
  - Garantir a confidencialidade dos dados trocados entre duas ou mais entidades, que têm de partilhar a mesma chave secreta.

Vantagens	Desvantagens
Desempenho - normalmente, muito eficientes	Num universo de N interlocutores, se se pretender ter uma chave secreta partilhada por cada par de interlocutores, são necessários $N*(N-1)/2$ , se as chaves não forem usadas de forma bidirecional

**Problema:** Distribuição de chaves - Número de chaves cresce exponencialmente com o quadrado da população

- **Cifras assimétricas** (par de chaves) - Usam um par de chaves distintas - uma pública para cifrar e uma privada (pessoal e intransmissível) para decifrar. Não é possível, dada uma chave pública, calcular a correspondente chave privada. A componente privada só deve ser conhecida e usada pela entidade a que está associada; a componente pública pode e deve ser ampla e publicamente divulgada para poder ser usada por qualquer entidade.

Vantagens	Desvantagens
<p>Exigir menos chaves para efetuar interações seguras, porque permitem uma relação de um-para-muitos.</p> <p><b>Permitem:</b></p> <ul style="list-style-type: none"><li>- Confidencialidade sem troca de segredos</li><li>- Autenticação<ul style="list-style-type: none"><li>- De conteúdos (integridade)</li><li>- De autoria (assinaturas digitais)</li></ul></li></ul>	<p>Muito pouco eficientes porque se baseiam em operações matemáticas complexas.</p> <p><b>Desvantagens a nível administrativo:</b></p> <ul style="list-style-type: none"><li>- Confinamento rigoroso das chaves privadas aos detentores</li><li>- distribuição fidedigna de chaves públicas a todos os que as pretendem usar</li><li>- Gestão do tempo de vida dos pares de chaves.</li></ul>

- **Cifras híbridas** (ou mista) - Surgiram como uma solução intermédia muito usada na troca confidencial de mensagens, tentando juntar o que de melhor oferecem as cifras simétricas e assimétricas.

Uma cifra híbrida usa cifras simétricas para cifrar em massa, por estas serem mais eficientes, e cifras assimétricas para distribuição de chaves, nomeadamente para transmitir a chave simétrica usada na cifra a granel ao interlocutor.

Deste modo, obtém-se uma cifra assimétrica com uma eficiência muito próxima das cifras simétricas.

#### Modo de Operação:

- Documento cifrado com a chave simétrica
- Destinatário envia a sua chave pública
- Chave simétrica é cifrada com a chave pública do destinatário
  - O documento e a chave (cifrada) são enviados
- O destinatário decifra a chave (cifrada) com a sua chave privada e decifra o documento com a chave simétrica
  - Destinatário vê o documento

## Cifras modernas: exemplos

### Cifras simétricas por blocos

As cifras simétricas por blocos usam os princípios básicos de difusão e confusão. Tal é feito recorrendo às seguintes operações:

- Aplicação iterativa de uma operação complexa a um bloco de grande dimensão (mais de 64 bits)
- Operações elementares de permutações, substituição, expansão e compreensão de blocos

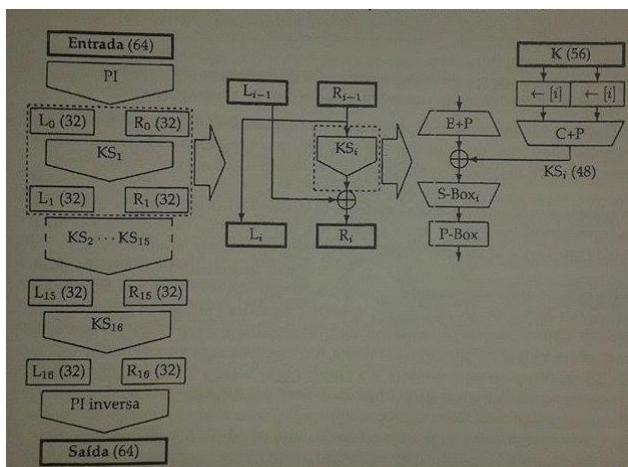
Algoritmos mais usados			
DES	IDEA	AES	Outros
- Bloco(bits) = 64 - Chave(bits) = 54	- Bloco(bits) = 64 - Chave(bits) = 128	- Bloco(bits) = 128 - Chave(bits) = 128, 192, 256	- Blowfish, Cast, RC5

#### • Caso de Estudo: DES

- Cifra simétrica por blocos que usa blocos de 64 bits e chaves de 56 bits. A figura a baixo resume a operação interna do DES.

Esta segue os princípios de confusão e difusão de Shannon, usando unidades elementares de permutação, substituição, expansão e compressão de blocos de bits, e 16 iterações com redes de Feistel.

- Em termos de segurança, o DES pode usar quase todos os valores de 56 bits como chaves igualmente seguras.



O DES só pode ser atacado usando pesquisa exaustiva, o que hoje em dia é viável, tanto técnica como economicamente, por causa de a sua chave ter apenas 56 bits (uma crítica feita desde a sua apresentação).

**Solução:** Usar cifra múltipla, nomeadamente cifra tripla ou branqueamento.

- **Caso de Estudo: AES**

- Utiliza operações algébricas de forma inteligente: a segurança é conseguida através de operações complexas.
- Blocos variáveis com chaves de 128, 192 ou 256 bits.

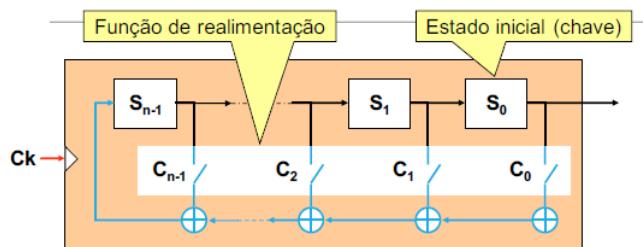
## **Cifras simétricas contínuas**

As cifras simétricas contínuas são aproximações realistas à cifra de Vernan (a chave tem de ter comprimento maior ou igual à mensagem a cifrar).

Aproximações usadas: Geradores baseados em registos de deslocamento com realimentação linear (LFSR), geradores baseados em cifras por blocos.

A maioria das cifras contínuas são síncronas, ou seja, a operação do seu gerador é independente dos dados cifrados e decifrados, o que obriga os dois extremos da comunicação, o que cifra e o que decifra, a gerirem o sincronismo.

Algoritmos mais usados			
A5	RC4	SEAL	Cifra por blocos em modo OFB ou CFB
-Chave(bits) = 64	-Chave(bits) = 40-2048 (depende)	-Chave(bits) = 160	-Chave(bits) = depende da cifra por blocos



### 2n-1 sequências não nulas

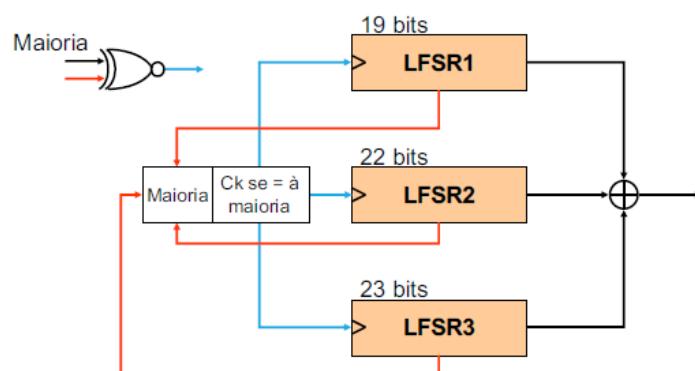
- Se uma delas tiver período  $2n-1$  então todas o têm

### Funções de realimentação primitivas

- Todas as sequências não nulas têm comprimento  $2n - 1$

- **Caso de Estudo: A5**

- A5 é o algoritmo usado em comunicações GSM e usa internamente três LFSR.
- Um LFSR é uma máquina de estados que produz sequências cíclicas de bits. Internamente é formado por um registo de  $N$  bits com deslocamento e por uma função de realimentação, também designada como polinómio de realimentação.
- A sequência de bits gerada por um LFSR depende de dois factores: 1. do estado do registo; 2. da função de realimentação
- Um LFSR pode produzir várias sequências diferentes, no máximo  $2^N - 1$  dependendo esse número da função de realimentação.
- O A5 permite usar diretamente chaves até 64 bits, o número de bits que se pode introduzir como estado inicial dos três LFSR, e produz chaves contínuas com comprimento máximo de  $2^{64}$  bits.



## Cifras assimétricas por blocos

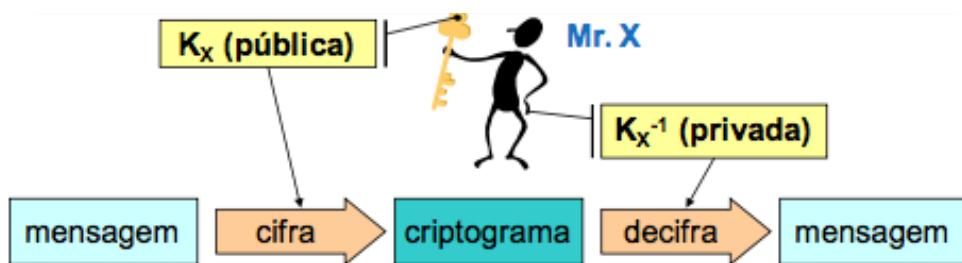
As cifras assimétricas não usam os princípios de difusão e de confusão de Shannon. Usam, em sua substituição, problemas matemáticos complexos, para os quais não existe solução em tempo polinomial. O facto de não existir uma solução em tempo polinomial e de se usarem grandes números é o que confere segurança aos algoritmos baseados nesses problemas matemáticos.

Até agora foram usados fundamentalmente três tipos de problemas:

1. Fatorização
2. Cálculo de logaritmos discretos
3. Knapsacks

## Confidencialidade com cifras assimétricas

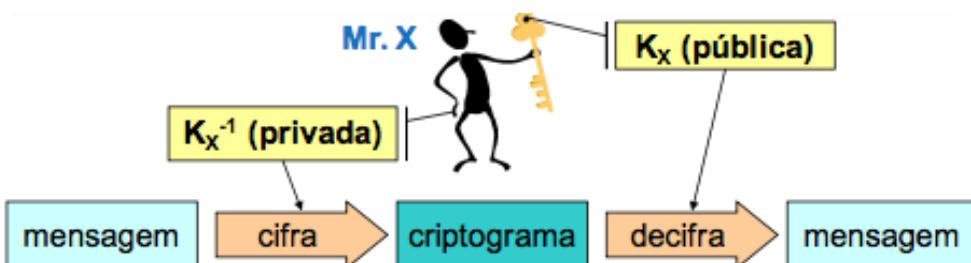
Ciframos com a chave pública de X e deciframos com a privada de X. Aqui a mensagem fica codificada e ninguém pode ter acesso ao conteúdo.



- Menos chaves
  - Para comunicar confidencialmente com X basta conhecer a chave pública de X
- Não há autenticação
  - X não sabe quem produziu o criptograma
  - Se a chave pública de X for efetivamente pública, qualquer um o pode fazer

## Autenticidade da fonte com cifras assimétricas

Cifra com a chave privada e decifra com a chave pública o que não tem qualquer interesse para esconder a informação, mas é importante para garantir a autoria.



- O criptograma não pode ser alterado
  - Só X conhece a chave privada com que foi gerado
- Não há confidencialidade
  - Quem conhecer a chave pública decifra o criptograma
  - Se a chave pública for verdadeiramente pública, qualquer um o pode fazer

### • Caso de Estudo: RSA

- Este algoritmo baseia a sua segurança na complexidade de fatorização e cálculo de logaritmos modulares (de grandes números).

Valores públicos	$n$	valor de grande dimensão (centenas de bits), produto de dois grandes primos $p$ e $q$ secretos
Chave pública	$e$	$e < n$ , coprimo de $\phi(n) = (p - 1)(q - 1)$
Chave privada	$p, q, d$	$d < n$ , $e \cdot d \equiv 1 \pmod{\phi(n)}$
Cifra	$C = P^e \pmod{n}$	
Decifra	$P = C^d \pmod{n}$	

- Para decifrar um valor cifrado com a chave pública  $e$ , é preciso conhecer a chave privada  $d$ .

- O RSA pode igualmente ser usado com um algoritmo de assinatura...

### • Caso de Estudo: ElGamal

- Este algoritmo baseia a sua segurança apenas na complexidade de cálculo de logaritmos modulares (de grandes números). A complexidade inerente ao cálculo de logaritmos discretos de grandes números impede que: 1. de  $y$  se consiga obter a chave privada de  $x$ ; 2. de  $c_1$  se consiga obter  $k$ , com o qual seria trivial recuperar o texto em claro a partir de  $c_2$ . O valor de  $k$  deve ser, por isso, gerado aleatoriamente para cada cifra e descartado logo após para evitar a divulgação.

Valores públicos	$p$ $g$	valor primo de grande dimensão (centenas de bits) elemento primitivo módulo $p$ , ou de $\mathbb{Z}_p$
Chave privada	$x$	$0 \leq x < p$
Chave pública	$y$	$y = g^x \pmod{p}$
Cifra	$C = (c_1, c_2)$	valor aleatório secreto $k < p - 1$ $c_1 = g^k \pmod{p}$ $c_2 = P \cdot y^k \pmod{p}$
Decifra		$P = c_2 \cdot (c_1^x)^{-1} \pmod{p}$ , onde $c_1^x \cdot (c_1^x)^{-1} \equiv 1 \pmod{p}$

- A cifra de ElGamal é um exemplo de cifra homofônica (isto porque textos em claro iguais e cifrados com a mesma chave pública  $y$  podem originar valores diferentes, dependendo do valor de  $k$  escolhido antes de efetuar a cifra).

- O algoritmo de ElGamal é mais lento do que o RSA, especialmente nas operações de cifra, porque no caso do RSA se podem escolher valores pequenos para chaves públicas, acelerando muito a operação de cifra.

## Randomização de Cifras com Chave Pública

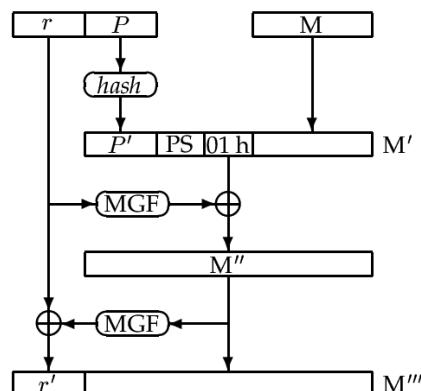
O resultado de uma cifra com chave pública não deverá ser determinístico (previsível)

- N cifras do mesmo valor, com a mesma chave, devem produzir N resultados diferentes
- Objetivo: impedir a descoberta de valores cifrados por tentativa erro

Técnicas:

- Concatenação do valor a cifrar com dois valores
  - um fixo (para controlo de erros)
  - um aleatório (para randomização)

### • OAEP (Optimal Asymmetric Encryption Padding)



## Aplicações das cifras por blocos: Modos de cifra

Um modo de cifra estabelece um modelo de aplicação de um algoritmo de cifra a um texto de dimensão arbitrária. O modo de cifra manipula blocos de texto e de criptogramas, os quais compõe de diferentes maneiras antes e depois da sua efetiva cifra ou decifra através de um algoritmo de cifra por blocos.

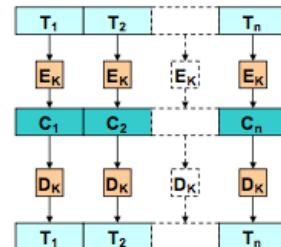
### Modos de cifra propostos inicialmente para o DES

- ECB (Electronic Code Book)
- CBC (Cipher Block Chaining)
- OFB (Output Feedback Mode)
- CFB (Cipher Feedback Mode)
- CTR (Counter)

#### • ECB (Electronic Code Book)

- Permite o acesso aleatório ao conteúdo do ficheiro
- O modo de cifra ECB é o método mais simples e intuitivo de usar uma cifra por blocos. Útil para cifrar grandes quantidades de dados.
  - Consiste em dividir a mensagem em blocos de tamanho adequado, cifrar os blocos em separados e concatenar os blocos cifrados na mesma ordem.
  - Na decifra é seguido o mesmo processo.
  - O grande inconveniente desta técnica é que os blocos de mensagem original idênticos vão produzir blocos cifrados idênticos - ou seja, não oculta padrões de dados.
  - Produz protocolos de criptografia sem garantia de integridade e bastante suscetíveis a ataques de replicação, pois cada bloco é decifrado de igual forma
  - Não oferece uma perfeita confidencialidade da mensagem e não é recomendado para uso em protocolos criptográficos.

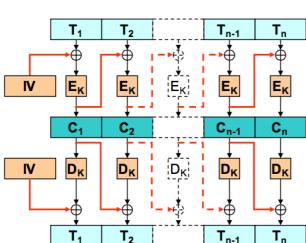
Problema	Solução
Reprodução de padrões do texto original	Uso de blocos de maior dimensão ou outro modo de cifrar CBC



#### • CBC (Cipher Block Chaining) - Evita o inconveniente do ECB

- O acesso aleatório ao conteúdo do ficheiro só é possível na decifra
- Cada bloco de texto simples é submetido a uma operação XOR com o bloco de texto cifrado anterior, antes de ser criptografado por algum algoritmo de criptografia.
  - Consequentemente, o mesmo bloco de texto simples não é mais mapeado para o mesmo bloco de texto cifrado, o que leva a que deixe de ser uma grande cifra de substituição monoalfabética.
  - O primeiro bloco de texto simples é submetido a uma operação XOR com um vetor de inicialização (escolhido ao acaso), o que tem de ser transmitido (em texto simples) juntamente com o texto cifrado.
  - Na decifra é seguido o processo inverso, ou seja, cada bloco decifrado é somado com o bloco anterior do criptograma para recuperar o bloco de texto original.

Vantagem	Problema
O mesmo bloco de texto simples não resultará no mesmo bloco de texto cifrado	Como não pode ser usado em paralelo (pois depende do resultado anterior) o seu uso dificulta o processamento de blocos em paralelo, o que melhoraria o desempenho do método



Um vetor de inicialização é um meio de aumentar a segurança da cifra através da introdução de um grau de aleatoriedade.

CFB - O acesso aleatório ao conteúdo do ficheiro só é possível na decifra

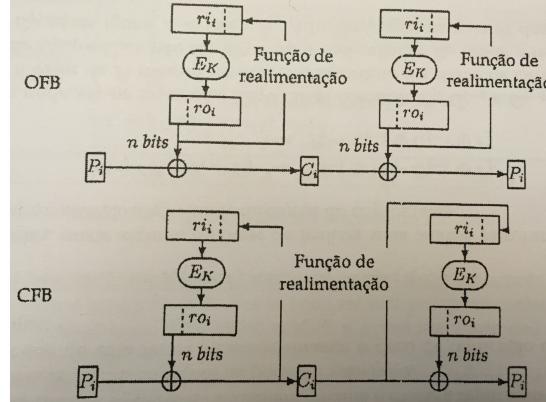
- **OFB (Output Feedback Mode) e CFB (Cipher Feedback Mode)**

- Os modos de cifra OFB e CFB transformam uma cifra por blocos numa cifra contínua. Útil para cifrar quantidades muito pequenas de dados (bytes)
- Cifragem: O VI é iniciado aleatoriamente; o algoritmo de criptografia (DES, AES) opera sobre o deslocamento para gerar um texto cifrado.

O byte da extremidade mais à esquerda do registador de deslocamento de R é registado. Uma operação XOR é feita com o byte em vez do texto simples P. O byte é cifrado e transmitido.

- Decifragem: Funcionamento idêntico como na cifragem.
- Problemas: Se um bit de um texto cifrado for invertido accidentalmente durante a transmissão, os bytes no registador do deslocamento R no receptor, serão danificados, enquanto o byte defeituoso estiver no registador de deslocamento.
- Deste modo, os efeitos de um único bit invertido são relativamente localizados e não arruinam a restante mensagem. Mas, arruinam uma quantidade de bits igual ao comprimento do registador de R de deslocamento

Modo de Funcionamento	Diferenças
O gerador de cifra contínua é constituído por uma função de cifra por blocos, por 2 registos com o comprimento do bloco, $ri$ e $ro$ , e por uma função de realimentação. A função cifra com o conteúdo de $ri$ e guarda o resultado em $ro$ . Desse resultado, os $n$ bits mais significativos são usados para cifrar dados.	No OFB a realimentação é feita a partir da saída do gerador. No CFB a realimentação é feita a partir do criptograma

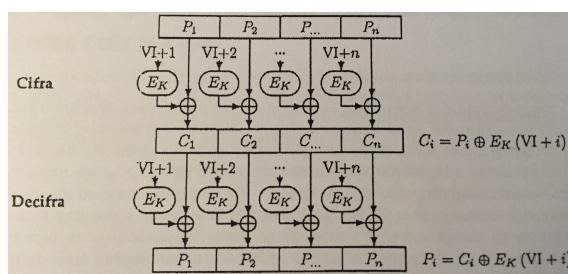


- O modo de OFB é análogo ao CFB, mas que pode ser utilizado em aplicações em que a propagação de erros não pode ser tolerada.

### CTR (Counter)

Permite o acesso aleatório ao conteúdo do ficheiro

- Um problema apresentado por CBC, CFB, excepto ECB é a impossibilidade de conseguir acesso aleatório a dados codificados, os ficheiros em disco são acedidos em ordem não sequencial.
  - No caso de um ficheiro codificado por CBC, o acesso a um bloco aleatório exige primeiro a decifragem de todos os blocos anteriores, ou seja, uma proposta dispendiosa.
  - Esta é a razão de se criar um modo contador, o texto inicial não é cifrado diretamente e o vetor VI é somado a uma constante inteira e cifrada.
- O texto cifrado resultante é submetido a um XOR com o texto simples.
- Aumentando o VI numa unidade a cada novo bloco do texto simples para ser cifrado, facilita a decifragem de um bloco em qualquer lugar no arquivo, sem que seja necessário, primeiramente decifrar todos os seus blocos precedentes.
- A cifra do  $i$ -ésimo bloco  $P_i$  é feita somando-o, bit a bit e módulo 2, com o resultado da cifra de  $VI + i$  com a chave  $K$ , onde  $VI$  é o valor inicial de um contador.
  - A decifra faz-se somando novamente o mesmo valor.



### Propagação de Erros

<b>ECB</b>	Este modo não apresenta problemas de propagação de erros entre blocos. Um erro afeta apenas um bloco de texto simples. Erros de perda de bits são irrecuperáveis.
<b>CBC</b>	Um erro num bit do criptograma afeta o bloco de texto original correspondente, e um bit no bloco seguinte. Erros de perda de bits são irrecuperáveis.
<b>CFB</b>	Um erro no criptograma tem como efeito imediato numa decifragem errada do bit de texto limpo correspondente.
<b>OFB</b>	Neste modo não há propagação de erros. Um erro no criptograma afeta apenas um bit no texto limpo. Erros de sincronização não são recuperáveis.

### • ~ Comparação ~

	ECB	CBC	OFB	CFB	CTR
<b>Não exposição padrões</b>		✓	✓	✓	✓
<b>Confusão na entrada da cifra</b>		✓		✓	contador secreto
<b>Mesma chave para mensagens diferentes</b>	✓	✓	outro IV	outro IV (contador)	
<b>Dificuldade de alteração</b>	✓	✓ (...)			
<b>Pré-processamento</b>			✓		✓
<b>Paralelização</b>	✓	decifra	com pré-processam.	decifra	✓
<b>Acesso aleatório uniforme</b>					
<b>Propagação de erros</b>		bloco seguinte		alguns bits seguintes	
<b>Capacidade de recuperar a sincronização</b>	perda de blocos	perda de blocos		perda de múltiplos de n-bits	

## **Problemas causados por sub-blocos**

As cifras por blocos, em alguns modos (ECB, CBC) têm de se aplicar a textos com dimensões múltipla do tamanho do bloco. Existem vários métodos para aumentar a dimensão do texto de forma previsível, tais como CypherText Stealing, PKCS#7 e PKCS#5. A este processo dá-se o nome de **padding**.

O **CypherText Stealing** é um método em que se roubam N bytes do final do penúltimo bloco cifrado, sendo que são adicionados estes bytes ao último bloco de texto de forma a tornar o texto múltiplo do tamanho do bloco.

O último bloco é depois cifrado e enviado como penúltimo bloco (troca-se a ordem entre último e penúltimo). O resultado é que a cifra ocorre normalmente mas o tamanho do criptograma não aumenta. No entanto, necessita que o texto ocupe um mínimo de 2 blocos.

Na decifra, depois de se decifrar o penúltimo bloco do criptograma, roubam-se de volta os bytes suficientes para compor o último bloco. Este depois é decifrado e volta-se a trocar a sua ordem (último pelo penúltimo). De notar que, os bytes roubados são sempre cifrados e decifrados duas vezes. No entanto, o número de blocos cifrados ou decifrados não se altera.

Este método é o mais complexo. Os outros métodos são mais simples mas têm o inconveniente de aumentar sempre o tamanho do criptograma.

O **PKCS#7** funciona adicionando bytes com o valor dos bytes em falta. Ou seja, se o último bloco tiver 5 bytes em falta para ser múltiplo do tamanho do bloco, são adicionados 5 bytes com valor 5.

O **PKCS#5** é igual mas apenas foi definido para blocos de 8 bytes (DES).

## Reforço de Segurança

- **Cifra múltipla**

- **Cifra Dupla**

- A cifra múltipla consiste em cifrar um texto mais do que uma vez, usando em cada cifra uma chave diferente. A segurança será, à partida, tanto maior quanto maior for o número de cifras independentes aplicadas, mas também o desempenho será menor.

- Ao usar chaves com  $n$  bits, consegue-se descobrir as chaves em  $2^{n+1}$  tentativas e não em  $2^{2n}$ , como seria de esperar. Teoricamente pouco segura.

- Pouco viável: Para realizar o algoritmo é necessário dispor muita memória.

- **Cifra Tripla (EDE)**

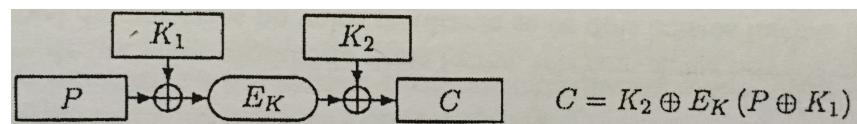
- Como forma de melhoria foi adoptada a cifra tripla, que usa três operações de cifra ou decifra e uma a três chaves distintas.

Número de chaves	Cifra tripla EDE	Decifra tripla EDE
1	$C = E_K(D_K(E_K(P)))$	$P = D_K(E_K(D_K(C)))$
2	$C = E_{K1}(D_{K2}(E_{K1}(P)))$	$P = D_{K1}(E_{K2}(D_{K1}(C)))$
3	$C = E_{K3}(D_{K2}(E_{K1}(P)))$	$P = D_{K1}(E_{K2}(D_{K3}(C)))$

Mais conhecida como EDE, onde se efetuam, sequencialmente um cifra, uma decifra e uma cifra. O modelo EDE é atrativo, em relação a outras combinações alternativas, porque permite compatibilizar cifras simples com cifras triples usando uma única chave, o que facilita a interação com aplicações ou equipamentos antigos. De facto, se usar-se cifra tripla EDE apenas com uma chave o resultado é equivalente a uma cifra simples (porque a cifra e decifra inicial anulam-se).

- **Branqueamento (Whitening)**

- Técnica simples e eficiente de efetuar cifra múltipla. Consiste em usar duas chaves extra, do comprimento do bloco usado pelo algoritmo de cifra, que se somam módulo 2 à entrada e à saída da cifra.



# Funções de Síntese (Digest)

- As funções de síntese (*digest functions*) não são propriamente funções criptográficas, uma vez que não servem para cifrar ou decifrar dados, mas são úteis para complementar, com segurança criptográfica, outros mecanismos de segurança.
- São úteis para gerar e validar assinaturas digitais, para calcular autenticadores de mensagens e para derivar chaves a partir de chaves mestras ou de senhas textuais.
- As funções de síntese produzem valores de dimensão constante a partir de textos de dimensão variável.

## Propriedades:

- Resistência à descoberta de um texto original - Dada uma síntese, é difícil encontrar um texto que o produza
- Resistência à descoberta de um 2º texto original \* - Dado um texto, é difícil encontrar um segundo texto com a mesma síntese
- Resistência à colisão - É difícil encontrar dois textos com a mesma síntese; paradoxo do aniversário
  - Sem estas três características não poderá ser classificada como função de síntese

As duas primeiras propriedades definem o caráter unidirecional das funções de síntese, sendo por isso também chamadas de dispersão unidirecionais.

Uma função de síntese com uma saída de  $n$  bits diz-se uma função de dispersão unidirecional ideal se a procura de um texto original ou de um segundo texto requerer  $2^n$  tentativas.

Aproximações	Aproximações
<ul style="list-style-type: none"><li>- Difusão e confusão em funções de compressão</li><li>- Construção Merkle-Damgard</li><li>-(compressão iterativa; padding com o comprimento)</li></ul>	<ul style="list-style-type: none"><li>- <b>MD5</b> - não é seguro; fácil de descobrir colisões</li><li>- <b>SHA1</b> - não se conhecem colisões</li></ul>

\* Se a segunda propriedade se verificar, então uma síntese é equivalente a uma impressão digital de um texto, no sentido em que é virtualmente única (como as impressões digitais dos humanos), não é forjável e pode servir, por isso, para identificar ou representar o texto. Uma consequência da segunda propriedade é que, para complicar a pesquisa adaptativa de colisões, textos muito parecidos geram sínteses muito diferentes. Esta propriedade é comum às funções de cifra por blocos, onde blocos de texto muito parecidos cifrados com a mesma chave produzem criptogramas muito diferentes.

# **Autenticadores de dados**

Os autenticadores de dados são conjuntos de *bits* que acompanham mensagens e que garantem a sua correção e origem. Os valores gerados apenas a partir das mensagens por funções de síntese não são, por si só, suficientes para este fim, porque apenas garantem correção mas não origem.

## **Autenticadores de mensagens (MAC - Message Authentication Code)**

Um autenticador de mensagem é um valor produzido a partir de uma mensagem e de uma chave simétrica partilhada pelo emissor e pelo receptor da mesma.

Assim, um MAC autentica uma mensagem de forma a garantir a integridade (alteração da informação) e autenticação (validar a emissão).

Um MAC apenas pode ser gerado e validado por estas duas entidades (chave simétrica partilhada).

- **Produção de um MAC:**

- Cifrar uma mensagem e a sua síntese com uma cifra por blocos. Esta cifra pode abranger estas duas componentes ou apenas uma delas. No entanto, deve-se evitar a cifra apenas da síntese porque tal fornece dados úteis para uma criptanálise com texto conhecido da chave partilhada.
- Usar funções de cifra específicas, baseadas em:
  1. funções de cifra por blocos;
  2. funções de cifra contínua;
  3. funções de síntese.

- **Caso de estudo: CBC-MAC**

Gera um MAC que é um conjunto de bits do último bloco do criptograma gerado com uma cifra por blocos em modo CBC. Este algoritmo é eficaz para autenticar mensagens de com igual comprimento mas permite a geração de mensagens válidas juntando outras autenticadas com a mesma chave.

- **Caso de estudo: DES-MAC**

Gera um MAC que é um conjunto de bits do último bloco do criptograma gerado com DES em modo CBC ou CFB de 64 bits – no caso do CBC o VI é nulo já no CFB o VI é o primeiro bloco da mensagem.

- **Caso de estudo: Keyed-MD5**

Gera um MAC aplicando a função de síntese MD5 a um bloco de dados formado pela concatenação de uma chave com a mensagem de excipientes.

$$\text{Keyed-MD5} = \text{MD5} ( k | \text{keyfill} | \text{mensagem} | k )$$

- **Caso de estudo: HMAC**

É semelhante ao Keyed-MD5, mas mais robusto e versátil porque pode ser usado como diversas funções de síntese.

Gera um MAC aplicando a função de síntese 2 vezes, uma dita interior (inner) onde são processados a chave e a mensagem e outro exterior (outer) onde se processam a chave e a síntese interior.

$$\text{HMAC} = h [ k \oplus \text{opad} | h (k \oplus \text{ipad} | \text{mensagem}) ]$$

# Assinaturas Digitais

O objetivo das assinaturas digitais é ir mais longe na garantia de origem e assegurar a autoria de uma mensagem perante terceiros. Uma mensagem assinada digitalmente deverá ser associável a uma e uma só entidade e assinatura deverá poder ser validada universalmente.

A criptografia assimétrica é a que melhor se adequa a este fim, uma vez que os pares chaves têm um cariz pessoal (pertencem apenas a uma entidade).

Uma assinatura digital de um documento consiste na cifra do mesmo com a chave privada do autor ou subscritor do documento. O criptograma resultante não serve para esconder o documento original mas sim para garantir, a quem o decifrar com a chave pública correspondente, que o texto recuperado, esteja igual ao original, está correto e foi assinado pelo detentor da chave pública.

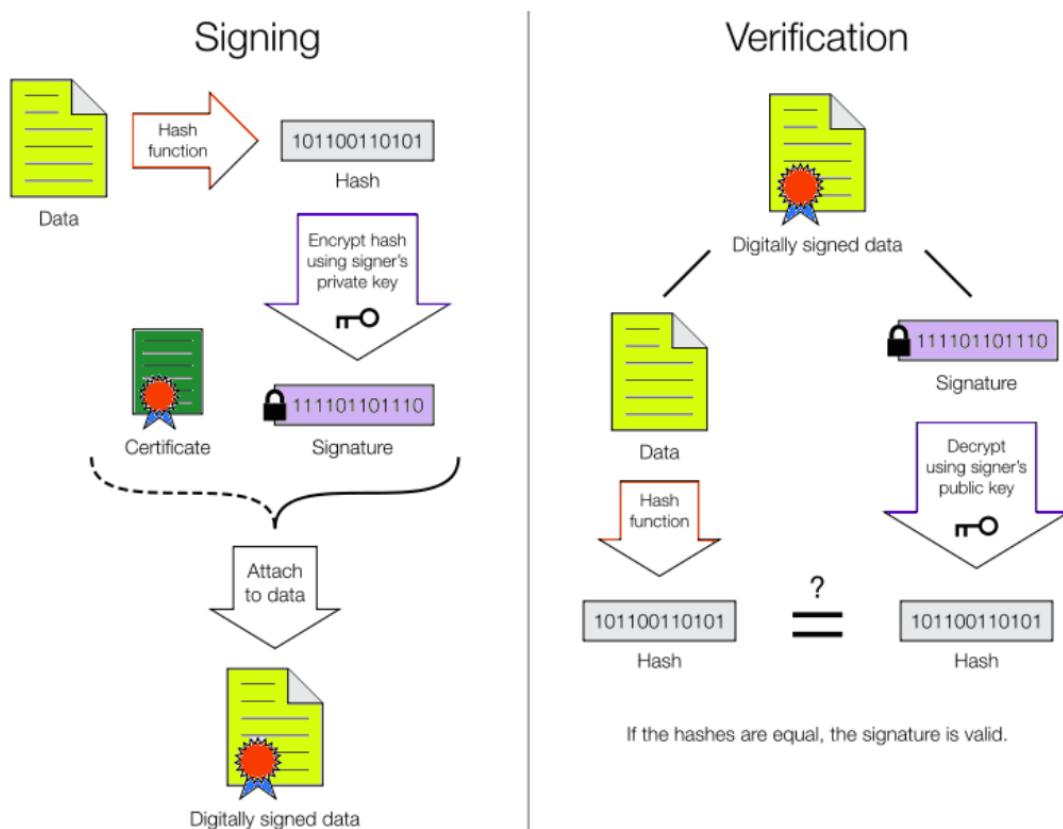
Assim, uma assinatura digital de um documento é muito semelhante a uma assinatura convencional em papel, no sentido em que associa um autor ao documento e permite que tal associação seja validada por terceiros.

Autenticar o conteúdo de um documento	Autenticar o seu assinante	Pode assegurar a autenticação perante terceiros
- Garantir a sua integridade	- Assegurar a identidade do criador/originador	- Os autores genuínos não podem negar a autoria; não-repúdio

## Aproximações usadas

- Cifra de chave pública
- Funções de síntese (apenas para aumentar o desempenho!)

$$\text{Geração: } A_X = \text{Info}, E_{K_X^{-1}}(h(\text{Info}, \text{Doc}))$$
$$\text{Validação: } D_{K_X}(A_X) \equiv h(\text{Info}, \text{Doc})$$



## **Assinaturas às cegas**

Uma assinatura diz-se às cegas quando quem assim não sabe o que está a assinar - o grau de desconhecimento vai ao ponto de quem assina, mais tarde, não ser capaz de reconhecer uma sua assinatura específica.

O objetivo final é o de impedir que o assinante consiga associar o requisitante da assinatura aos dados que este último lhe pede para assinar.

### **Servem para garantir o anonimato e a não alteração da informação assinada**

- O assinante X sabe quem lhe pede a assinatura (Y)
- X assina T1, mas Y depois recupera a assinatura sobre T2 (T2 está relacionado com T1)
- O requerente pode apresentar T2 assinado por X (mas não pode alterar T2; X não consegue associar T2 ao T1 que viu e assinou)

**Obscurecimento:**  $m = h(Doc), m' = f_{\text{obscurecimento}}(m)$

**Assinatura normal:**  $A_X(m') = E_{K_X^{-1}}(m')$

**Anulação do obscurecimento:**  $A_X(m) = f_{\text{obscurecimento}}^{-1}(A_X(m'))$

### **Exemplos:**

- Nos protocolos de pagamento eletrónico as assinaturas às cegas são úteis para permitir o anonimato do dinheiro de uma pessoa entregue pelo banco, onde essa pessoa tem conta, a um comerciante onde essa pessoa comprou algo. O objetivo final é evitar que o banco que gere o dinheiro do comprador consiga saber quais as lojas que frequenta e os bens que adquire, ou seja, tornar as transferências electrónicas de dinheiro tão anónimas quanto o são as transferências de dinheiro em numerário.
- Nos protocolos de votação electrónica as assinaturas às cegas são úteis para validar boletins de voto pertencentes a votantes autorizados sem conseguir fazer qualquer ligação entre a assinatura gerada, o voto e o votante.

# Capítulo 4

## Gestão de chaves assimétricas

---

### Problemas a resolver

- Assegurar uma geração apropriada dos pares de chaves
  - Geração aleatória de valores secretos
  - Aumentar eficiência sem reduzir a segurança
- Assegurar um uso apropriado dos pares de chaves assimétricas
  - Uso / conhecimento exclusivo das chaves privadas
    - para impedir o repúdio das assinaturas digitais
  - Distribuição correta das chaves públicas
    - para assegurar confidencialidade
    - para assegurar uma correta validação de assinaturas digitais
- Evolução temporal das relações entidade <-> par de chave
  - Para lidar com situações catastróficas (ex: perda da chave privada)
  - Para lidar com requisitos operacionais normais (ex: refrescamento de pares de chaves para reduzir riscos de personificação)

### Cuidados a ter

- A chave privada deve ser gerada pelo próprio
  - Para assegurar ao máximo a sua privacidade
  - Este princípio pode ser relaxado se não pretender assinaturas digitais
- Uso correto
  - A chave privada representa o próprio
    - o seu comprometimento tem de ser minimizado
    - cópias de salvaguarda fisicamente seguras
  - O caminho de acesso à chave privada deveria ser controlado
    - proteção com senha ; correção das aplicações que a usam
- Confinamento
  - Salvaguarda e uso da chave privada num dispositivo autónomo (ex: smartcard)
  - O dispositivo gera pares de chaves
  - O dispositivo apenas envia para o exterior a chave pública - e nunca a privada
  - O dispositivo cifra / decifra dados com a chave privada

## Distribuição de chaves públicas

- Distribuição aos remetentes de dados confidenciais
  - Manual
  - Usando um segredo partilhado
  - Distribuição *ad hoc* usando certificados digitais
    - a distribuição *ad hoc* consiste na possibilidade de importação de uma chave pública, a partir de vários repositórios públicos. Para isso é preciso garantir que a cópia importada é correta, ou seja, que é mesmo a chave pública da entidade pretendida. Essa garantia é realizada a partir de certificados digitais.
- Distribuição aos receptores de assinaturas digitais
  - Distribuição *ad hoc* usando certificados digitais

## Certificados Digitais de Chaves Públicas

A certificação digital consiste na emissão de certificados digitais de chaves públicas. Os certificados são documentos com uma estrutura predefinida que possuem, entre outros elementos, uma chave pública de uma dada entidade e uma assinatura digital do certificado feita pela entidade emissora do mesmo.

Os certificados são documentos com um tempo de validade limitado. Esse tempo pode ser controlado de duas formas: através de um prazo de validade não alterável indicado no próprio certificado e através de certificados de revogação.

- Documentos emitidos por uma Entidade Certificadora (EC)
  - Certification Authority (CA)
  - Associam uma chave (pública) a uma entidade
    - pessoa, servidor, serviço
  - São documentos públicos
    - não contêm informação privada, apenas pública
  - São criptograficamente seguros
    - assinados digitalmente pelo emissor
- Úteis para a distribuição confiável de chaves públicas
  - O receptor do certificado pode validar o mesmo
    - usando a chave pública da CA
  - Se confiar no assinante (CA) e a assinatura estiver correta, pode confiar na chave pública certificada
    - como a CA confia na K+ certificada, se confiar em KCA+ pode confiar em K+

Padrão X.509v3	PKCS #6	Formatos Binários	Outros formatos
<ul style="list-style-type: none"><li>• Campos obrigatórios<ul style="list-style-type: none"><li>- <u>versão</u>; <u>sujeito</u> (nome da entidade a quem a chave pertence); <u>chave pública e respetivo algoritmo</u>; <u>datas</u> (de emissão, de validade); <u>emissor</u> (nome da entidade emissora de certificado); <u>assinatura</u>; <u>número de série</u></li><li>• Extensões</li></ul></li></ul>	<ul style="list-style-type: none"><li>• Extended-Certificate Syntax Standard</li></ul>	<ul style="list-style-type: none"><li>• ASN.1</li><li>- DER, CER, BER</li><li>• PKCS #7</li><li>- Cryptographic Message Syntax Standard</li><li>• PKCS #12</li><li>- Personal Information Exchange Syntax Standard</li></ul>	<ul style="list-style-type: none"><li>• PEM (Privacy Enhanced Mail)</li><li>• Codificação de X.509 em base64</li></ul>

## Entidades Certificadoras

- Organizações que gerem certificados

- Definem políticas e mecanismos para:
  - Emitir / Revogar / Distribuir certificados
  - Emitir e distribuir as chaves privadas correspondentes
  - Gerem listas de revogação de certificados

- CAs confiáveis

- CAs para as quais se possui uma chave pública confiável
  - Âncora de confiança
    - Normalmente concretizada através de certificados autoassinados (ou autocertificados, sujeito=emissor)
  - Distribuição manual das suas chaves públicas
    - ex: nos navegadores (Internet Explorer, Netscape, etc...)
- CAs certificados por outras CAs
  - Certificados de chave pública de CAs ; Hierarquias de certificação

## Renovação de Pares de Chaves Assimétricas

- Os pares de chaves devem ter um período de validade limitado

- Porque as chaves privadas podem-se perder / ser descobertas
- Para lidar com políticas de alteração regular de chaves assimétricas

- Problema

- Os certificados podem ser reproduzidos sem qualquer controlo
- Não se conhece o universo de detentores de um certificado que pretende eliminar
  - portanto, não se podem contactar para eliminar determinados certificados

- Soluções

- Certificados com prazos de validade
- Listas de revogação de certificados
  - para certificados revogados antes do termo do seu prazo de validade

## Lista de Certificados Revogados (CRL)

- Criado para facilitar a renovação de pares de chaves assimétricas.

É uma lista disponibilizada publicamente por uma PKI X.509v3 com todos os seus certificados que foram revogados e cujo prazo de validade ainda não expirou. Esta lista contém, para cada certificado revogado, uma entrada que possui informação relevante sobre o mesmo, a razão para a sua revogação e a data da mesma.

- Certificate Revocation Lists

- base ou delta

- São listas assinadas de identificadores de certificados revogados antecipadamente

- Devem ser consultadas regularmente pelos detentores de certificados
- Protocolo OCSP para certificados X.509 individuais (RFC 2560)
- Podem indicar a justificação da revogação

- Manutenção e divulgação das CRL

- Cada CA mantém e permite a consulta da sua CRL
- As CAs trocam listas entre si para facilitar o conhecimento das CRL

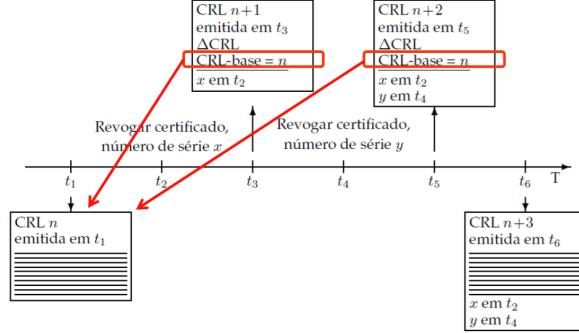
- **Distribuição das CRL**

- **Distribuição integral**

- É fornecida a lista completa de certificados revogados e não expirados relativos a uma PKI numa dada data.
- Numa distribuição integral, uma CRL mais recente anula completamente uma CRL mais antiga.

- **Distribuição parcial**

- São fornecidas CRL parciais, denominadas delta CRL, criadas com base numa CRL completa de referência.
- **DELTA CRL**: possuem apenas entradas relativas a certificados que entraram ou saíram da CRL de referência. Sabendo esta última, é possível ir mantendo atualizada uma lista própria de certificados de revogação atualizando a mesma com as entradas da última delta CRL.
- As principais diferenças entre os elementos que constituem uma CRL completa e uma delta CRL é que esta última pode referir a remoção de entradas (ou seja, de certificados de revogação) e tem sempre de referir o identificador da CRL completa de referência.



Desvantagem: A principal desvantagem do CRL é que pode criar uma grande sobrecarga enquanto o cliente pesquisa sobre a lista de revogação

## OCSP - Online Certificate Status Protocol

Protocolo simples de pergunta-resposta onde é questionado o certificado a consultar através do seu número de série.

A principal vantagem é o cliente poder consultar o estado de um único certificado, em vez de descarregar e analisar uma lista inteira (menos sobrecarga para cliente e rede).

A principal desvantagem é que os pedidos são enviados para cada certificado, devido a isso pode haver uma sobrecarga sobre o OCSP Responder para sites de alto tráfego.

## PKI - Public Key Infrastructure

- Infra-estrutura de apoio ao uso de chaves públicas

- Criação segura de pares de chaves assimétricas
- Criação e distribuição de certificados de chaves públicas
- Definição e uso de cadeias de certificação
- Atualização, publicação e consulta de listas de certificados revogados
- Uso de estruturas de dados e protocolos que permitem a inter-operação entre componentes

## PKI - Exemplo: Políticas do Cartão Cidadão

### Inscrição

- Em locais próprios, pessoal

### Vários pares de chaves por pessoa

- Um para autenticação
- Uma para assinaturas qualificadas
- Ambos gerados dentro do cartão, não exportáveis
- Ambos requerem um PIN em cada operação

### Uso autorizado dos certificados

- Autenticação
  - SSL Client Certificate, Email (Netscape cert. type)
  - Signing, Key Agreement (key usage)
- Assinatura
  - Email (Netscape cert. type)
  - Non-repudiation (key usage)

### Caminho de certificação

- raiz bem conhecida e amplamente divulgada
  - GTE Cyber Trust Global Root
  - CA raiz PT debaixo da GTE
  - CA raiz CC debaixo de CA raiz PT
  - CAs Autenticação CC e Assinatura CC debaixo CA raiz CC

### CRLs

- Certificados de assinatura pré-revogados por omissão
  - A revogação é removida se o dono do CC explicitamente requerer o uso de assinaturas digitais
- Todos os certificados são removidos a pedido do dono
  - Mediante a apresentação de um PIN de revogação
- Os pontos de distribuição das CRL estão explicitamente indicados em cada certificado

## PKI - Exemplo: Políticas do Cartão Cidadão

- Um PKI estabelece relações de confiança de duas formas

- Emitindo certificados de chaves públicas de outras CAs
  - abaixo na hierarquia; ou não relacionadas hierarquicamente
- Requerendo a certificação da sua chave pública a outras CAs
  - acima na hierarquia; ou não relacionadas hierarquicamente

- Relações de confiança características

Hierárquicas	Cruzadas	Ad-Hoc
	A certificação cruzada é uma forma prática de lidar com o problema de validação de certificados pertencentes a hierarquias de certificação diferentes. A certificação cruzada consiste na emissão recíproca de certificados de chaves públicas entre duas EC, tipicamente duas EC raiz.	A distribuição ad-hoc consiste na possibilidade de importação de uma chave pública, em caso de falta da mesma, a partir de vários repositórios públicos. Para que tal seja possível, é preciso garantir que a cópia importada é correta, ou seja, que é mesmo a chave pública da entidade pretendida. Essa garantia de correção é dada através de um processo de certificação digital.

# Capítulo 5

## Cartão de Cidadão

O cartão de cidadão é um *smartcard*, porque possui um microcomputador embbebido (*chip*).

### Funcionalidades

- **Guardar informação pessoal** - para validação informática interna da identidade do titular. Concretamente, esta informação é constituída por elementos descritivos de impressões digitais do titular.
- **Guardar informação privada** - informação que o titular pode usar, mas não conhecer ou divulgar. Concretamente, esta informação é constituída por três chaves criptográficas:
  - Uma chave simétrica de autenticação do titular
  - Uma chave privada de um par de chaves assimétricas RSA, que serve para autenticar o titular.
  - Uma chave privada de um par de chaves assimétricas RSA, que serve para produzir assinaturas digitais do titular
- **Guardar informação reservada** - informação que o titular conhece mas que apenas disponibiliza de forma fidedigna, via *smartcard* - morada do titular.
- **Guardar informação pública de grande dimensão, não memorizável** - esta informação é constituída pela fotografia do titular e por certificados X.509v3 de chaves públicas do titular, chaves essas que podem ser usadas para autenticar o titular ou a sua assinatura.
- **Guardar informação observável no CC** - fotografia, nome, data nascimento, diversos números de identificação, validade do cartão
- **Efetuar operações criptográficas usando as chaves que fazem parte da sua informação privada**

### Atributos informáticos

Morada	Template de impressão digital biométrica	2 pares de chaves criptográficos (Assinatura e Autenticação)	7 certificados de chave pública	1 chave secreta, simétrica para EMV-CAP	4 PIN
			- 2 relativos às chaves do próprio - 5 para indicar a cadeia de certificação	<i>Europay, MasterCard, and Visa Chip Authentication Program</i>	

## Proteção por PIN

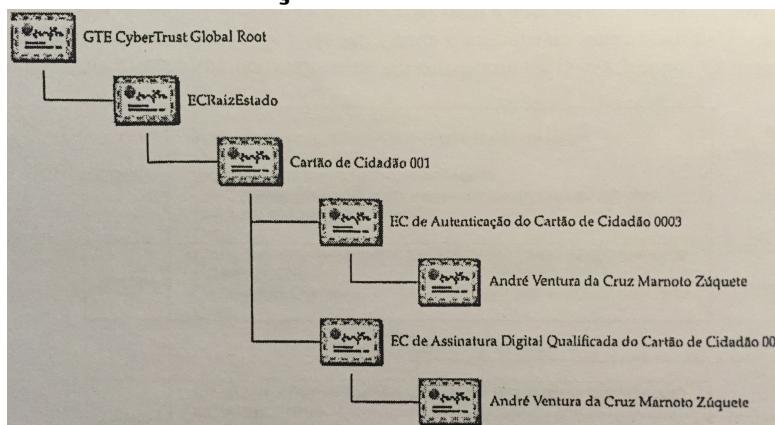
- Possuir o cartão é insuficiente para
  - Obter morada
  - Obter / usar a chave privada de autenticação
  - Obter / usar a chave privada de assinatura
  - Obter / usar a chave secreta da EMV-CAP
- Operações protegidas por PIN
  - PIN de 4 números
  - PIN é bloqueado após 3 tentativas incorretas
- Exceções
  - Forças policiais podem obter a morada sem o PIN

## Assinaturas digitais com o Cartão Cidadão

O Cartão de Cidadão possui um par de chaves assimétricas de assinatura digital qualificada, para assinar documentos. O *smartcard* possui e disponibiliza um certificado X.509v3 com a chave pública de validação da assinatura digital qualificada do titular.

- Como ativar a assinatura digital
  - Através da publicação de um certificado de revogação, na CRL da sua EC, das credenciais de assinatura digital presentes no *smartcard*.
- CC tem 2 pares de chaves criptográficos (autenticação e assinatura)

## Hierarquias de certificação no Cartão Cidadão



7 certificados de chave pública: 2 relativas às chaves do próprio, 5 para indicar a cadeia de certificação

## Certificados no SmartCard: Objetivos

- Possibilita autenticar o dono do cartão
  - O dono pode distribuir o seu certificado para outras pessoas/serviços que passa a poder verificar a sua identidade
- Possibilita o dono autenticar outras pessoas com cartões semelhantes
  - Cadeia de certificação presente no cartão
- Possibilita o cartão autenticar clientes com certificados semelhantes
  - Algumas operações podem ser pedidas ao cartão com certificados “especiais” que o cartão valida

# **Smartcards**

Cartão com capacidade de computação.

## **Componentes**

CPU	ROM	EEPROM
•8/16 bit •Crypto-coprocessor	•Sistema Operativo •Comunicação •Algoritmos criptográficos	•Sistema de Ficheiros - programas / aplicações - chaves / passwords
RAM	Contactos Mecânicos	Segurança Física
•Dados temporários - apagados quando cartão é desligado	•ISO 7816-2 - power ; soft reset ; clock ; half duplex I/O	•Resistente a acessos físicos diretos •Resistente a ataques por canais paralelos

## **Aplicações em SmartCards: Exemplo Cartão Cidadão**

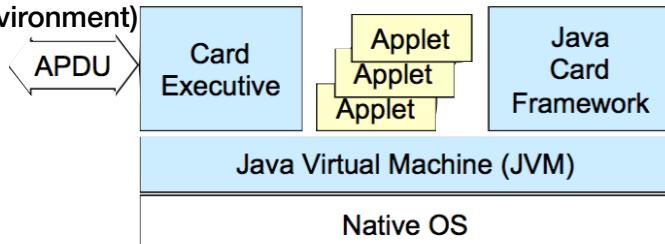
IAS	EMV-CAP	Match-on-Card
•Autenticação e assinatura digital •Utilização de pares de chave assimétricas	•Geração de one-time-password para canais alternativos (telefone, fax, etc)	•Validação de impressões digitais

## **Modelo de computação do Smartcard: Cartões Java**

- Smartcards executem Applets Java
  - Utilizam o JCRE
  - O JCRE executa no topo do SO nativo

### • JCRE (Java Card Runtime Environment)

- Java Virtual Machine
- Card Executive
  - Gestão do Cartão
  - Comunicações
- Java Card Framework
  - Bibliotecas de funções



## **Serviços criptográficos do Smartcard: Middleware**

Para fazer a ponte entre uma aplicação e um conjunto alargado de smartcards é preciso que exista um middleware que permita usar diversos tipos de smartcards e que as aplicações estejam preparadas para utilizar esses middleware.

### • No caso do Cartão de Cidadão:

- Existem dois tipos de middleware:
  1. pteidpkcs11 - é o que permite usar o Cartão de Cidadão como um dispositivo criptográfico. São disponibilizadas bibliotecas PKCS #11 com um subconjunto da interface Cryptoki
  2. pteidl1ib - permite realizar operações com o Cartão de Cidadão que são específicas da sua natureza de documento de identificação e que não têm paralelo nos dispositivos criptográficos.

# Capítulo 6

## Protocolos de Identificação

A autenticação de entidades consiste na obtenção de um comprovativo de que elas possuem um atributo que afirmam possuir, ou que é suposto que possuam.

A autenticação de entidades envolve um processo de prova, na qual o autenticador obtém uma prova fidedigna de que a entidade autenticada, ou autenticado, possui o atributo que afirma possuir.

Um protocolo de autenticação é um conjunto de mensagens trocadas entre vários interlocutores e que tem por objetivo realizar a autenticação de um ou mais deles perante um ou mais dos demais.

### Caracterização dos protocolos de autenticação

#### • Elementos de prova

São usados três tipos de paradigmas em termos de elementos de prova:

- *O que sabe*: Uma entidade prova a sua autenticidade mostrando que conhece uma determinada informação secreta, denominada genericamente por senha. Se a senha for conhecida pelos intervenientes diretos no processo de autenticação, pode provar que o interlocutor é quem afirma ser.
- *O que possui*: Neste paradigma uma entidade prova a sua autenticidade mostrando que possui um determinado dispositivo de segurança ou que é o dono legítimo desse dispositivo de segurança.
- *O que se é*: Neste paradigma é apresentado alguma característica que permite diferenciar das demais. Normalmente este paradigma aplica-se a humanos e a característica diferenciadora é obtida através da biometria.

Quando se usam estes três paradigmas combinados diz-se que a sua autenticação é multimétodo.

### Autenticação

#### • Objetivos

- Autenticar entidades interatuantes
  - pessoas, serviços, servidores, máquinas, redes, etc
- Permitir aplicação de políticas e mecanismos de autorização
  - autorização -> autenticação
- Apoiar outras ações no âmbito de segurança
  - distribuição de chaves para comunicação segura

#### • Requisitos

Confiança	Secretismo	Robustez
Nível de confiança	Não divulgação de credenciais usadas pelas entidades legítimas	<ul style="list-style-type: none"><li>- Impedir ataques às trocas de dados do protocolo</li><li>- Impedir cenários de DoS interativos</li><li>- Impedir ataques desligados com dicionários</li></ul>
Simplicidade	<b>Lidar com vulnerabilidades vindas de pessoas</b>	
Deverá ser tão simples quanto possível para evitar que os utentes escolham simplificações perigosas	Têm uma tendência natural para facilitar ou para tomarem iniciativas perigosas	

- *Entidades e modelos de implantação*

Entidades	Modelos de Implantação
Pessoa Máquinas Redes Serviços / Servidores	- Ao longo do tempo - quando a interação se inicia - continuamente ao longo da interação - Direcional - unidirecional - bidirecional

## Protocolos de Autenticação: Aproximações Elementares

- *Aproximação Direta*

Apresentar credenciais e esperar pelo veredicto

- *Aproximação com Desafio-Resposta*

É lançado um desafio, o utilizador responde e é calculado e fornecido uma resposta com base no desafio e nas credenciais. Espera-se pelo veredicto.

## Autenticação de pessoas

### - Aproximação Direta com senha memorizada

<b>Funcionamento</b>	A senha é confrontada com um valor guardado para a pessoa que está a ser autenticada, dada a sua entidade reclamada ( <i>username</i> ) Valor pessoal guardado
<b>Vantagens</b>	Simplicidade
<b>Problemas</b>	Utilização de senhas fracas/inseguras (permite ataques por dicionário) Transmissão de senhas em claro em canais de comunicação inseguros (escutas podem revelar senhas)

### - Aproximação Direta com biometria

A autenticação biométrica baseia-se na avaliação de características físicas dos autenticadores para aferir a sua autenticidade face a uma identidade reclamada. Essas características podem ser diversas, e tanto fisiológicas e estáticas (dimensões e distâncias faciais) como comportamentos e dinâmicas (ritmo de escrita num teclado).

<b>Funcionamento</b>	- Uma pessoa autentica-se com as medidas do seu corpo (impressão digital, íris, geometria da face, timbre) - Estas medidas são comparadas com um registo pessoal e similar - através de uma referência biométrica
<b>Vantagens</b>	- As pessoas não necessitam de memorizar nada - As pessoas não necessitam de escolher senhas - As credenciais não podem ser transferidas entre pessoas
<b>Problemas</b>	- A biometria ainda está incipiente (início) - As pessoas não podem mudar as credenciais caso sejam roubadas - Pode criar riscos para as pessoas (remoção de partes do corpo para personificar a vítima) - Pode revelar informação pessoal sensível (doenças) - Não é uma solução interessante e segura para autenticações remotas - Não é um método de autenticação ideal quando se tem muitos clientes

## - Aproximação Direta com senhas descartáveis

A autenticação com senhas descartáveis é um tipo de autenticação com apresentação direta de credenciais onde as mesmas nunca se repetem, só são usadas uma vez. Este tipo de autenticação é interessante quando se pretende evitar riscos que o mesmo apresenta quando as credenciais podem ser capturadas por terceiros e reutilizadas novamente.

Exemplos: RSA SecurID, matriz com códigos bancários



<b>Descrição</b>	<ul style="list-style-type: none"><li>- Senhas <i>one-time-password</i>, só se podem utilizar uma vez</li><li>- É uma solução interessante para criar sessões remotas sobre comunicação não seguras</li><li>- Pode envolver a troca de um desafio para indicar a senha descartável a ser usada</li></ul>
<b>Vantagens</b>	<ul style="list-style-type: none"><li>- Podem ser escutadas (isso não adianta a quem o fizer para personificar o dono da senha)</li></ul>
<b>Problemas</b>	<ul style="list-style-type: none"><li>- Não evita todos os problemas decorrentes da captura de senhas trocadas entre eles</li><li>- Tipicamente não permite autenticação mútua</li><li>- As entidades precisam de saber que senhas devem usar em diferentes ocasiões. Implica uma forma de sincronização.</li><li>- As pessoas podem precisar de recursos extras para manter ou gerir senhas descartáveis.</li></ul>

### RSA SecurID

O RSA SecurID é um sistema de autenticação com senhas descartáveis que usa chaves secretas, partilhadas entre autenticador e autenticado. O autenticado guarda a chave num equipamento próprio, que a usa para produzir senhas descartáveis num ritmo fixo.



- Equipamento de autenticação pessoal
- Geram um número único a uma taxa fixa (normalmente de um em um minuto, associado a uma pessoa)
- Não realiza autenticação mútua
- Autenticação com senhas únicas
  - uma pessoa gera um OTP combinando o seu userID com o número apresentado no equipamento
  - um RSA ACE Server faz o mesmo, dado o userID e verifica a igualdade
  - robusto contra ataques de dicionários - pois as chaves não são escolhidas



## - Aproximação Desafio-Resposta

<b>Funcionamento</b>	<ul style="list-style-type: none"><li>- O autenticador fornece um desafio</li><li>- A entidade a ser autenticada transforma o desafio usando as suas credenciais de autenticação</li><li>- O resultado é enviado para o autenticador</li><li>- O autenticador verifica o resultado, produzindo um resultado semelhante e verifica a igualdade</li></ul>
<b>Vantagens</b>	<ul style="list-style-type: none"><li>- As credenciais de autenticação não são expostas</li></ul>
<b>Problemas</b>	<ul style="list-style-type: none"><li>- Ataques com dicionários autónomos usando pares desafio-resposta.</li></ul>

### **- Aproximação Desafio-Resposta com Smartcards**

<b>Credenciais de Autenticação</b>	<ul style="list-style-type: none"> <li>- Smartcard</li> <li>- A chave privada nele guardada e o pin de acesso à chave privada</li> </ul>
<b>O autenticador sabe</b>	<ul style="list-style-type: none"> <li>- A chave pública correspondente</li> </ul>
<b>Protocolo</b>	<ul style="list-style-type: none"> <li>- O autenticador gera um desafio aleatório</li> <li>- O dono do smartcard cifra o desafio com a sua chave privada</li> <li>- O autenticador decifra o resultado com a chave pública, se o resultado for igual ao desafio, a autenticação teve sucesso.</li> </ul>

### **- Aproximação Desafio-Resposta com Senha Memorizada**

<b>Credenciais de Autenticação</b>	<ul style="list-style-type: none"> <li>- Senha selecionada pelo utente</li> </ul>
<b>O autenticador sabe</b>	<ul style="list-style-type: none"> <li>- Uma transformação da senha</li> </ul>
<b>Protocolo</b>	<ul style="list-style-type: none"> <li>- O autenticador gera um desafio aleatório</li> <li>- O utente calcula uma transformação do desafio e da senha</li> <li style="text-align: center;">resposta = síntese (desafio, senha)</li> <li>- O autenticador faz o mesmo ou o inverso, se os resultados forem iguais, a autenticação teve sucesso</li> </ul>

#### Caso de Estudo: S/Key

- Credenciais de autenticação: senha
- O autenticador sabe:
  - A última chave única (OTP)
  - O índice da última OTP usada
  - Uma semente (ou raíz) de todas as
- Preparação do autenticador:
  - O autenticador define uma semente aleatória
  - A pessoa gera a OTP inicial
  - O autenticador guarda a semente, o  $n$ (o índice) e  $OTP_n$  como elementos de validação da autenticidade.
- Não pode ser adaptado para usar pares de chaves assimétricos com credências
- A sua principal vulnerabilidade está no facto de não facultar autenticação mútua, uma vez que o autenticador não consegue ser autenticado. Assim, um utente pode ser iludido e iniciar processos de autenticação com autenticadores falsos, facultando-lhes senhas descartáveis que poderão usar para personificar a vítima.

### Caso de Estudo: PAP, CHAP e MS-CHAP

- Protocolos usados com PPP (Point-to-Point Protocol)
  - Autenticação unidirecional: Apenas o cliente se autentica, o autenticador não se autentica
- PAP (PPP Authentication Protocol)
  - Apresentação simples de um par UID/Senha
  - Transmissão (insegura) da senha em claro
- CHAP (Challenge - response Authentication Protocol) - Protocolo Desafio-Resposta
  - O autenticador pode requerer a autenticação em qualquer instante
  - versão 2: autenticação bidirecional (autenticação mútua)
- MS-CHAP (Microsoft CHAP)
  - Autenticação mútua
  - As senhas podem ser alteradas

### **- Aproximação Desafio-Resposta com chave partilhada**

Uma solução para problemas com ataques consiste na substituição de uma senha memorizável por uma chave secreta, guardada de uma qualquer forma mas não memorizada. O facto de não ter de ser memorizável tem como vantagem o facto de não precisar de ser escolhida pelos utentes, podendo ser gerada aleatoriamente.

Assim, usa uma chave assimétrica criptográfica partilhada em vez de uma senha o que torna mais robusto contra ataques de dicionário e requer um dispositivo para guardar a chave.

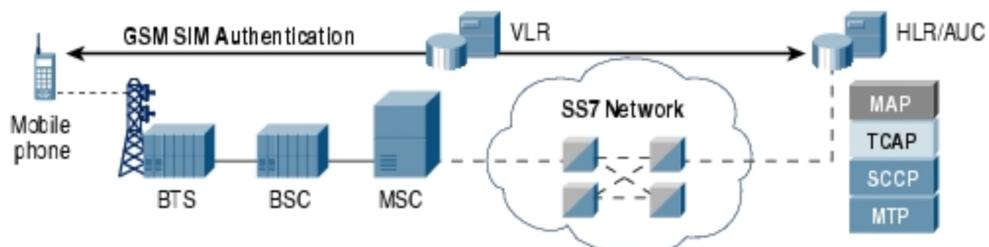
- Não implica que os autenticadores protejam as credenciais de autenticação dos seus clientes.

### Caso de Estudo: GSM

Nas redes “celulares” GSM, cada cliente, designado por um subscritor, possui um smartcard com um módulo SIM (Subscriber Identification Module). Um módulo SIM é uma componente da arquitetura de autenticação do GSM que é responsável pelo armazenamento, proteção e exploração de uma chave secreta de autenticação do subscritor titular. Na prática os módulos SIM são concretizados por smartcards de reduzida dimensão que são colocados no interior dos telefones.

O processo de autenticação consiste num protocolo desafio-resposta com chave secreta partilhada.

- É imune a ataques com dicionário



### **Autenticação de máquinas**

A autenticação de máquinas pode ser efetuada por nome ou endereço ou com chaves criptográficas.

Por nome ou endereço: nome DNS, endereço IP, endereço MAC, entre outros.

É extremamente fraco pois não existe prova criptográfica.

Com chaves criptográficas: as chaves secretas são partilhadas com interlocutores usuais. Pares de chaves assimétricas por máquina, onde chaves públicas são pré-partilhadas com interlocutores e chaves públicas certificadas por terceiros.

## **Autenticação de Serviços / Servidores**

A autenticação da máquina hospedeira diz que: todos os serviços co-localizados são automaticamente e indiretamente autenticados. Existem credenciais próprias do serviço.

A autenticação é feita por chaves secretas partilhadas com clientes quando evolvem a autenticação dos clientes com as mesmas e com pares de chaves assimétricas por máquina/serviço, certificadas por terceiros ou não.

### Caso de Estudo: SSL / TLS

- Protocolo de comunicação segura sobre TCP/IP
- Mecanismos de Segurança
  - Confidencialidade e integridade da comunicação
  - Autenticação de interlocutores
- Serve para garantir a negociação de uma chave de sessão entre os interlocutores
- Permite opcionalmente autenticar o cliente
- A autenticação do cliente implica uma autenticação mútua, mas o inverso não
- Permite que o servidor use chaves públicas não certificadas
- O cliente pode escolher livremente quais credenciais que usa na autenticação

### Caso de Estudo: SSH

O SSH permite duas formas de autenticar os clientes: usando senhas partilhadas e usando pares de chaves assimétricas.

A primeira consiste numa exploração direta de métodos de autenticação nativos do sistema operativo do autenticador, baseados em processos elementares de apresentação direta da senha pelo cliente. No caso SSH, esta apresentação da senha não tem riscos de segurança porque a senha circula entre cliente e servidor dentro do canal de comunicação seguro e criado previamente pelo SSH.

A segunda, usando o par de chaves assimétricas para autenticar o cliente, o mesmo apenas precisa, no máximo, de saber uma senha: a que protege a sua chave privada. Se essa senha for comprometida é apenas necessário troca-la num único local: no sistema onde a chave privada está guardada. A aplicação cliente SSH, onde quer que seja usada por esse cliente, terá de ser configurada para usar a sua chave privada a partir do local onde a mesma está guardada.

Estes pares de chaves assimétricos podem ser gerados por aplicações próprias apenas para serem usados pelo SSH, mas é igualmente possível usar outros pares de chaves assimétricas geradas para outros fins.

A aplicação cliente baseada e adaptada para trabalhar com smartcards através da interface PKCS#11 do Cartão de Cidadão na qual se indicam quais as credenciais a usar para autenticação do utente (nomeadamente, um cartão com o rótulo “CARTAO DE CIDADAO” e umas credenciais assimétricas, cujo certificado de chave pública possui o rótulo “CITIZEN AUTHENTICATION CERTIFICATE”).

- É vulnerável a ataques de interposição (*man in the middle*)
- Permite que os utentes se autentiquem de forma flexível
- Protege a autenticação dos clientes realizando-a no âmbito de uma comunicação segura
- Pode criar problemas de decisão aos clientes quando se mudam as credenciais dos servidores

- Gere consolas seguras sobre TCP/IP
- Inicialmente concebido para substituir o telnet
- Atualmente usada para outras aplicações: criação de túneis seguros e FTP
- Mecanismos de segurança
  - Confidencialidade e integridade da comunicação: Distribuição de chaves
  - Autenticação de interlocutores
    - Servidores / Máquinas
- Arquitetura SOHO

# Capítulo 7

## Segurança em Redes IEEE 802.11

As redes sem fios, em particular as redes 802.11, são também conhecidas como redes WLAN (*Wireless Local Area Network*) ou redes Wi-Fi.

Os problemas de segurança colocados pelas redes sem fios são:

- A autenticação entre um equipamento móvel (STA - *station*) e as redes sem fios a que acede
- O controlo de acesso de um STA a uma rede sem fios
- A confidencialidade das mensagens trocadas via rádio
- A autenticidade, ou controlo de integridade, das mensagens recebidas

### Redes Cabladas e Wireless

- **Elementos de prova**

- Difícil aplicar limites físicos de propagação
- Características físicas vulneráveis onde existe interferência nas comunicações e observação das comunicações

- **Mitigação**

Mecanismos para reduzir interferências e observação	
Nível Físico	Nível de Dados
<ul style="list-style-type: none"><li>- Impossibilitar os atacantes de descodificar o canal onde a codificação necessita de usar um segredo partilhado e as condições de transmissão dependem deste segredo.</li><li>- Prevenir transmissores de monopolizarem o canal (políticas de acesso ao meio físico)</li></ul>	<ul style="list-style-type: none"><li>- Prevenir que os atacantes identifiquem participantes da comunicação, é cifrado os cabeçalhos e criação de identificadores temporários</li><li>- Prevenir que atacantes compreendam os dados transmitidos, os pacotes são cifrados</li><li>- Prevenir que atacantes criem pacotes de dados válidos, os pacotes têm de ser autenticados (autenticação da origem ou do grupo)</li></ul>

### Arquitetura

- **STA (Station)** - Dispositivo que se liga a uma rede sem fios. Possui um identificador único, como o endereço MAC.
- **Access Point (AP)** - Dispositivo que serve de ponto de coordenação para os dispositivos de uma rede.
- **Redes sem Fios (Wireless)** - Rede formada por um conjunto de STAs e APs que comunicam com sinais de rádio.

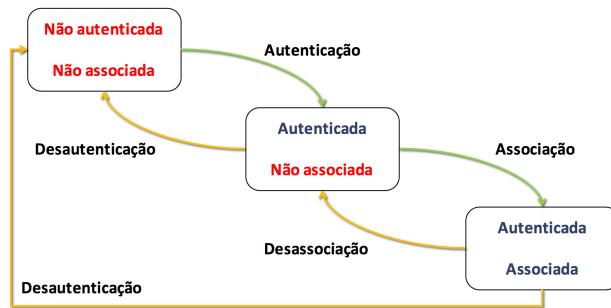
O padrão 802.11 permite duas arquiteturas de redes alternativas:

- **ad-hoc** - nesta arquitetura cada STA pode comunicar com outros, segundo um modelo P2P. O conjunto de equipamentos que constitui cada rede ad-hoc forma uma BSS.
- **estruturado** - nesta arquitetura os STA comunicam com os AP, apenas possuindo portas para comunicar com redes cabladas e antenas para comunicar com os STA.

## Terminologia de uma Rede

- **Basic Service Set (BSS)** - Rede formada por STA associadas a um AP.
- **Extended Service Set (ESS)** - Rede formada por várias BSS ligadas por um sistema de distribuição.
- **Service Set ID (SSID)** - Identificador de uma rede servida num BSS ou ESS. A mesma infraestrutura pode usar vários SSID.

## Máquina de Estados de Autenticação e Associação



<b>Autenticação</b>	<ul style="list-style-type: none"> <li>- A autenticação é feita recorrendo a múltiplas trocas de pacotes <i>Authentication Request / Authentication Response</i>.</li> <li>- No processo de autenticação, o AP pode pedir ao STA que prove pertencer a um determinado utente.</li> </ul>
<b>Associação</b>	<ul style="list-style-type: none"> <li>- A etapa de associação, associa o STA a um AP, o que na prática significa que o AP reserva recursos para identificar o STA e para gerir a comunicação com o mesmo.</li> <li>- A associação normalmente é realizada com a troca de pacotes <i>Association Request</i> e <i>Association Response</i>.</li> </ul>
<b>Desautenticação</b>	<ul style="list-style-type: none"> <li>- A desautenticação entre um STA e um AP pode ser comunicada por qualquer um dos interlocutores através de um pacote <i>Deauthentication</i>. A desautenticação permite que sejam libertados recursos (chaves criptográficas partilhadas).</li> <li>- A desautenticação implica uma desassociação automática.</li> </ul>
<b>Desassociação</b>	<ul style="list-style-type: none"> <li>- A desassociação entre o STA e o AP pode ser comunicado por qualquer um dos dois interlocutores através de um pacote <i>Desassociation</i>.</li> </ul>

## Tipos de Pacotes

- **Pacotes de Dados** - Os pacotes de dados servem para efetuar uma troca de dados útil, nomeadamente datagramas IP, entre o STA e AP.
- **Pacotes de Gestão** - Os pacotes de gestão permitem que um STA e um AP negoçiem e mantenham uma ligação entre si.
  - Authentication Request & Response;
  - Deauthentication;
  - Association Request & Response;
  - Reassociation Request & Response;
  - Disassociation
- **Pacotes de Controlo** - Os pacotes de controlo servem para gerir a comunicação entre o STA e o AP. Estes pacotes são usados para gerir o acesso ao meio de comunicação e para evitar a ocorrência de colisões provocadas por comunicações simultâneas.
  - Request to Send
  - Clear to Send
  - Acknowledgment

## Segurança do Nível dos Dados

Os problemas de segurança das redes WLAN, derivam do facto de ser complexo ou mesmo impossível limitar fisicamente o acesso de pessoas não autorizadas ao sinal de rádio usando nas redes WLAN ou aos AP que as suportam.

- Inicialmente, a segurança das redes estruturadas 802.11 era baseada no protocolo WEP. Este protocolo permite a autenticação unidirecional dos STA e a confidencialidade e o controlo de integridade dos dados trocados entre STA e os AP.
- O WPA tem a vantagem de permitir reutilizar os equipamentos de rede dos STA que suportam apenas WEP mas exige que os AP saibam operar com WPA. O WPA permite configurações de segurança mais simples, particularmente para ambientes SOHO.

Funcionalidade	Tipo de Rede	RSN (Robust Security Network)		
		WEP	WPA	802.11i (ou WPA2)
Autenticação		Unilateral (STA)	Bilateral com 802.1X (STA, AP e rede)	
Distribuição de Chaves			EAP ou PSK, 4-Way Handshake	
Política de Gestão de IV			TKIP	AES-CCMP
Cifra dos dados		RC4		AES-CTR
Controlo de Integridade	Cabeçalhos		Michael	AES CBC-MAC
	Dados	CRC-32	CRC-32, Michael	

## WEP

O WEP inclui duas funcionalidades distintas:

- autenticação do STA
- confidencialidade e controlo de integridade dos dados trocados

O WEP não permite distinguir utentes que acedem à rede.

### • Autenticação

OSA	SKA
<ul style="list-style-type: none"><li>- Não existe qualquer autenticação dos STA, logo a sua associação ao AP é sempre autorizada. Apenas ocorre o processo de associação e autenticação (do AP).</li><li>- Este modelo de autenticação é útil em alguns cenários específicos, por exemplo, caso se pretenda fornecer um acesso totalmente público e livre a determinada rede.</li></ul>	<ul style="list-style-type: none"><li>- A autenticação é feita usando um processo simples de desafio-resposta, o AP envia um desafio ao STA e este deverá devolver o cifrado com a chave partilhada de autenticação.</li><li>- A autenticação com SKA pressupõe uma pré-distribuição de chaves PSK ao STA e AP.</li></ul>

- SKA é completamente inseguro pois um atacante possui toda a informação para se fazer passar por uma vítima e não é necessário saber a chave, e os APs falsos não podem ser detetados.
- A mesma chave é usada para autenticação e confidencialidade, sem distribuição de chaves.
- Um dos problemas do WEP é a inexistência de políticas e mecanismos de geração de novas chaves WEP de cada vez que um dado utente se associa a um AP. A chave WEP é sempre a mesma - a pré distribuição entre o utente e o STA e os gestores do AP. Como o VI tem uma dimensão finita, tal significa que ao fim de algum tempo (ou tráfego) vão-se repetir as chaves contínuas geradas para cada utilizador.

### • Confidencialidade e Controlo de Integridade

Para cada pacote é escolhido um vetor de iniciação (VI) que juntamente com a chave WEP, são usadas como chave do algoritmo RC4 para gerar uma chave contínua. Esta chave contínua é somada aos dados a enviar via rádio e à sua soma de controlo calculada com CRC-32, transformando-os num criptograma. A decifra do criptograma segue o processo inverso: o receptor retira o VI da mensagem que recebeu, usa-o juntamente com a chave WEP para gerar a chave contínua e soma-a ao criptograma recebido, de onde resultam os dados em claro inicialmente apresentados na cípia.

## WPA

O WPA manteve toda a funcionalidade do WEP, tipicamente fornecida pelas interfaces de rede, e acrescentando-lhe funcionalidades ao nível de gestão de chaves de cifra e ao nível do controlo de integridade dos pacotes.

Com o WPA, cada pacote é cifrado com uma chave WEP diferente de forma a que não seja possível construir dicionários de chaves contínuas até mesmo quando se usa a mesma PSK repetidas vezes.

- A autenticação do WPA no acesso a um terminal móvel à rede permite o modelo *Enterprise* para redes de médio/grande dimensão.
- Permite a autenticação mas não a obriga

## IEEE 802.11i ou WPA2

O 802.11i, também designado por WPA2, é um padrão complexo que define um modelo de segurança para redes 802.11.

O 802.11i usa o conceito de redes de segurança robusta, RSN (*Robust Security Network*). Uma rede diz-se RSN se suportar uma autenticação mais eficaz dos interlocutores, baseada em 802.1X.

São usados mecanismos mais avançados para proteção das tramas, ou seja, métodos que não implicam suporte do hardware existente, como AES-CCMP, AES-CTR, CBC-MAC.

### AES-CCMP

O AES-CCMP é a combinação-base de mecanismos de segurança do 802.11i para proteger trama 802.11. Esta combinação tem por base o algoritmo criptográfico AES com chaves e blocos de dados 128 bits. Para controlo de integridade, o AES-CCMP usa o modo de operação CCM (Counter with CBC-MAC). Este é um modo de operação concebido para fornecer simultaneamente autenticação e controlo de integridade usando cifra por blocos de 128 bits.

A cifra do CCM é uma cifra contínua com base numa cifra por blocos operando em modo CTR. O controlo de integridade do CCM é realizado com CBC-MAC.

O modelo de operação AES-CCMP é muito semelhante ao do TKIP, mas usando apenas uma chave de sessão para cifra e controlo de integridade TK (*temporal key*).

## O WPA assenta em dois pilares

TKIP	802.1x
<ul style="list-style-type: none"><li>- Lida com a autenticação e confidencialidade das tramas.</li><li>- O TKIP encapsula o WEP, usa-o mas de forma a não expor as vulnerabilidades.</li><li>- O TKIP corrige a deficiencia de chaves e do VI do WEP</li><li>- O TKIP usa três chaves partilhadas com o interlocutor<ul style="list-style-type: none"><li>- <u>uma chave para confidencialidade</u>, TK de 128 bits</li><li>- <u>duas outras para controlo de integridade</u> (chaves MIC de 64 bits), uma para cada sentido da comunicação.</li></ul></li></ul>	<ul style="list-style-type: none"><li>- Lida com a autenticação entre interlocutores e distribuição de chaves de sessão após uma operação.</li><li>- Este protocolo serve para efetuar a autenticação mútua entre interlocutores, STA e rede, aquando da ligação de um STA a uma rede sem fios. <u>Este protocolo permite criar e distribuir chaves de sessão frescas aos equipamentos que efetuam a troca efetiva de mensagens via rádio, STA e AP.</u></li></ul> <p><b>Três tipo de interlocutores:</b></p> <ul style="list-style-type: none"><li>• <b>Suplicante</b> - equipamento (móvel) que se pretende ligar à rede</li><li>• <b>Autenticador</b> - elemento que controla o estado do porto de acesso do suplicante à rede</li><li>• <b>Servidor de autenticação</b> - servidor central gerido no âmbito do domínio de segurança da rede, que efetivamente conduz o processo de autenticação mútua entre os suplicantes e a rede</li></ul>

Um porto pode ser controlado ou não controlado. Um porto não controlado não impõe qualquer restrição à troca de dados através de si. Um porto controlado possui estados distintos e permite efetuar controlo de trocas de dados em cada estado

- “não autorizado” não permite a troca de dados, enquanto no estado “autorizado” permite.

## **Etapas do 802.1x**

As operações realizadas no âmbito 802.1x em redes sem fios dividem-se em três etapas. Após a terceira etapa pode ter lugar a troca de dados segura entre o STA e a rede a que o AP está ligado. Os dados serão protegidos usando o material criptográfico e os algoritmos negociados entre o AP, servidor de autenticação e o STA.

### **• Primeira Etapa: Descoberta e Associação 802.11**

- O suplicante (STA) liga-se à rede sem fios. É efetuado o processo normal das redes 802.11 da descoberta da rede, autenticação do STA e de associação entre o STA e o AP.
- No final desta etapa o suplicante deverá estar autenticado e associado junto de um AP que irá supervisionar ou controlar as etapas seguintes. No final desta etapa o porto controlado está no estado “não autorizado”.

### **• Segunda Etapa: Autenticação EAP**

- É realizada a autenticação mútua e uma distribuição de chaves de sessão entre o suplicante (STA) e o servidor de autenticação (SA). O autenticador supervisiona um diálogo entre o suplicante e o servidor de autenticação, o qual é o único permitindo através do porto não controlado.
- A troca de mensagens relativa à autenticação segue o metaprotocolo EAP. No final desta etapa o porto controlado continua no estado “não autorizado”.

#### **• EAP (*Extensible Authentication Protocol*)**

- O EAP é um metaprotocolo concebido para encapsular outros protocolos de autenticação.
- No caso do 802.1x, o EAP é fundamental para libertar o AP (autenticador) da tarefa de gerir aspectos particulares do modelo de autenticação adotado. A autenticação é centralizada no servidor de autenticação e consegue-se alterar os paradigmas de autenticação da rede sem alterar o software dos AP.
- A autenticação deverá ser mútua, resistente a ataques por interposição (“*man in the middle*”) e resistente a ataques com dicionários.
- Têm de gerar e distribuir aos interlocutores uma chave secreta simétrica. Essa chave deverá ter pelo menos 64 octetos e na sua geração deverão ser usados pelo menos 128 bits aleatórios e secretos.
- Embora o EAP permita autenticações unilaterais, no caso do 802.1X normalmente usa-se com autenticação bilateral.

### **• Terceira Etapa: Acordo em 4 Passos**

- É realizada uma autenticação mútua e uma distribuição de chaves de sessão entre o suplicante (STA) e o autenticador (AP). A autenticação é fundamental para o suplicante garantir que está a interagir com um autenticador (AP) que pertence ao mesmo domínio de segurança do servidor de autenticação, e não a um impostor. A distribuição de chaves visa criar uma chave de sessão fresca entre o suplicante e o autenticador, que irá servir de base à proteção dos dados trocados entre ambos.
- No final desta etapa o porto controlado já está no estado “autorizado”.

## **Todos os problemas estão resolvidos?**

Não ...

- O PSK e alguns métodos EAP vulneráveis a ataques por dicionário, continuarão a existir enquanto as passwords forem escolhidas pelos utilizadores
- Proteção apenas abrange tramas de dados:
  - Tramas de gestão
  - Atacantes podem desautenticar / desassociar STAs
  - Atacantes podem adivinhar o tipo de tráfego pelos tempos / tamanhos
  - Muitos protocolos expõem identidade do utilizador

# Capítulo 8

## Firewalls

Uma *firewall* tem dois objetivos fundamentais:

- 1) Proteção por isolamento de máquinas ligadas à rede
- 2) Controlo de interações entre máquinas

Em ambos os casos as decisões tomadas por uma firewall são controladas por um conjunto de regras e aplicação que as interpretam e reagem em função do tráfego que chega à firewall.

A proteção por isolamento de uma máquina ligada à rede é atualmente um requisito crítico, tanto para máquinas pessoais como organizacionais.

É uma vantagem, porque lhe permite usar serviços contactando outras máquinas ligadas direta ou indiretamente a essa rede. É também uma vantagem, porque lhe permite disponibilizar serviços a essas mesmas máquinas.

Mas é um risco, pois expõe vulnerabilidades da máquina que podem ser exploradas por atacantes.

É também um risco para outras máquinas, visto que a máquina pode ser usada para lançar ataques, o que pode acontecer independentemente da vontade dos seus utentes (por exemplo, após o comprometimento da mesma por uma ciberpraga).

Permite...	Funcionalidades
<ul style="list-style-type: none"><li>- Minimizar o impacto de vulnerabilidades locais</li><li>- Facilitar a tomada de posições mais drásticas</li><li>- Centralizar a deteção de problemas e o seu tratamento</li></ul>	<ul style="list-style-type: none"><li>- Supervisão de toda comunicação in &lt;-&gt; out</li><li>- Controlo (uso dos recursos protegidos; uso da rede exterior pelas máquinas)</li><li>- Defesa (contra ataques externos ao perímetro protegido; contra ataques iniciados no interior lançados para o exterior)</li></ul>
Limitações	
<ul style="list-style-type: none"><li>- Não resolvem o problema dos atacantes dentro da rede interna</li><li>- Só são eficazes se controlarem totalmente as ligações ao exterior</li><li>- São difíceis de administrar em ambientes com interesses heterogéneos (universidades)</li></ul>	

Uma firewall é um elo de ligação entre os sistemas computacionais (conjunto de redes e máquinas) que se pretende proteger, designado por perímetro protegido e as redes a que esse perímetro está ligado através da firewall.

É um elemento indispensável na ligação de máquinas pessoais e redes privadas a redes alheias potencialmente perigosas, nomeadamente a Internet.

A firewall é construída por diversas componentes funcionais, quer de hardware – máquinas, redes e equipamentos de interligação como hubs, switches, gateways, routers, etc – quer de software – aplicações específicas para filtrar, controlar e modificar fluxos de comunicação. Ou seja, uma firewall não é uma máquina, mas sim uma infraestrutura, que isola um perímetro protegido de redes perigosas a que o mesmo se liga.



## Tipos de Firewalls

<b>Packet-Filters</b> Filtro de Datagramas	<ul style="list-style-type: none"> <li>- É um filtro que atua fundamentalmente ao nível da rede, nomeadamente ao nível da troca de datagramas IP. Estes filtros normalmente limitam-se a aceitar ou rejeitar a passagem de um datagrama pela firewall, no âmbito do seu encaminhamento através da mesma.</li> <li>- Rejeitam interacções não autorizadas segundo o conteúdo dos pacotes IP (endereços IP, através das opções de cabeçalho, dimensão dos datagramas)</li> <li>- Podem registar fluxos informação ou conteúdo do tráfego</li> <li>- É transparente para as aplicações responsáveis pelos fluxos que avalia</li> </ul>
<b>Application-Level Gateways</b> Filtro Aplicacional	<ul style="list-style-type: none"> <li>- As firewalls do tipo “filtro aplicacional” operam ao nível do protocolo aplicacional. A sua função é dividir a parte ou a totalidade das interações aplicacionais entre interlocutores remotos, localizados em redes inteligentes pela firewall, de forma a controlar a execução desse mesmo protocolo. Por isso, as firewalls deste tipo são normalmente concretizadas usando um conjunto de aplicações designadas como <i>proxies</i> que executam em máquinas firewall.</li> </ul> <p>Para cada protocolo aplicacional é preciso que exista um mediador próprio, ao contrário dos filtros de datagramas.</p> <ul style="list-style-type: none"> <li>- Controlam interações ao nível da aplicação</li> <li>- Existe normalmente uma firewall diferente por protocolo</li> <li>- Protocolo proxy (controlo de acessos por utilizador, análise e alterações de conteúdos)</li> <li>- Focam-se na troca de dados aplicacionais e trabalham com conteúdos enviados de um lado para o outro</li> <li>- Não é aplicado filtros aos pacotes, só filtros aos fluxos</li> </ul>
<b>Circuit Gateways</b> Filtro de Circuitos	<ul style="list-style-type: none"> <li>- As firewalls do tipo “filtro de circuitos” controlam o estabelecimento de circuitos de formas não acessíveis aos filtros de datagramas, mas sem interferir de forma alguma com o protocolo aplicacional.</li> <li>- Podem registar fluxos informação ou conteúdo do tráfego</li> <li>- Detém facilmente conteúdos perigosos em fluxos de dados aplicacionais específicos</li> <li>- Obriga a que existam múltiplas aplicações, uma para cada tipo de tráfego aplicacional</li> <li>- Exemplo: Redigir o estabelecimento de ligações TCP</li> <li>- Exemplo: Autorizar ou não o estabelecimento de um circuito virtual após autenticação do requerente</li> </ul>
<b>Stateful Packet Filter</b>	<ul style="list-style-type: none"> <li>- Realizam Stateful Packet Inspection que analisa pacotes completamente incluindo o seu contexto, determinando e caracterizando a aplicação em causa e aplicam regras de filtragem/limitação.</li> <li>- Essa filtragem é feita a partir dos pacotes de IP.</li> </ul>

## Bastião

Deve executar versões seguras de sistemas operativos com uma configuração segura tendo instalados apenas os serviços considerados essenciais como Proxy de Telnet, DNS, FTP, SMTP e autenticação.

Em geral é uma plataforma para *application-level gateways* mas quanto mais proxies houverem no bastião, menor será o seu desempenho. Os proxies podem ser executados em *appliances* específicas. O bastião apenas encaminha tráfego para as *appliances* apropriadas. Este executa os *application-level gateways* de forma segura, ou seja, independente do comprometimento de um não afeta os restantes e sem privilégios especiais em que o seu comprometimento não permite afetar a máquina.

Os servidores públicos não devem ser colocados num bastião, como por exemplo: DNS, SMTP, HTTP, FTP, SSH, RAS, etc. Devem executar em máquinas dentro de DMZs. Assim, o bastião apenas encaminha tráfego para a máquina apropriada dentro de uma DMZ.

- Estação bastião é uma máquina segura instalada num ponto crítico da rede, onde executa um sistema operacional estável e seguro e um conjunto mínimo, seguro e controlado de serviços. Pode ser plataforma para Firewalls gateways de aplicação ou a nível de circuito.
- Gateway exposto a ataques, ou seja, não protegido por um filtro (normalmente o OUT)

## Topologia Dual-Homed

Arquitetura	Vantagens
<p>Uma única máquina - gateway bastião</p>	<ul style="list-style-type: none"><li>- Simplicidade</li><li>- Economia de recursos</li></ul>
Problemas / Desvantagens	<ul style="list-style-type: none"><li>- O comprometimento da máquina desativa a firewall</li><li>- A carga de processamento da firewall está toda sobre uma única máquina</li><li>- Os serviços públicos estão dentro da rede protegida</li></ul>

## Serviços de Segurança

<b>Autorização</b>	<ul style="list-style-type: none"><li>- De fluxo de dados (Packet Filtering)</li><li>- De utentes (App-Level / Circuit-Level)</li></ul>
<b>Redirecionamento de Tráfego</b>	<ul style="list-style-type: none"><li>- Para máquinas dedicadas (mail, www, ftp)</li><li>- Proxying (explícito ou transporte)</li></ul>
<b>Processamento de Conteúdos</b>	<ul style="list-style-type: none"><li>- Alteração de conteúdos (alteração de protocolos de alto nível)</li><li>- Análise de conteúdos</li></ul>
<b>Comunicação Segurança</b>	<ul style="list-style-type: none"><li>- VPN (cifra e controlo de integridade de fluxos de dados sobre redes públicas (inseguras))</li><li>- Encapsulamento (IPsec Tunneling)</li></ul>
<b>Defesa contra Tentativas de DoS</b>	<ul style="list-style-type: none"><li>- Detecção de ataques</li><li>- Filtragem de datagramas perigosos</li></ul>

## Firewalls Pessoais

As firewalls pessoais não são mais do que firewalls que se destinam a proteger uma única máquina e fazem parte do sistema da mesma.

Uma firewall pessoal normalmente é um sistema de software que executa na mesma máquina que se quer proteger, ou seja, a firewall e o perímetro protegido são exatamente a mesma máquina.

As firewalls pessoais distinguem-se também das demais por permitirem controlar quais as aplicações locais capazes de efectuar determinadas interações com o exterior. Este controlo é importante para detetar acessos ilegítimos à rede exterior.

- Permite controlar aspectos interessantes que são impossíveis para as demais em que as aplicações estão ou não autorizadas a efetuar determinada comunicação.
- Permite minimizar o comprometido de máquinas alheias no mesmo perímetro de segurança.
- Tem a capacidade de controlar o tráfego de aplicações concretas.
- É uma firewall que atual tipicamente como Filtro Aplicacional (Application Gateway) e Filtro de Pacotes (Packet Filter)
- São arquitecturalmente mais simples. Não existe filtro interior nem DMZ, o perímetro protegido confunde-se com o gateway e o filtro exterior a existir, é providenciado por quem fornece a ligação à rede.

### • Problemas

Nem todos os utentes são especialistas em segurança em redes, pois não sabem nada de protocolos de comunicação e não sabem também como devem forçar um nível de privilégio mínimo. A variedade de interações remotas leva a um grande número de regras onde existem ambientes de trabalho distintos, onde existem diferentes requisitos de segurança, tratamento uniforme / diferenciado de múltiplas interfaces de rede e onde a confusão e as incoerências são vulnerabilidades difíceis de detetar.

## Componentes

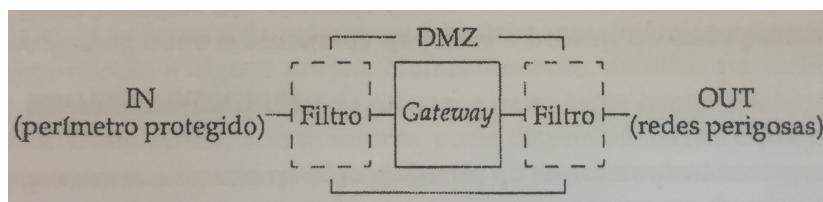
Uma firewall é formada por um gateway, dois filtros e uma rede de interligação de todas estas componentes, denominada por DMZ - zona desmilitarizada.

- A gateway é constituída por uma ou mais máquinas cuja função é controlar e encaminhar corretamente a comunicação IN-OUT, ou seja, entre o perímetro protegido e as redes perigosas exteriores.
- Os filtros destinam-se a fazer alguma filtragem do tráfego autorizado a passar através da firewall e, mais importante, impedir que o gateway possa ser contactado diretamente por outras máquinas, tanto da zona IN como da OUT.

## DMZ - Zona Desmilitarizada

A DMZ é a rede inerente à firewall, ou seja, a rede que estabelece a ligação entre os filtros e a gateway. A DMZ, como o seu nome sugere, uma “zona de ninguém”, não pode ser considerada uma rede do perímetro protegido porque parte das suas componentes podem ser comprometidas; e não é uma rede exterior porque é controlada pela organização que se pretende defender com a firewall.

- Porção de rede onde se colocam máquinas que são expostas a tráfego perigoso do exterior
- Porção de rede onde não existem máquinas endereçáveis a partir do exterior



## Tradução de Endereços (NAT)

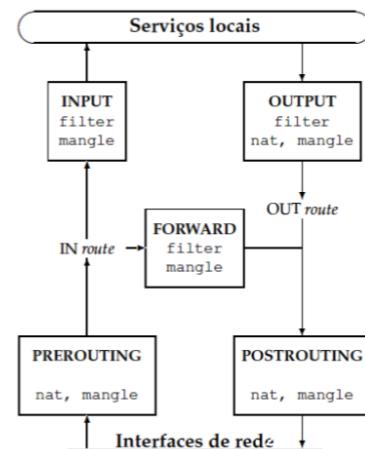
O NAT tem duplo objetivo: (i) simplificar a gestão de endereços das redes internas ligadas à Internet através da gateway; e (ii) impedir um endereçamento *ad hoc* de máquinas internas originado na rede externa.

## Caso de Estudo: iptables

- O *iptable* é um filtro de pacotes integrado com uma cadeira de processamento de pacotes IP dentro do sistema operativo Linux. Passível de estendido de várias maneiras: em módulos do sistema operativo e, aplicações em modo utilizador.
- As firewalls *iptables* aceitam, rejeitam ou alteram pacotes que fluem através de uma máquina - firewall do tipo Packet Filter.
- Servem para controlar o tráfego que entra e sai de uma máquina.
- O *iptable* usa um conceito de cadeias (chains) para analisar datagramas. Uma cadeia é uma sequência de regras e cada regra possui zero ou mais condições de aplicabilidade e uma decisão.

O *iptables* possui cinco cadeias padrão:

- INPUT - aplica-se a datagramas recebidos pela máquina e que lhe são dirigidos
- OUTPUT - aplica-se a datagramas enviados pela máquina e com origem na mesma
- FORWARD - aplica-se a datagramas recebidos pela máquina mas que não lhe são dirigidos, ou seja, que passam em transito pela máquina que faz o seu encaminhamento
- PREROUTING - aplica-se a todos os datagramas recebidos pela máquina
- POSTROUTING - aplica-se a todos os datagramas enviados pela máquina



O *iptables* usa tabelas para subdividir a aplicação de regras em cada cadeia para agrupar modelos de operação e dependem do modo como o *iptables* foi criado e instalado.

Existem três tabelas base:

- filter - existe sempre por omissão e serve para filtrar datagramas, ou seja, para decidir apenas sobre a sua aceitação ou rejeição
- nat - serve para detetar e atuar em situações em que seja necessário fazer NAT
- mangle - serve para efetuar diversos tipos de alterações nos datagramas

A decisão (target) expressa por cada regra é uma decisão-padrão ou o nome de outra cadeia, porque a decisão deverá ser tomada pelas regras dessa cadeia.

As decisões base são:

ACCEPT - indica que o datagrama deve ser aceite

DROP - datagrama deve ser descartado

QUEUE - o datagrama deve ser enviado para uma fila de espera destinada a uma aplicação local

RETURN - indica que a cadeia atual deve ser abandonada e retomada a análise de regras na regra seguinte da cadeia anterior)

Vantagens	Desvantagens
<ul style="list-style-type: none"><li>- O facto de ser um produto comparável em eficácia as demais firewalls comerciais,</li><li>- Ser apenas o núcleo de uma arquitetura mais complexa e extensível</li><li>- Ser relativamente estável, confiável e escalável</li><li>- Ser económico em termos de recursos computacionais necessários</li></ul>	<ul style="list-style-type: none"><li>- O facto de se ter de perceber bem como funciona a interação entre o núcleo LINUX, o <i>iptables</i> e diversos outros módulos que interagem com os dois anteriores.</li><li>- Não ser uma solução “chave na mão”</li><li>- Falta de ferramentas gráficas adequadas aos administradores menos habituados à administração de máquinas LINUX</li></ul>

# Capítulo 9

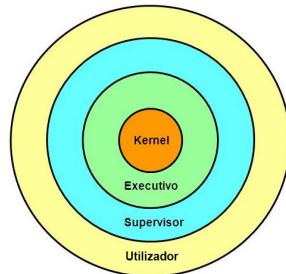
## Segurança em Sistemas Operativos

### Objetivos do Núcleo do SO

- Inicializar os dispositivos de hardware (*booting*)
- Visualizar o hardware, fornecendo uma interface para aplicações (Modelo Computacional)
- Aplicação das políticas de proteção e fornecimento de mecanismos de proteção, contra enganos involuntários e contra atividades não autorizadas
- Fornecer um sistema de ficheiros virtuais (VFS)

### Modos de Execução

- Diferentes níveis de privilégio, em que normalmente são ilustrados por um conjunto de anéis concêntricos. São usados em CPU's para evitarem que aplicações não privilegiadas executem instruções privilegiadas, como por exemplo: IN/OUT
- Os processadores atuais têm 4 anéis, mas os SO's normalmente só usam 2, em que o 0 corresponde ao modo supervisor e o 3 ao modo de utilizador.
- A transferência de controlo entre anéis requer mecanismos de passagem especiais, os quais são usados pelas *system calls*.



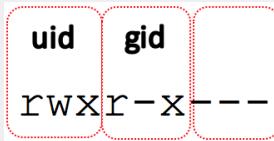
### Modelo Computacional

Conjunto de entidades (objetos) geridos pelo núcleo do SO

Identificadores de Utilizadores	Identificadores de Grupos
<ul style="list-style-type: none"><li>- Para um sistema operativo, um utilizador é um número, estabelecido durante a operação de login -&gt; userID (UID)</li><li>- As atividades executadas num computador fazem-se sempre associadas a um UID, permitindo assim estabelecer o que é permitido ou negado às atividades.</li><li>- Em Linux, o UID 0 é omnipotente (<i>root</i>)<ul style="list-style-type: none"><li>- A administração da máquina é feita recorrendo a atividades com UID 0</li></ul></li><li>- Em Windows, existe o conceito de privilégios de administração<ul style="list-style-type: none"><li>- Não existe um UID único e bem estabelecido para um administrador</li><li>- Privilégios de administração podem ser dados a diversos UIDs</li></ul></li></ul>	<ul style="list-style-type: none"><li>- Um grupo é um conjunto de utilizadores</li><li>- Um grupo (GID) pode ser definido à custa de outros grupos</li><li>- Um utilizador pode pertencer a vários grupos<ul style="list-style-type: none"><li>- Os privilégios são determinados através do conjunto de privilégios atribuídos a si e aos grupos a que pertence</li></ul><math display="block">\text{Direitos} = \text{Direitos UID} + \text{Direitos GID}</math></li><li>- Em Linux, as atividades executadas são sempre associadas a um conjunto de grupos<ul style="list-style-type: none"><li>- <b>Grupo Primário</b> - usado para definir proteções de novos ficheiros</li><li>- <b>Grupo Secundário</b> - usado juntamente com o anterior, para definir se tem ou não acesso a recursos</li></ul></li></ul>

<b>Processos</b>	<b>Memória Virtual</b>
<ul style="list-style-type: none"> <li>- Um processo contextualiza uma atividade para efeitos de decisões de segurança e para outros fins.</li> <li>- Contexto com relevância para a segurança <ul style="list-style-type: none"> <li>- Identidade (UID e GID) - fundamental para efeitos de controlo de acesso do processo</li> <li>- Recursos actualmente em uso - ficheiros abertos (incluindo canais de comunicação); áreas de memória virtual reservada; tempo de CPU usado</li> <li>- Um processo pode alterar livremente o seu <i>effective UID</i> para <i>real UID</i></li> </ul> </li> </ul>	<ul style="list-style-type: none"> <li>- É um espaço de memória onde têm lugar ações efetuadas por uma atividade</li> <li>- Tem uma dimensão máxima que é definida pela arquitetura do hardware <ul style="list-style-type: none"> <li>- 32 bits -&gt; <math>2^{32}</math> B (4GB) máximo</li> <li>- 64 bits -&gt; <math>2^{64}</math> B máximo</li> </ul> </li> <li>- A memória virtual não precisa e não pode ser usada na integra, apenas é usada uma paralela</li> <li>- A memória virtual é mapeada em memória física (RAM) quando é necessário nela ler ou escrever <ul style="list-style-type: none"> <li>- Num dado instante, a memória física possui partes de várias memórias virtuais</li> <li>- A escolha automática dessas partes é uma das funções mais importantes de um SO.</li> </ul> </li> </ul>
<b>Ficheiros</b>	<b>Sistemas de Ficheiros</b>
<ul style="list-style-type: none"> <li>- Servem para armazenar dados de forma duradoura, sendo a longevidade dada pelo suporte físico e não pelo conceito de ficheiro</li> <li>- São sequências ordenadas de bytes associadas a um nome</li> <li>- O seu conteúdo pode ser alterado, removido ou acrescentado</li> <li>- Possuem uma proteção que controla o seu uso <ul style="list-style-type: none"> <li>- Permissões de leitura, escrita, execução e remoção</li> <li>- O modelo de proteção depende do sistema de ficheiros</li> </ul> </li> <li>- O direito de alterar o dono de um ficheiro está vedado (excepto se for <i>root</i>)</li> <li>- Porém é possível alterar o seu set-UID</li> </ul>	<ul style="list-style-type: none"> <li>- Estruturas hierárquicas de arrumação de ficheiros</li> <li>- São formados por diretórios (nós) e ficheiros (folhas)</li> <li>- A diretoria no topo é a raiz do sistema de ficheiros</li> </ul>
<b>Canais de Comunicação</b>	<b>Proteção com ACLs</b>
<ul style="list-style-type: none"> <li>- Permite a troca de dados entre atividades distintas mas cooperantes <ul style="list-style-type: none"> <li>- Processos do mesmo SO/máquina (Socks UNIX, streams)</li> <li>- Processos em máquinas distintas (Sockets TCP/IP e UDP/IP)</li> </ul> </li> </ul>	<ul style="list-style-type: none"> <li>- Lista de controlo de acessos (ACL) <ul style="list-style-type: none"> <li>- cada “objeto” possui uma ACL (diz quem pode fazer o quê)</li> </ul> </li> <li>- A ACL pode ser: <ul style="list-style-type: none"> <li>- <b>discricionária</b> - quando pode ser alterado pelo dono do objeto</li> <li>- <b>obrigatória</b> - não se consegue alterar (é fixado pelo criador)</li> </ul> </li> <li>- É verificada quando uma atividade pretende manipular o “objeto” <ul style="list-style-type: none"> <li>- se o pedido de manipulação não estiver autorizado, é negado</li> <li>- quem faz as validações das ACL é o núcleo do SO (monitor de segurança)</li> </ul> </li> </ul>

## Proteção de Ficheiros em Linux

ACLs de dimensão e estrutura fixa	Entidades
<ul style="list-style-type: none"> <li>- Cada elemento do sistema de ficheiros possui uma ACL onde atribui 3 tipos de direitos a 3 entidades e onde apenas o dono do elemento pode mudar a ACL</li> <li>- Direitos: <ul style="list-style-type: none"> <li>- R (read) ; W (write) ; X (execute)</li> <li>- Para ficheiros normais significa direito de: leitura; escrita; execução</li> <li>- Para as diretórias significam direito de: listagem; adição/remoção de ficheiros ou subdiretórios; uso como diretória corrente do processo</li> </ul> </li> </ul>	<ul style="list-style-type: none"> <li>- Um UID (dono do ficheiro)</li> <li>- Um GID (grupo associado ao ficheiro)</li> <li>- Os Demais</li> </ul> 

## Elevação de Privilégios

- **Mecanismo Set-UID** - Esta funcionalidade serve para fazer uma distribuição do UID do processo que executa um determinado programa.
  - Se um programa possuir o UIDx e o bit set-UID ativa na sua ACL, então ele será executado num processo com UIDx independentemente do UID de quem o mandar executar
  - Na prática, esta funcionalidade serve para disponibilizar programas que realizam operações privilegiadas a utentes em que não se confia
  - Resumindo: O set-UID é um mecanismo de elevação de privilégios que serve para que se possa dar permissão a terceiros para executar curtas operações
- **Mecanismo SUDO** - A administração pelo *root* não é adequada
  - Aproximação preferível a vários utilizadores que podem ser administradores temporários (usam o UID 0, temporariamente) e o comando sudo
  - Sudo é uma aplicação set-UID com UID = 0

## Redução de Privilégios

- **Mecanismo Chroot** - Permite diminuir a visibilidade do sistema de ficheiros.
  - Menor visibilidade - menor risco de ver o que não interessa
  - Cada descritor do processo possui o *i-number* do *i-node* raiz, a partir da qual começa a resolução de nomes completos (nome/nome/nome/etc)
  - Chroot permite mudar esse número para referir o *i-node* de outra diretoria arbitrária
    - A vista do sistema de ficheiros de aplicações potencialmente perigosas
    - Servidores públicos, aplicações descarregadas
  - A manipulação da raiz do sistema de ficheiros por cada processo permite contextualizar políticas de privilégio mínimo

Real UID	Effective UID
Identifica o verdadeiro dono do processo e afeta as permissões para o envio de sinais. Um processo sem privilégio de super utilizador pode sinalizar outro processo apenas se UID real do remetente corresponde com o UID real do receptor. Como os processos filho herdam as credenciais do pai, eles podem sinalizar um ao outro.	Afeta a criação e o acesso de ficheiros. Durante a criação do ficheiro, o kernel define os atributos do proprietário do ficheiro para o UID efetivo e o GID efetivo do processo de criação. Durante o acesso ao ficheiro, o kernel usa o UID efetivo e o GID efetivo do processo para determinar se ele pode aceder o ficheiro.

# Capítulo 10

## Armazenamento da Informação

### Problemas

- Os discos avariam
  - E cada vez há mais informação digital vital
  - É preciso minimizar a falta de discos ou a perda de informação
- O acesso mecânico à informação é lento
  - $\text{tempo} = \text{tempo de translação} + \text{tempo de rotação}$

↓                            ↓  
relativo à agulha        relativo ao disco

- Mais informação -> maior estrangulamento
- São precisos discos mais eficientes
- Alternativas de solução
  - cópias de segurança (*backups*) - locais ou remotas
  - RAID

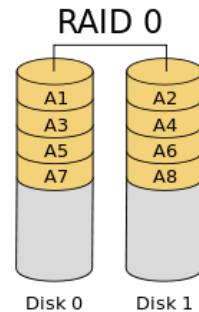
### Objetivos

- Garantir a sobrevivência da informação
  - Os dados só se perdem se falharem mais do que X discos do RAID, onde o valor de X depende do tipo de RAID
- Solução de baixo custo e eficiente
  - Permite usar hardware barato e fálgivel
  - Acelerar o desempenho nas leituras e escritas em discos
- O RAID não substitui o backup!
  - Não tolera falhas catastróficas em mais do que X discos em N
  - Não tolera erros dos utentes ou do sistema
- O RAID pode aumentar a probabilidade de falha do sistema!
  - Se o objetivo for apenas acelerar o mesmo

### RAID 0 (*striping*)

Se um disco falhar, falha tudo!

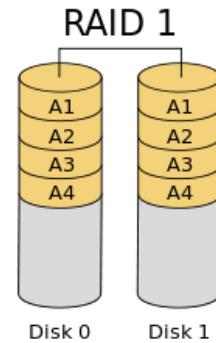
- Objetivo: Acelerar o acesso à informação em disco
- Aproximação: Acesso a discos em paralelo
  - Stripping:
    - A informação lógica de um volume é subdividido em fatias (*stripes*)
    - As fatias são intercaladas nos discos
  - Não há desperdício de informação (não aumenta em razão direta)
- Prós: Aceleração dos acessos aos discos até N vezes
  - Não é necessário percorrer o disco todo, basta aceder a partes dos N discos
- Contras: Maior probabilidade de perda de informação
  - Se  $P_F$  for a probabilidade de falha num disco, a probabilidade de perder informação com N discos é  $1 - (1 - P_F)^N$
  - Aumento do número de dispositivos, pelo menos para o dobro



## RAID 1 (*mirroring*)

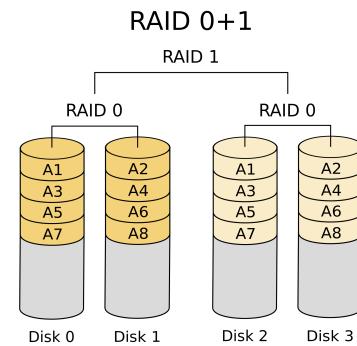
Se um disco falhar, os dados podem ser recuperados porque existem cópias

- Objetivo: Tolerar a falha de discos
- Aproximação: Acesso a discos em paralelo
  - Duplicação da informação (*mirroring*)
    - A mesma informação nos N discos, escrita sincronizada
    - Na leitura é feita uma verificação de coerência (igualdade)
    - O sistema RAID1 deve funcionar aos pares de forma a que haja um clone
    - Aumento do desperdício, tudo o que é colocado é redundância (aumenta na razão direta)
  - Prós: Diminuição da probabilidade de perda de informação
    - Se  $P_F$  for a probabilidade de falha de um disco, a probabilidade de perder informação com N discos é  $(P_F)^N$
  - Contra: Desperdício da capacidade de armazenamento, mais de 50% de capacidade total de armazenamento  $\left(\frac{N-1}{N}\right)$ 
    - Sistema que apresenta maior desperdício de espaço de armazenamento
    - Aumento do número de dispositivos, no mínimo para o dobro



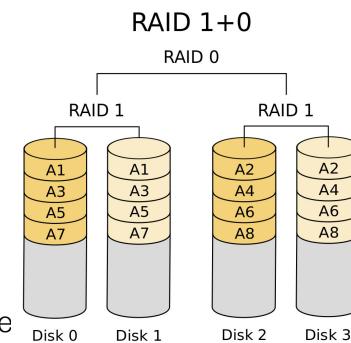
## RAID 0+1

- Objetivo: Benefícios do RAID 0 (desempenho)  
Benefícios do RAID 1 (tolerância a falhas)
- Aproximação: RAID 0 num primeiro nível  
RAID 1 num segundo nível
  - *Mirroring de volumes striped*
  - É um sistema híbrido!
    - Combina RAID 0 com RAID 1
    - O sistema precisa de ter pelo menos 4 unidades de armazenamento, duas para cada nível
    - RAID 0+1 considera o aspeto do desempenho e redundância
- Vantagens: Maior desempenho graças ao paralelismo  
Proteção contra perdas graças ao RAID 1
- Desvantagens: Desperdício de capacidade de armazenamento, mais de 50% da capacidade total de armazenamento  $\left(\frac{N-1}{N}\right)$ 
  - Aumento do número de dispositivos, no mínimo para o dobro



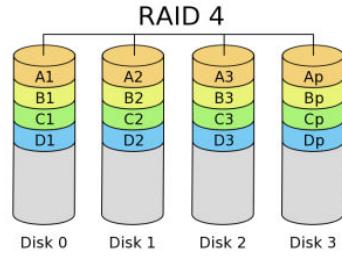
## RAID 1+0

- Objetivo: Semelhante ao 0+1  
Inverte *stripping* e *mirroring*
- Aproximação: RAID 1 num primeiro nível  
RAID 0 num segundo nível
  - *Stripping de volumes sobre volumes mirrored*
- Em caso de falha
  - RAID 0+1 - O sistema transforma-se em RAID 0
  - RAID 1+0 - O sistema assume o nível RAID 1
- Desvantagem: Ligeiramente pior fiabilidade prática, se perder-se todo um subsistema com RAID 1



## RAID 4

- Objetivo: Ter proteção do RAID 1, tendo um desempenho e um aproveitamento de espaço próximo do RAID 0
- Aproximação: Armazenamento de dados em N-1 discos
  - Há um disco reservado para a paridade
  - Desperdício de espaço é igual à capacidade de cada disco
  - Os dados de quaisquer N-1 discos geram um outro
- Problemas: Necessita de 3 ou mais discos
  - A atualização da paridade é complexa e demorada
  - A recuperação é mais demorada do que com o RAID 1
  - Se falhar dois ou mais discos, o sistema falha e perde informação  $1 - (1 - P_F)^N$
  - Se falhar um disco, o sistema perde informação e recupera-a  $1 - (1 - P_F)^N - N(P_F(1 - P_F)^{N-1})$



## RAID 5

- Objetivo: Semelhante ao RAID 4, mas mais eficiente nas escritas
- Aproximações: Blocos de paridade dispersos por todos os discos
  - O desperdício de espaço é igual ao do RAID 4 (igual à capacidade de cada disco)
  - A concorrência nas escritas é melhorada
  - Em vez de existir uma unidade de armazenamento inteira como réplica, os próprios discos servem de proteção
  - Os dados são divididos em pequenos blocos, cada um deles recebe um bit de paridade
  - As informações de paridade, assim como os próprios dados, são distribuídos entre todos os discos do sistema
  - O espaço destinado à paridade é equivalente ao tamanho de um dos discos
- Problemas: Mais complexo que o RAID 4
  - Necessita de 3 ou mais discos
  - Se falhar dois ou mais discos, o sistema falha e perde informação  $1 - (1 - P_F)^N$
  - Se falhar um disco, o sistema perde informação e recupera-a  $1 - (1 - P_F)^N - N(P_F(1 - P_F)^{N-1})$

