Universidade do Minho
Escola de Engenharia

Tecnologias Biométricas: aplicação no Controlo de Acesso a Sistemas de Informação

Lição de síntese

Prova de Agregação no ramo de conhecimento de Tecnologias e Sistemas de Informação
submetida à
Universidade do Minho
por
Henrique Manuel Dinis dos Santos

Enquadramento

Universidade do Minho
Escola de Engenharia

Sessão (semana)	Título	RAs	Conteúdos
0 (1)	Apresentação da UC Conceitos gerais de SegInfo	a)	1.1 Terminol
1 (2-3)	Conceitos gerais: modelo para a SegInfo (segundo a família de normas ISO/IEC 27000)	b), e) e h)	1.2 Ameaças, medidas de s 1.3 A gestão 1.4 Tipos e n 1.5 Taxonom
2 (4-5)	Utilização da criptografia em Segurança da Informação	c), d) e f)	2.1 Terminol 2.2 Cifra simétrica e assimétrica 2.3 Protocolos baseados em cifras
3 (6-7)	**Controlo de Acesso**	a), e) e f)	3.1 Fundamentos 3.2 Modelos e protocolos 3.3 Autenticação **3.4 Autenticação de utilizadores (ênfase nas tecnologias biométricas**
4 (8-9)	Segurança em redes TCP/IP: fundamentos e introdução à análise de tráfego	b), d) e g)	4.1 Modelo de comunicação nas redes TCP/IP 4.2 Protocolos de suporte 4.3 Ferramentas de análise de tráfego 4.4 Sinais de anomalias
5 (10-11)	Segurança em redes TCP/IP: ataques em redes	b), c), d) e g)	4.5 Anatomia de ataques em redes
6 (12-13)	Tecnologias de segurança em redes: protocolos	e) e f)	5.1 Considerações gerais (boas práticas de implementação) 5.2 Protocolos de segurança de redes (IPSec e SSL/TLS) 5.3 Redes Privadas Virtuais (VPN - Virtual Private Networking)
7 (14-15)	Tecnologias de segurança em redes: componentes	e) e f)	5.4 Firewalls 5.5 Sistemas de Detecção de Intrusões (IDS)

a) Reconhecer a importância de uma cultura de segurança …
e) Planear uma estratégia de segurança …
f) **Implementar e controlar tecnologias de segurança** …

Sumário

Universidade do Minho
Escola de Engenharia

1. Controlo de Acesso
2. Autenticação
3. Autenticação dos utilizadores
   - *Passwords* em maior detalhe
   - *Tokens* em maior detalhe
   - **Biometria em maior detalhe**
     - Introdução às biometrias
     - Características biológicas, propriedades e requisitos das biometrias
     - Exemplos de biometrias (estabelecidas e em investigação)
     - Taxonomia multidimensional
     - Sistemas biométricos
       - Arquitetura típica de um sistema biométrico
       - Modos de operação
       - Funções de similaridade
     - Precisão e avaliação
       - Tipos de avaliação
       - Instrumentos de avaliação do desempenho
     - Escalabilidade e segurança
     - Exemplos de aplicação

Controlo de Acesso

Universidade do Minho
Escola de Engenharia

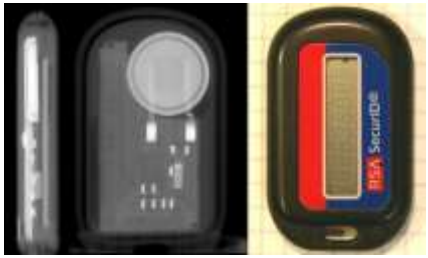
- Engloba serviços de: **Autenticação**, Autorização e Auditoria (AAA);
- Objetivo: controlar as condições de acesso de um ***subject*** a um ***object***, em particular o que pode fazer (autorização) – Read, Write, Execute…

Autenticação dos utilizadores

Universidade do Minho
Escola de Engenharia

- *Knowledge-based* (segredo)
  - Passwords

- *Object-based* (posse)
  - *Tokens*



- *ID-based* (caracteristica)
  - Biometria

Autenticação dos utilizadores

Universidade do Minho
Escola de Engenharia

Normalmente referida por:	***Password*; Segredo**	***Token;* Cartão**	**Biometria**
Autenticação baseada em:	Secretismo ou obscuridade	Posse	Individualização e personalização
Pressuposto da segurança:	Nunca é revelado	Nunca é extraviado	Impossível duplicar
Exemplo (digital):	Password de acesso ao computador	Cartão de acesso à garagem	Impressão digital
Limitações à segurança:	Menos seguro com a utilização; memorização	Inseguro se for perdido	Muito difícil substituir
Combinações (multifactor)	*Two-factor authentication*		
		Two-factor authentication	
	Two-factor		*authentication*
	Three-factor authentication		

Autenticação dos utilizadores

Universidade do Minho
Escola de Engenharia

- Níveis de aceitação dos utilizadores (estudo de Jones) (Jones 2007)
  - Palavra-chave é o mecanismo mais conhecido, seguido por algumas biometrias e, por fim, os *tokens*
  - Preferências:
    - Acesso a computadores – **palavra-chave**
    - Transacções financeiras – **palavra-chave e biometrias**
    - Saúde – **Biometrias**
    - Acesso físico – ***Tokens***
  - Percepção da segurança
    - Biometrias (íris; impressão digital; geometria da mão; reconhecimento de voz e face;…), seguido da palavra-chave; e, por fim, os *tokens*

Biometrias

Universidade do Minho
Escola de Engenharia

- Mais de um século passou desde que Alphonse Bertillon concebeu e "industrializou" uma ideia para identificar criminosos a partir de dados do corpo.
- Em 1893 o ministério dos assuntos internos do Reino Unido assume que nenhum par de indivíduos teria a mesma impressão digital.
- Em 1960 aparece o primeiro AFIS (*Automatic Fingerprint Identification System*).
- Nas últimas décadas muitas outras técnicas surgiram. Com a ajuda de Hollywood (CSI) criou-se a ideia que as Biometrias são um conjunto de técnicas robustas!
  - Em 2004, num concurso sobre AFIS, foi revelado que a melhor das técnicas gerava 2% de falsos negativos!

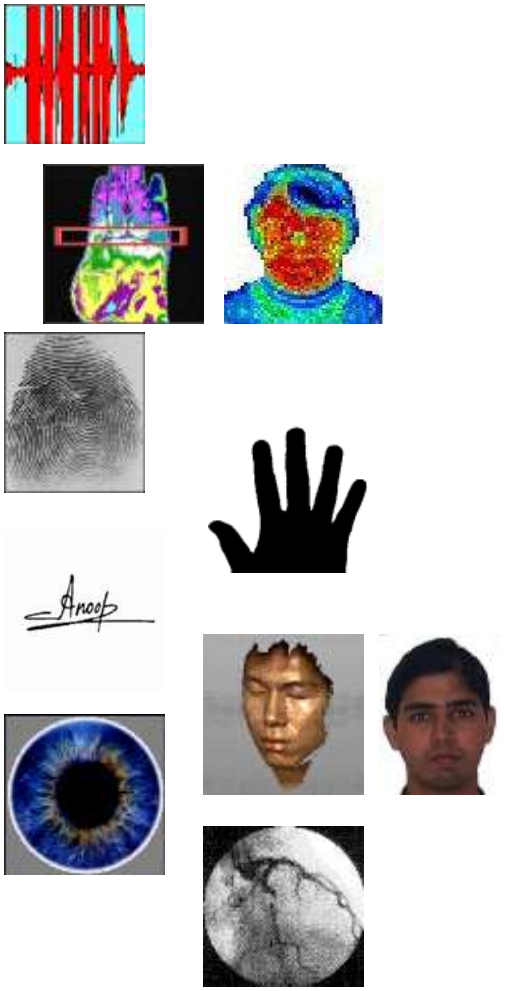
Biometrias

Universidade do Minho
Escola de Engenharia

- Que características biológicas podem ser usadas?
  - Propriedades fundamentais:
    - Universalidade
    - Unicidade (*Distinctiveness*)
    - Permanência (*Permanence*)
    - Mensurável (*Collectability*)
  - Outros requisitos
    - Desempenho (precisão, recursos, etc.)
    - Aceitação (*Acceptability*)
    - Resistência a ataques – (*Circumvention*)

Exemplos de Biometrias

- Estabelecidas
  - Voz
  - Termogramas infravermelhos: análise facial e padrão das veias da mão
  - Impressão digital
  - Geometria da mão
  - Assinatura
  - Face
  - Iris
  - Retina



Exemplos de Biometrias

- Em investigação
  - *Keystrokes dynamics*
  - Locomoção
  - Odor
  - Orelha
  - Eletrocardiograma
  - DNA
  - Multidimensionais

Exemplos de Biometrias

Universidade do Minho
Escola de Engenharia

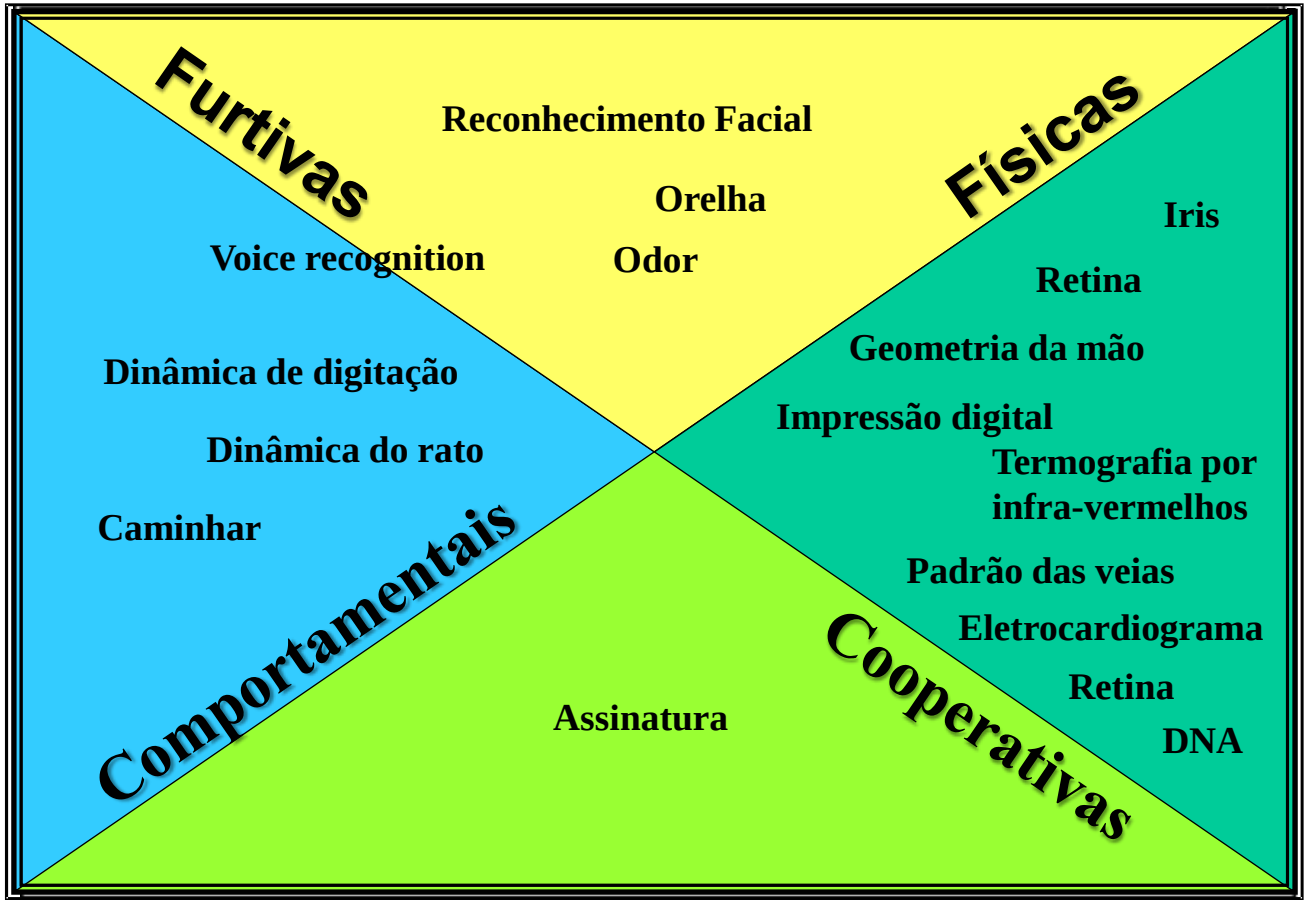
- Quais as melhores características?

Biometric characteristic	Universality	Distinctiveness	Permanence	Collectability	Performance	Acceptability	Circumvention
Facial thermogram	H	H	L	H	M	H	L
Hand vein	M	M	M	M	M	M	L
Gait	M	L	L	H	L	H	M
Keystroke	L	L	L	M	L	M	M
Odor	H	H	H	L	L	M	L
Ear	M	M	H	M	M	H	M
Hand geometry	M	M	M	H	M	M	M
Fingerprint	M	H	H	M	H	M	M
Face	H	L	M	H	L	H	H
Retina	H	H	M	L	H	L	L
Iris	H	H	H	M	H	L	L
Palmprint	M	H	H	M	H	M	M
Voice	M	L	L	M	L	H	H
Signature	L	L	L	H	L	H	H
DNA	H	H	H	L	H	L	L

(Delac, 2004)

Biometrias - taxinomia

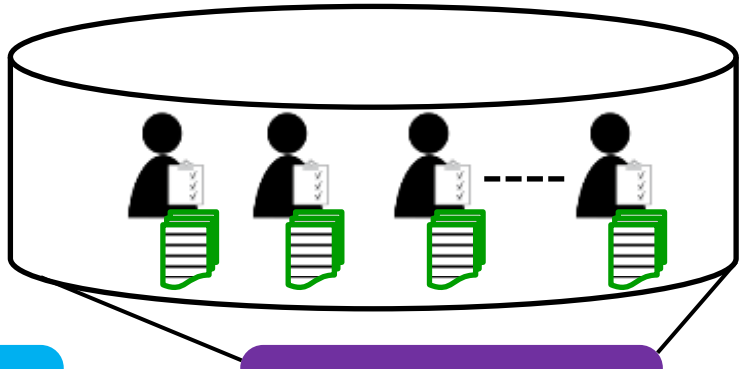
Universidade do Minho
Escola de Engenharia



Sistemas Biométricos

Universidade do Minho
Escola de Engenharia

- Modos de operação
  - *Enrollment*

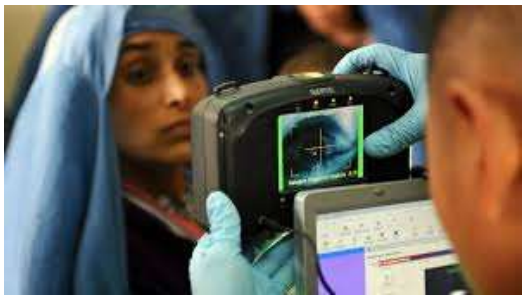


(Jain, Ross et al. 2004)

Sistemas Biométricos

Universidade do Minho
Escola de Engenharia

- Sensor
  - Recolha de dados em bruto, com eventual verificação de qualidade
  - Impressão digital, face e íris são os mais desenvolvidos
  - Algumas técnicas de processamento de sinal (filtragem) e de processamento de imagem (particularmente quando se trata de imagens ou vídeo)



Sistemas Biométricos

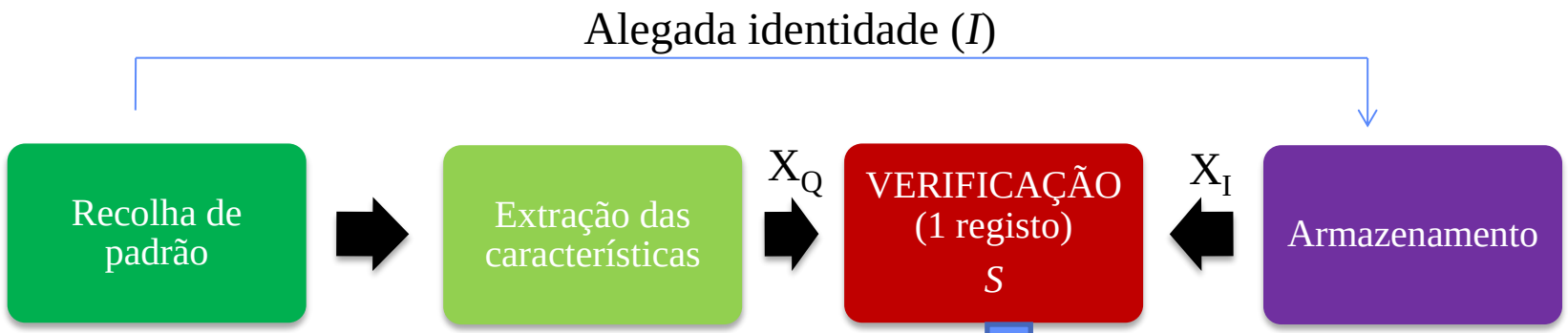
Universidade do Minho
Escola de Engenharia

- Extração de características
  - Problema de reconhecimento de padrões
  - Exemplos de técnicas usadas com algum sucesso
    - Análise em Componentes Principais – *Eigenfaces*
    - Filtros de Gabor
    - LDA – Análise Discriminante Linear
    - *Naive Bayes Classifier*
    - Rough Sets
    - Redes neuronais
    - *Support Vector Machines*
    - …
  - **Treino é crítico**

Sistemas Biométricos

Universidade do Minho
Escola de Engenharia

- Modos de operação
  - Verificação (tipicamente **reconhecimento** positivo)
    - O individuo é realmente quem ele diz ser? (e.g., autenticação perante um sistema)



$$(I, X_Q) \in \begin{cases} w_1 & if\ S(X_Q, X_I) \geq t, \\ w_2 & otherwise, \end{cases}$$

Sistemas Biométricos

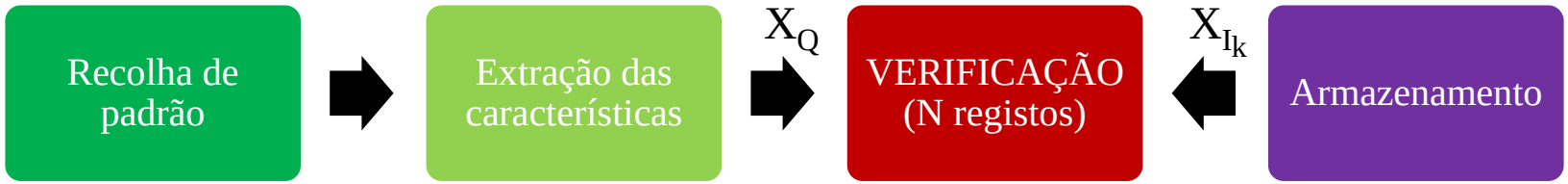
Universidade do Minho
Escola de Engenharia

- *S*: função de similaridade (produz um *matching score*), frequentemente:
  - Distância Euclidiana $S = \sqrt{\sum_{i=1}^{n}(X_{Qi} - X_{Ii})^2}$
  - Distância de Mahalanobis $S = \sqrt{(\overrightarrow{X_Q} - \overrightarrow{X_I})^T S^{-1}(\overrightarrow{X_Q} - \overrightarrow{X_I})}$
    onde S^{-1} é a matriz de covariância inversa, ou matriz de precisão
  - Distância de Hamming
- Efeito da variação (aleatória) de X_Q, ou mesmo de X_I.
- *t*: é um *threshold* pré-definido
- Em qualquer dos casos o modelo carece de estudos alargados sobre a população alvo

Sistemas Biométricos

Universidade do Minho
Escola de Engenharia

- Modos de operação
  - Identificação (tipicamente **reconhecimento** negativo) – apenas possível com tecnologias biométricas
    - A partir de um padrão biométrico, este indivíduo já se encontra registado?
  - Detecção (caso particular da identificação)
    - Este padrão biométrico pertence a um individuo incluído numa lista de "referenciados"? (e.g., segurança em aeroportos, ou passaporte eletrónico)



$$(X_Q) \in \begin{cases} I_K & if \ \max_K \{S(X_Q, X_{I_K})\} \geq t, K = 1,2,\dots,N, \\ I_{N+1} & otherwise, \end{cases}$$

Identificado/
Não identificado

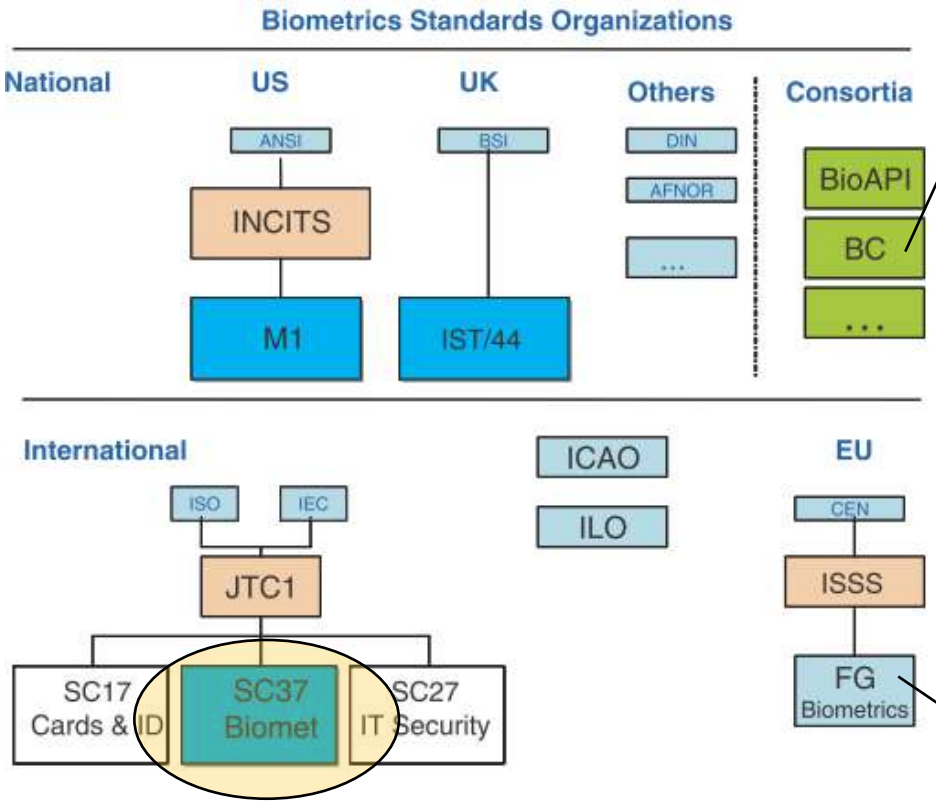
Sistemas Biométricos - Armazenamento

Universidade do Minho
Escola de Engenharia

- Padrões biométricos, complementados com…
  Indicadores de qualidade
  Contexto (sensores, algoritmos, etc.)
  Identificação
  Raw data (estudo e avaliação de biometrias)
  …
- Bases de dados disponíveis:
  - CASIA / Biometrics Ideal Test (http://biometrics.idealtest.org/)
  - FERET entre muitas outras, para reconhecimento da face: http://www.face-rec.org/databases/
  - Usadas em competições internacionais (http://www.nist.gov/biometrics-portal.cfm)
- Segurança no armazenamento
  - Criptografia

Biometrias - Normalização

Universidade do Minho
Escola de Engenharia



Biometric Consortium (NSA e NIST…)

Focus Group Biometrics, já fechado

(Deravi 2008)

Biometrias - desafios

Universidade do Minho
Escola de Engenharia

- Precisão e avaliação
- Escalabilidade
- Segurança
- Privacidade

Precisão e avaliação

Universidade do Minho
Escola de Engenharia

- Diferentes tipos de avaliações
  - Tecnológica
    - Carece de uma base de dados de teste “limpa” e normalizada; repetível; avaliar algoritmos
  - Operacional
    - Dados obtidos em tempo-real; ambiente não duplicável; avaliar o desempenho de um sistema
  - Cenário
    - Dados do ambiente real (reutilizáveis se a recolha for controlada); avaliar o desempenho de um sistema completo, através de um protótipo de aplicação ou um ambiente simulado
- Não obstante as diferenças, as ferramentas são as mesmas
- Mais crítico na Identificação, mas igualmente relevante na Verificação (Autenticação)

(Gamassi, Lazzaroni et al. 2005)

Precisão e avaliação

Universidade do Minho
Escola de Engenharia

- Problema: decisão discreta (aceita/rejeita) baseada em dados probabilísticos, subjacentes à definição de um *threshold*.

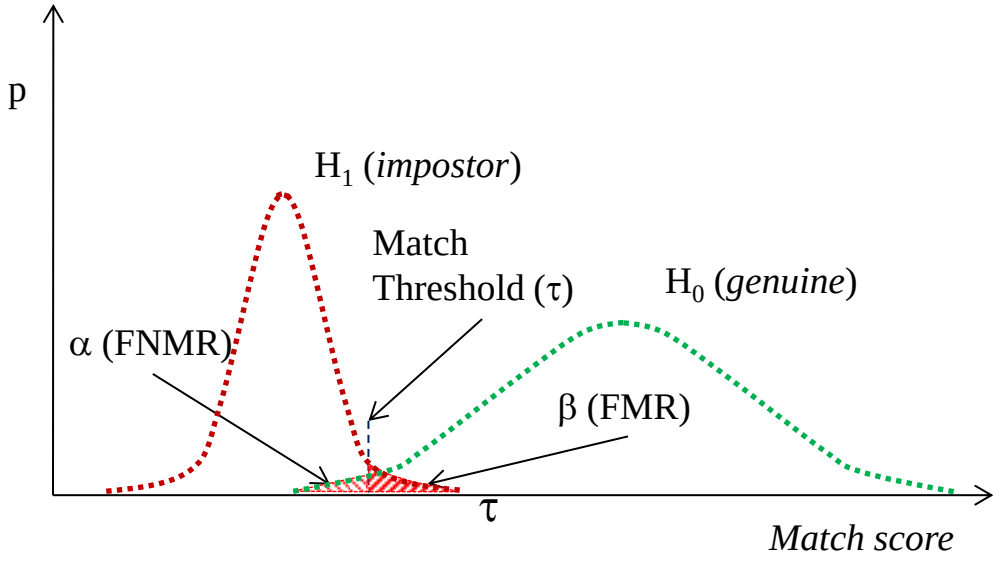
  "**Qual a probabilidade do sistema de verificação tomar uma decisão errada?**"

- Formulação: *Hypothesis testing*
  - *Null hypothesis* (H_0): a identidade reivindicada é verdadeira (genuíno)
  - *Alternative hypothesis* (H_1): a identidade reivindicada é falsa (impostor)
  - *Test statistic*: normalmente um valor escalar (*score*) que resume toda a informação que apoia a decisão.
  - Resultado: não rejeitar H_0; ou rejeitar H_0 a favor de H_1

Biometrias - verificação

Universidade do Minho
Escola de Engenharia

- Exemplo de possíveis funções de densidade de probabilidades dos valores de similaridade, para genuínos (H_0 verdadeira) e impostores (H_1 verdadeira)
- A sobreposição é a origem dos **erros de decisão** - definição do *threshold* é crítica
  - Erros do Tipo I – quando H_0 é verdadeira, mas a decisão é rejeitar (FR ou FNM)
    A probabilidade de ocorrência de um FNM é dada por α e designa-se por FNMR
  - Erros do Tipo II – quando H_0 é falsa, mas a decisão é aceitar (FA ou FM)
    A probabilidade de ocorrência de um FM é dada por β e designa-se por FMR



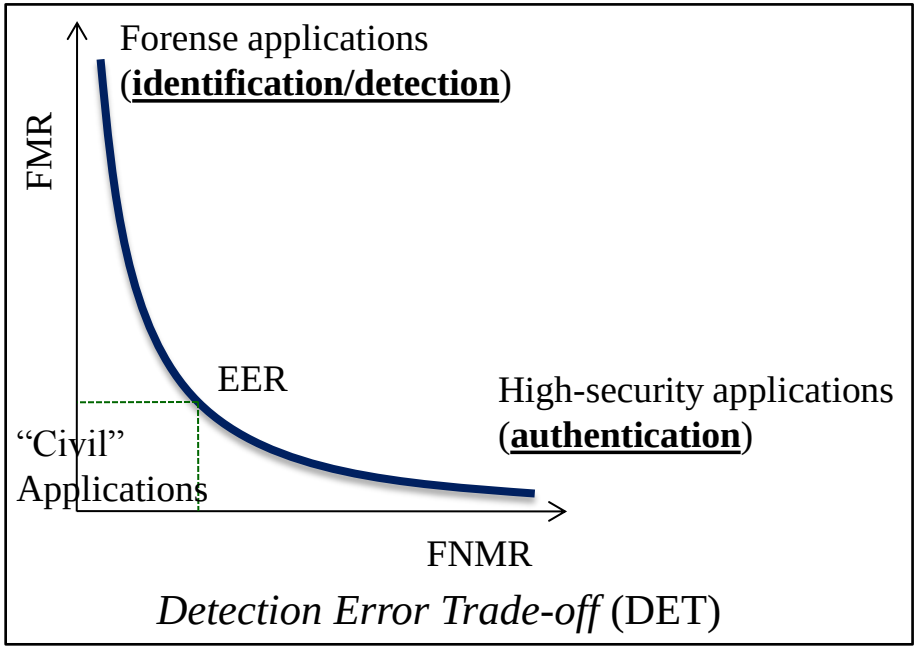
$$\beta = \int_{\tau}^{+\infty} f_{H1}(S)ds$$

$$\alpha = \int_{-\infty}^{\tau} f_{H0}(S)ds$$

Biometrias – avaliação na verificação (curvas DET)

Universidade do Minho
Escola de Engenharia

- FMR e FNMR variam de forma inversa em função de τ



(Delac, 2004)

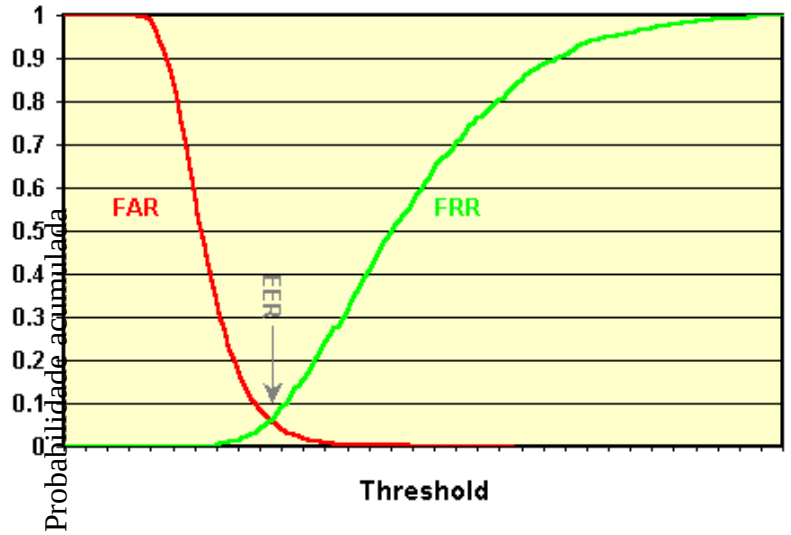
- EER – *Equal Error Rate* (resume num valor, um possível indicador de desempenho!)
  - Mas $EER_A < EER_B \not\Rightarrow$ A melhor que B

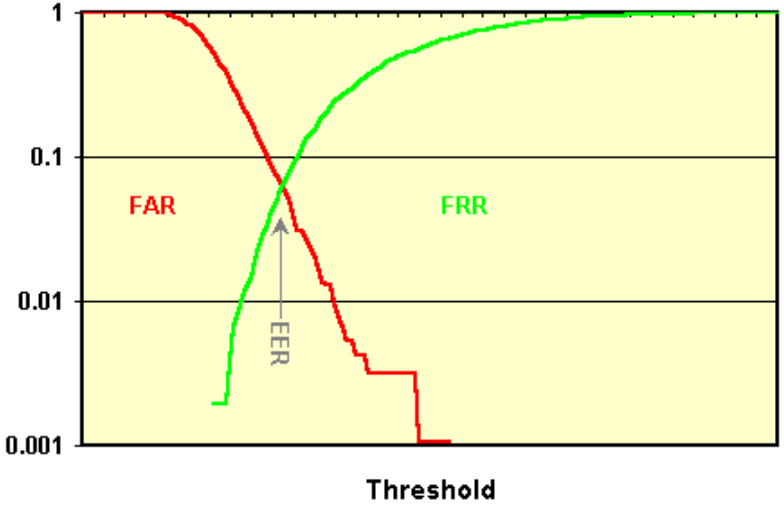
Nota: FMR e FNMR são valores estatísticos não estacionários!

Biometrias – avaliação na verificação (curvas DET)

Universidade do Minho
Escola de Engenharia

- Outra forma de apresentar as curvas DET (exemplo com escala linear e logarítmica)

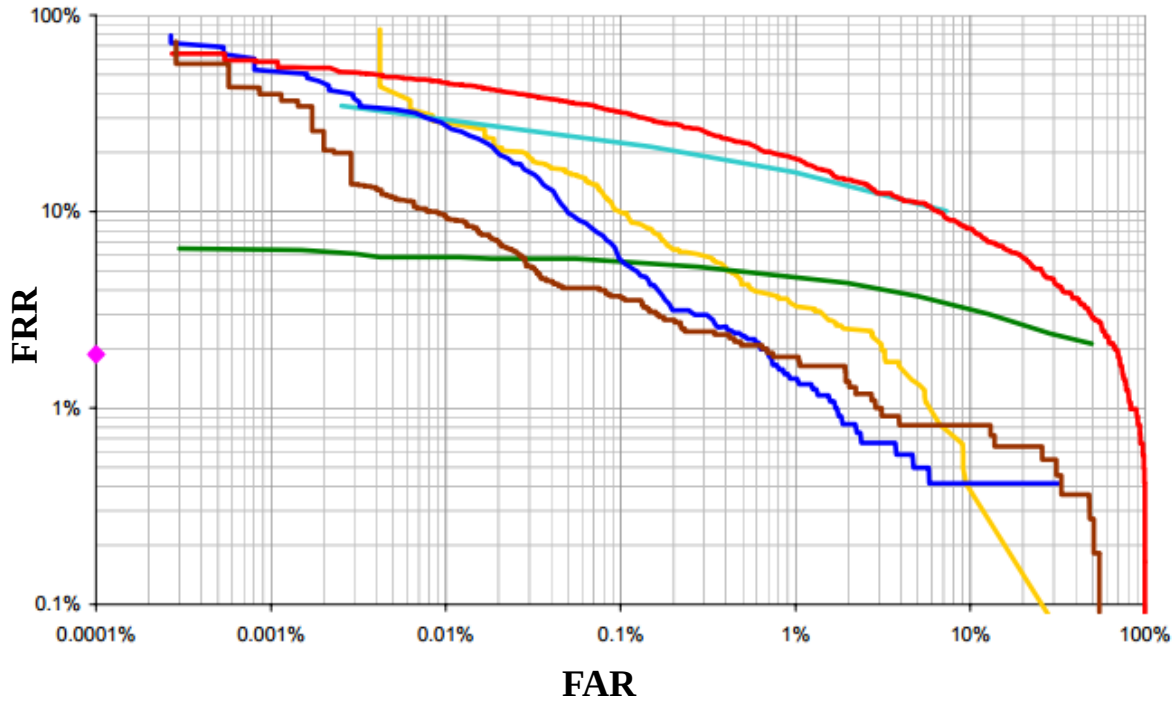




Biometrias – avaliação na verificação (curvas DET)

Universidade do Minho
Escola de Engenharia

- Outro exemplo de curvas DET explorando escalas logarítmicas



Biometrias – avaliação na verificação

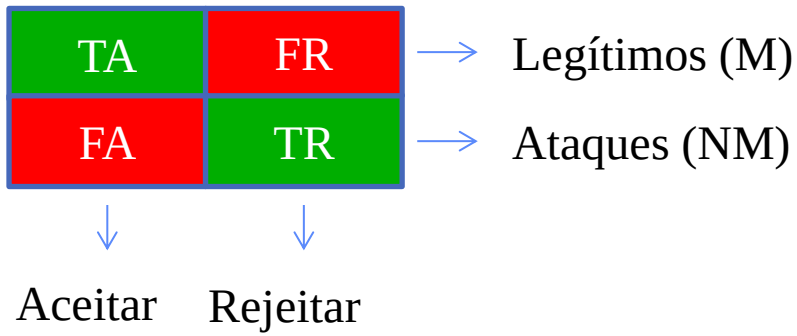
Universidade do Minho
Escola de Engenharia

- Outras definições típicas num sistema de decisão binária
  - TA – *hits*, ou verdadeiros positivos
  - TR – verdadeiros negativos, ou rejeições corretas
  - FR – falsos negativos (*type I error*)
  - FA – falsos positivos (*type II error*)

    M (nº total de legítimos) = TA + FR ⇔ TA = M - FR e

    NM (nº total de ataques) = TR + FA ⇔ TR = NM - FA
  - TAR = TA/M = 1 - FRR – sensibilidade
  - TRR = TR/NM = 1 - FAR – especificidade
  - ACC = (TA + TR)/(M + NM) – precisão

Confusion Table

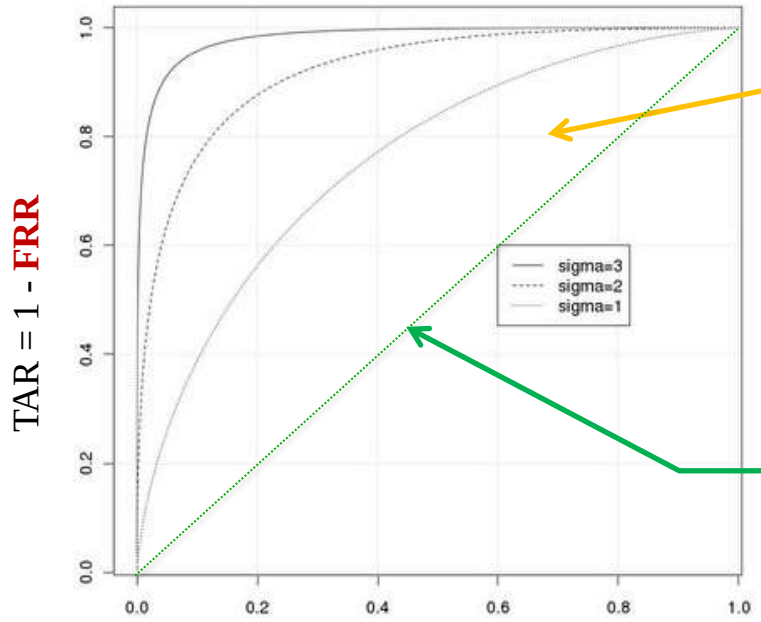


(Bewick, Cheek et al. 2004) e
(Ratha and Govindaraju 2008)

Biometrias – avaliação na verificação (curvas ROC)

Universidade do Minho
Escola de Engenharia

- As curvas ROC (*Receiver Operating Characteristic*) revelam-se mais úteis a relacionar FAR com FRR



Área definida pela curva ROC é um indicador do desempenho global

Limite do desempenho para qualquer algoritmo de decisão útil

(Fawcett 2006)

Biometrias – Avaliação individual

Universidade do Minho
Escola de Engenharia

- Limitações da análise global (dados agregados)
- Fatores individuais que condicionam a avaliação
  - Fisiológicos
  - Comportamentais
  - Interação
- Análise individual do valor de limiar τ …!
- Análise levou à criação da *Biometric Menagerie* (Yager, 2010)

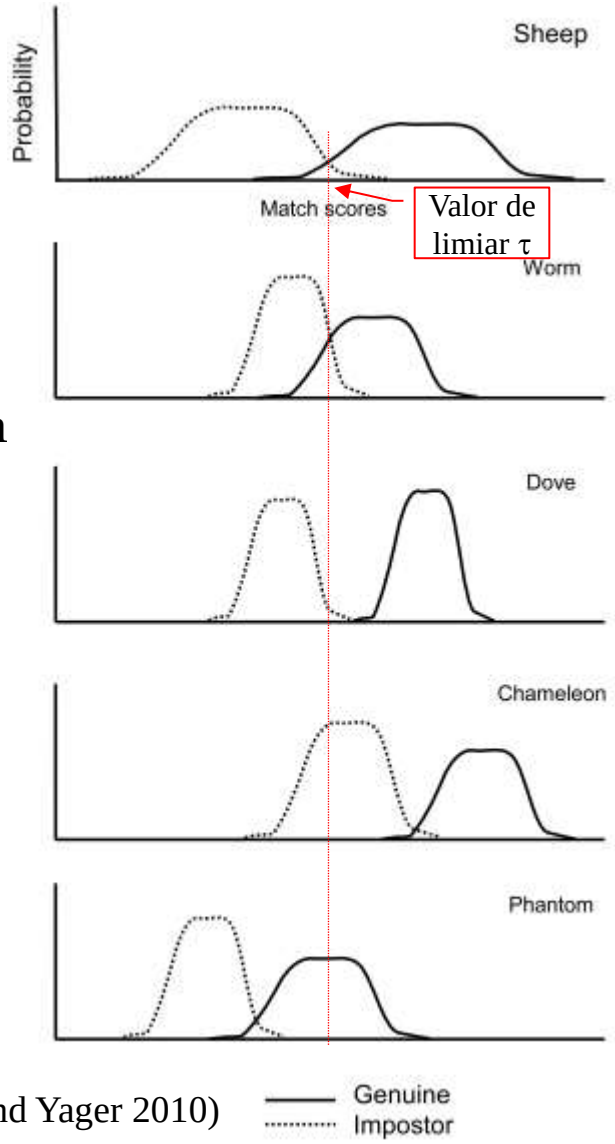
Biometrias – Avaliação individual

Universidade do Minho
Escola de Engenharia

- Classificação em função do desempenho global
  - *Sheep* – o normal
  - *Goats* – número muito elevado de FNM
  - *Lambs* e *Wolves* – número muito elevado de FA (similaridade como genuíno é baixa; similaridade como atacante é elevada)

Biometrias – Avaliação individual

- Classificação em função da distribuição individual
  - *Doves* – a melhor distribuição
  - *Worms* – a pior distribuição
  - *Chameleons* – facilmente impersonalizam
  - *Phantoms* – Dificilmente se autenticam

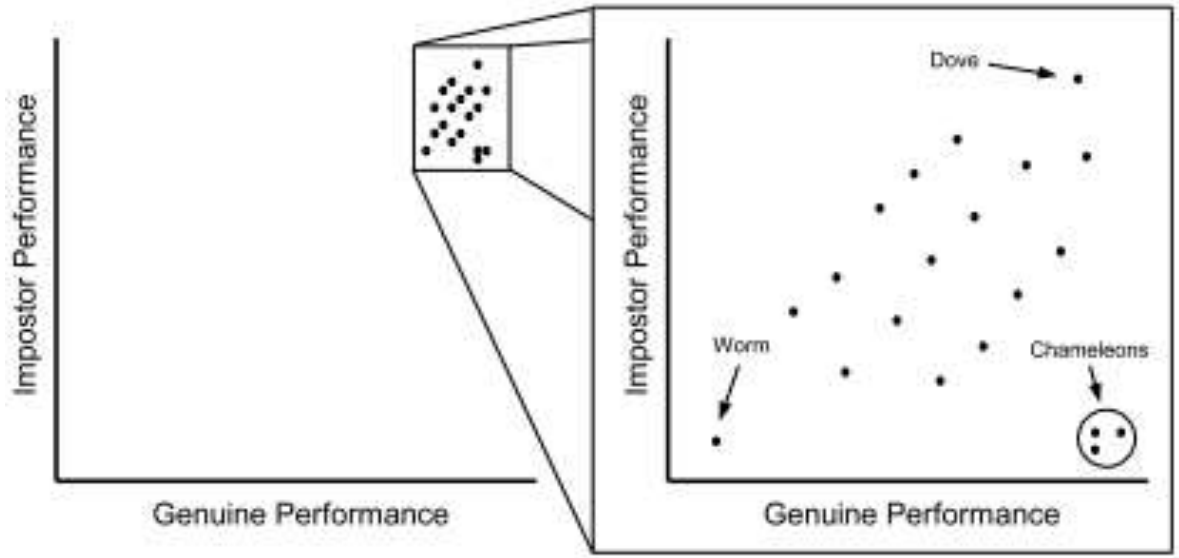


adaptado de (Dunstone and Yager 2010)

Biometrias – Avaliação individual

Universidade do Minho
Escola de Engenharia

- *Zoo Plot* (desempenho como genuíno e contra impostores); efeito de escala deve ser considerado para identificar os grupos



(Dunstone and Yager 2010)

Avaliação de Biometrias

Um caso prático

Biometrias – limitações na avaliação

Universidade do Minho
Escola de Engenharia

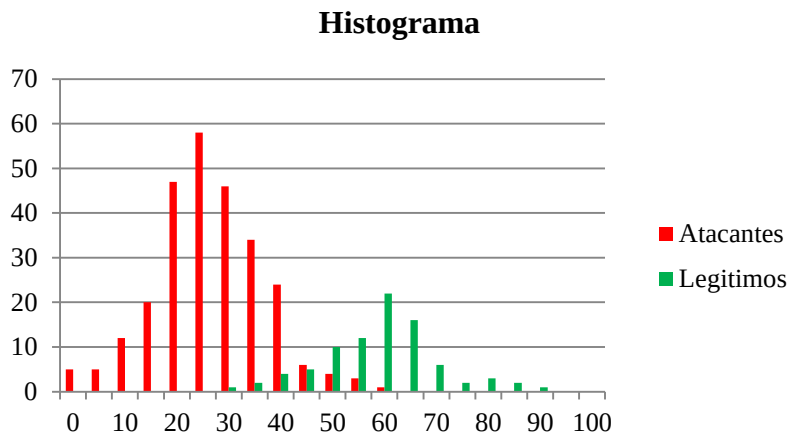
- Desempenho da biometria
  - Como determinar, à priori, as funções de densidade de probabilidades? Não são distribuições típicas e têm que ser determinadas empiricamente. A recolha das amostras é um processo determinante:
    - Os sujeitos devem ser representativos da população alvo
    - Todos os *scores* devem ser registados (em toda a gama de valores)
    - Deve recolher-se o máximo possível de amostras genuínas e impostoras
    - Nunca assumir alguma forma paramétrica de distribuição!

Exemplo prático

Universidade do Minho
Escola de Engenharia

- Exemplo: 10 impostores; 2 legítimos; 30 ou mais capturas de cada um

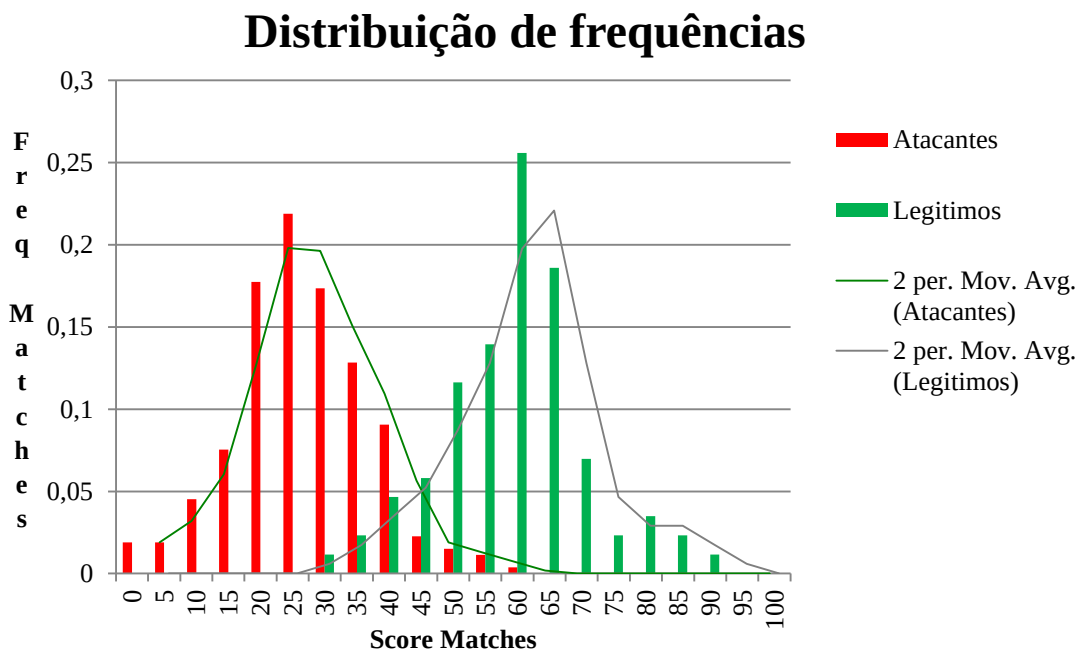
Scores	0	5	10	15	20	25	30	35	40	45	50	55	60	65	70	75	80	85	90	95	100	
Atacantes	5	5	12	20	47	58	46	34	24	6	4	3	1	0	0	0	0	0	0	0	0	265
Legitimos	0	0	0	0	0	0	1	2	4	5	10	12	22	16	6	2	3	2	1	0	0	86
Atacantes	0,02	0,02	0,05	0,08	0,18	0,22	0,17	0,13	0,09	0,02	0,02	0,01	0	0	0	0	0	0	0	0	0	1
Legitimos	0	0	0	0	0	0	0,01	0,02	0,05	0,06	0,12	0,14	0,26	0,19	0,07	0,02	0,03	0,02	0,01	0	0	1
FMR	1	0,98	0,96	0,92	0,84	0,66	0,45	0,27	0,14	0,05	0,03	0,02	0	0	0	0	0	0	0	0	0	
FNMR	0	0	0	0	0	0	0,01	0,03	0,08	0,14	0,26	0,4	0,65	0,84	0,91	0,93	0,97	0,99	1	1	1	
TMR	1	1	1	1	1	1	0,99	0,97	0,92	0,86	0,74	0,6	0,35	0,16	0,09	0,07	0,03	0,01	0	0	0	
Utiliz. 1	0	0	0	0	0	0	1	2	4	5	7	6	7	4	2	1	1	0	0	0	0	40
Utiliz. 1	0	0	0	0	0	0	0,03	0,05	0,1	0,13	0,18	0,15	0,18	0,1	0,05	0,03	0,03	0	0	0	0	1
Utiliz. 2	0	0	0	0	0	0	0	0	0	0	3	6	15	12	4	1	2	2	1	0	0	46
Utiliz. 2	0	0	0	0	0	0	0	0	0	0	0,07	0,13	0,33	0,26	0,09	0,02	0,04	0,04	0,02	0	0	1



- Indicadores obtidos para $\tau = 42$:
  - FM = 14 $\Rightarrow$ FMR = 0,05
  - FNM = 7 $\Rightarrow$ FNMR = 0,08
  - TM = 79 $\Rightarrow$ TMR = 0,92
  - TNM = 251 $\Rightarrow$ TNMR = 0,95

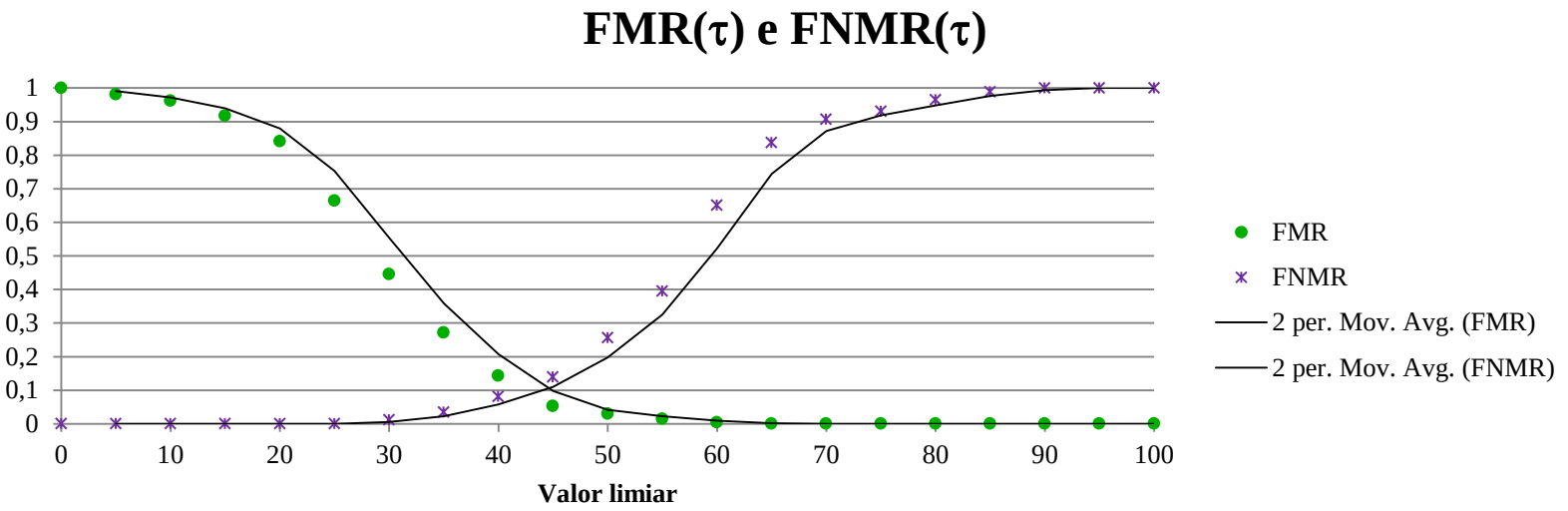
Exemplo prático - DF

Universidade do Minho
Escola de Engenharia



Exemplo prático – Curva DET

Universidade do Minho
Escola de Engenharia



$$\tau_1 = \max_{\tau}\{\tau | FNMR(\tau) \leq FMR(\tau)\},$$

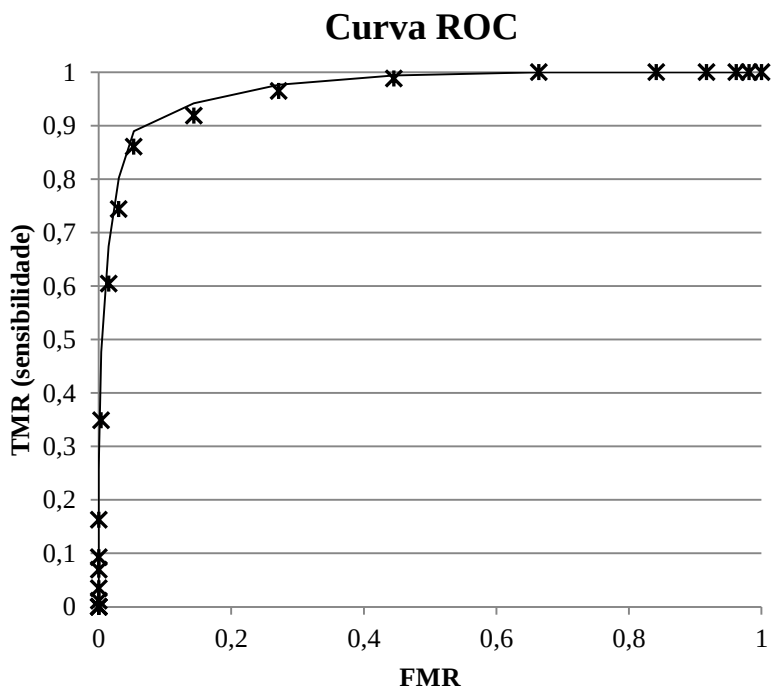
$$\tau_2 = \min_{\tau}\{\tau | FNMR(\tau) \geq FMR(\tau)\},$$

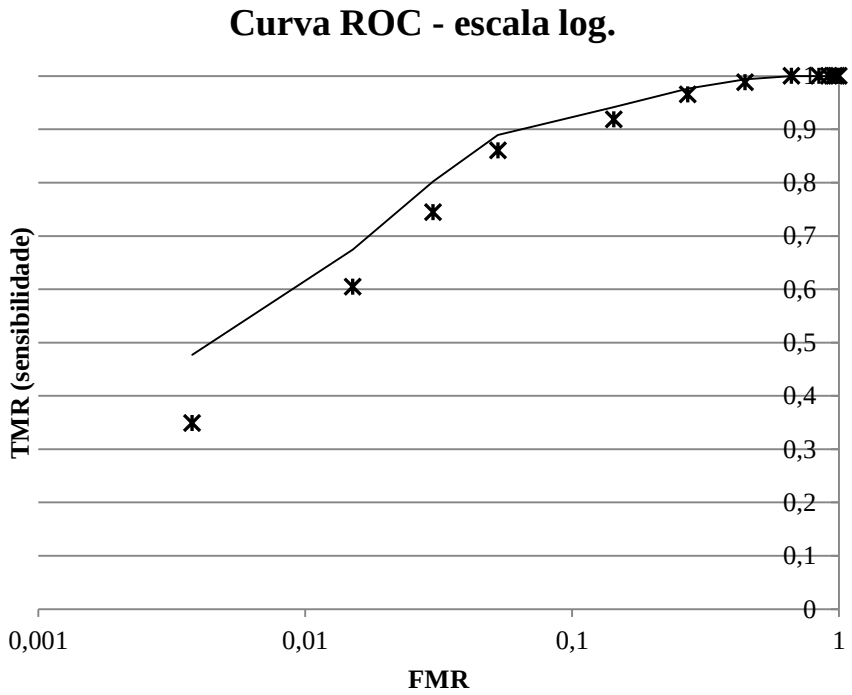
$$\left[EER_{low}, EER_{high}\right] = \begin{cases} [FNMR(\tau_1), FMR(\tau_1)] & if\ FNMR(\tau_1) + FMR(\tau_1) \leq \\ & FMR(\tau_2) + FNMR(\tau_2) \\ [FNMR(\tau_2), FMR(\tau_2)] & otherwise \end{cases}$$

$$e\ EER = \frac{EER_{low} + EER_{high}}{2}$$

Exemplo prático – Curvas ROC

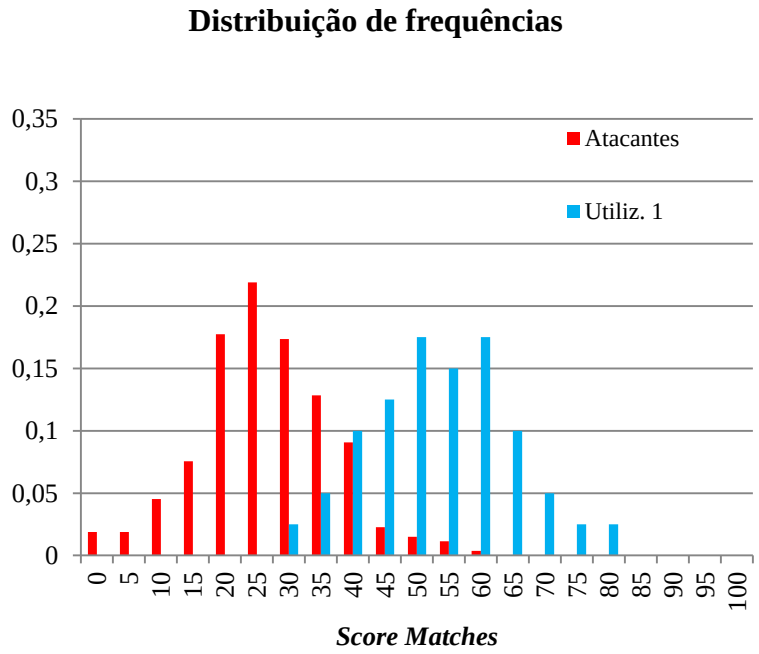
Universidade do Minho
Escola de Engenharia

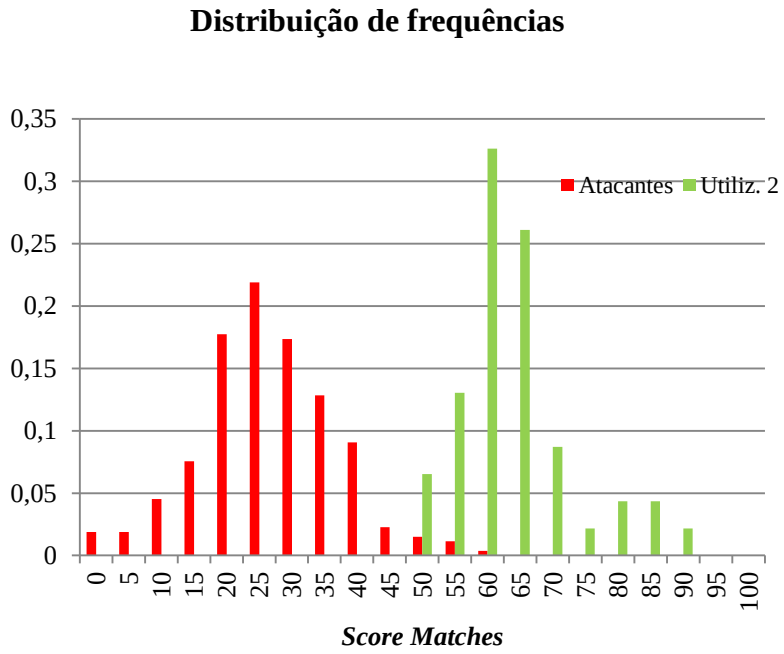




Exemplo prático – Anal. individual

Universidade do Minho
Escola de Engenharia





Biometrias - desempenho

Universidade do Minho
Escola de Engenharia

- Outros factores a considerar no desempenho
  - FTE (*Failure To Enroll*): traduz o número de falhas no processo de registo
  - FTC (*Failure To Capture*): traduz o número de falhas no processo de captura das biometrias
  - Limitações da informação inerente ao método
  - Limitações da representação
  - Limitações das invariantes (frequentemente devido à utilização de um conjunto limitado de dados de teste/aprendizagem)

Biometrias - escalabilidade

Universidade do Minho
Escola de Engenharia

- Em que medida o número de indivíduos arrolados afectam o desempenho do sistema?
  - Verificação (não há problema, uma vez que se trata de uma operação **1:1**)
  - Identificação em larga escala e detecção
    - Não é praticável fazer **N** operações de **1:1**
  - Soluções
    - Multiplicação de recursos ☹
    - Classificação de padrões através de dados exógenos e/ou em vários grupos (e.g, *whorl, right loop, arch, tented arch*)
    - Algoritmos de verificação mais complexos e eficientes
    - Soluções baseadas nestas duas últimas alternativas tendem a reflectir-se no desempenho ☹

Biometrias – segurança

Universidade do Minho
Escola de Engenharia

- Factos
  - Informação biométrica não é secreta
  - Padrões biométricos não são revogáveis, nem refutáveis
- Ataques
  - É "possível" duplicar o padrão biométrico
  - O legitimo possuidor de um padrão biométrico tem muita dificuldade em refutar o seu envolvimento num ataque
  - Bio-exclusão
  - Infra-estruturas tecnológicas de suporte
- Soluções
  - Garantir utilização apenas de utilizadores "vivos" e sensores mais eficazes
  - Sistemas **multi-dimensionais**

Consequência da **unicidade** dos dados biométricos

Biometrias – segurança (tecnológica)

Universidade do Minho
Escola de Engenharia

Sensor

Extracção do padrão biométrico

Classificador

Decisão

Base de dados (Modelos)

Padrões falsos. Algum tipo de software malicioso (bastante difícil).

Resultados da similaridade falsos (eventualmente independentes do padrão real). Algum tipo de software malicioso.

Solução: Criptografia!…

Característica falsa (duplicação ou ataques por "força bruta"):

- Voz gravada
- Impressões digitais "fabricadas"
- Olho sintético
- Disfarce
- etc.

Ataques à Base de Dados

- Ataques genéricos (DoS, *SQL injection*, etc.)
- Integridade de padrões armazenados…

Biometrias – privacidade

Universidade do Minho
Escola de Engenharia

- Os dados biométricos poderão ser usados violando o direito à privacidade?
- Os dados biométricos poderão ser usados para outro fim?
- Os dados biométricos poderão ser utilizados para cruzar informação envolvendo a identidade do indivíduo?
- Soluções:
  - Criptografia biométrica
  - Total transparência
  - Sistemas de detecção de “má utilização”
  - …

Conclusões

Universidade do Minho
Escola de Engenharia

- Controlo de Acesso é um controlo chave em segurança da informação
- Autenticação do utilizador é uma das questões centrais
- Várias tecnologias com níveis de maturidade elevada. Mas…
  - Escalabilidade e usabilidade ainda são problemas
  - Necessário investir mais em sistemas multi-dimensionais
- Questões de usabilidade são relevantes!
- Capacidade para explorar a autenticação contínua, possibilitando a "autenticação automática"

Bibliografia

Universidade do Minho
Escola de Engenharia

1. Kaufman, C., Perlman, R. and Speciner, M. Network Security: Private Communication in a Public World. Prentice Hall PTR, Upper Saddle River, NJ 07458, 2002. (cap. 9)
2. **Jain, A. K., Ross, A. and Prabhakar, S., An introduction to biometric recognition, Circuits and Systems for Video Technology, IEEE Transactions on, 14, 1, 4-20, 2004**
3. Bishop, M., Introduction to Computer Security, Prentice Hall PTR, 2004. (cap 3 a 7)
4. **Sandhu, R. S. and Samarati, P., Access control: Principles and practice. IEEE Communications Magazine 32(9): 40-49, 1994**
5. Sandhu, R. S., E. J. Coyne, et al., Role based access control models, Computer 29(2): 38-47, 1996
6. **Dunstone, T. and Yager, N. Biometric System and Data Analysis: design, evaluation and data mining. Springer, 2010**
7. Maltoni, D., et. all, Biometric Systems: Technology, Design and Performance Evaluation, Springer, 2005
8. Jain, A. K., Biometrics: Personal Identification in Networked Society, Kluwer Academic Publishers, 1999
9. Delac, K. and M. Grgic (2004). A survey of biometric recognition methods. 46th International Symposium Electronics in Marine, ELMAR-2004
10. **Magalhães, P. S., Estudo dos padrões de digitação e sua aplicação na autenticação biométrica Master Thesis, Departamento de Sistemas de Informação, Universidade do Minho, 2005**
11. A. Rashed and H. Santos, Multimodal Biometrics and Multilayered IDM for Secure Authentication, in Global Security, Safety, and Sustainability. vol. 92, S. Tenreiro de Magalhães, et al., Eds., ed: Springer Berlin Heidelberg, 2010, pp. 87-95
12. Strebe, M., Network Security Foundations: Technology Fundamentals for IT Success, Sybex, 2004. (cap. 3)

---

1. Yager, N. and Dunstone, T. The Biometric Menagerie. Pattern Analysis and Machine Intelligence, IEEE Transactions on, 32, 2 2010), 220-230
2. The Biometric Consortium http://www.biometrics.org/index.htm
3. Biometrics Research Homepage at MSU http://biometrics.cse.msu.edu/index.html
4. IBG BioPrivacy Initiative http://www.bioprivacy.org/