Actas da 4ª Conferência da Associação Portuguesa de Sistemas de Informação". Porto. Portugal. 15-17/10/2003 (edição em CD-ROM: ISBN 97 2-9354-42-1).

Biometria e autenticação

Paulo Sérgio Magalhães

Universidade do Minho, Guimarães, Portugal

psmagalhaes@mail.pt

Henrique Dinis Santos

Universidade do Minho, Guimarães, Portugal

hsantos@dsi.uminho.pt

Resumo

Com a utilização cada vez maior de Tecnologias da Informação e das Comunicações (TIC) nos Sistemas de Informação (SI) das organizações, surgem com crescente evidência os problemas de segurança e, em particular, a questão da autenticação do utilizador. Esta questão é hoje fundamental já que o acesso indevido a informação sensível pode provocar grandes prejuízos à organização. Neste trabalho descreve-se uma das técnicas utilizadas na autenticação, a biometria, como forma de aumentar a *qualidade da autenticação*. Nesse sentido, é analisado o estado da arte, são identificadas algumas vantagens, desvantagens e limitações das principais tecnologias desenvolvidas e procura-se perceber o impacto que a autenticação biométrica pode ter nas organizações, quando conjugada com a tecnologia proporcionada pelos cartões com capacidade de processamento e armazenamento seguro, conhecidos como Smart Cards. Finalmente, é brevemente introduzido o projecto de investigação em curso para o desenvolvimento de um sistema que explora estas tecnologias.

Palavras-chave: autenticação, biometria, segurança, Smart Cards

1. **Introdução**

O problema de estabelecer uma associação entre um indivíduo e uma identidade pode ser dividido em duas categorias: autenticação e identificação. *Autenticação* refere-se ao problema de confirmar ou negar uma alegada identidade de um indivíduo, enquanto *identificação* refere-se ao problema de estabelecer a identidade, desconhecida à partida, de um indivíduo [Thian 2001]. O âmbito deste documento é a autenticação de um sujeito ligado, directa ou indirectamente, ao indivíduo ou organização que pretende confirmar a sua identidade.

Quando um operário fabril, ao entrar no seu posto de trabalho, passa pelo relógio de ponto para carimbar o seu cartão ou registar a passagem do seu cartão magnético, fornece uma informação à organização: a que horas se apresentou ao serviço. Esta informação tem consequências no custo que a sua organização irá ter com o seu salário. A pergunta que se põe é "como é que sabemos que não é o primeiro operário a chegar e o último a sair quem carimba todos os cartões?".

O exemplo apresentado pode ser um tanto exagerado mas representa uma das situações em que a autenticação fraudulenta pode acarretar custos para uma organização. Muitos outros exemplos podem ser apresentados: o acesso não autorizado à contabilidade de uma empresa por alguém que obteve a palavra passe do contabilista, o acesso a um laboratório de alta segurança, ou simplesmente o acesso a informação estratégica por alguém que se faz passar por um utilizador legítimo.

A procura de um método de autenticação tem sido vasta, envolvendo, tradicionalmente, sistemas que têm a ver com a partilha de um segredo entre utilizador e objecto de segurança.

Um dos problemas deste método é a transmissibilidade do segredo que, como qualquer outro, pode ser cedido (voluntariamente ou não) por quem o conheça a terceiros. Outro problema deste método é a necessidade de armazenamento ou memorização do segredo. Quando o segredo é armazenado, naturalmente herdamos o conjunto de vulnerabilidades que o(s) sistema(s) de armazenamento evidencia(m). Quando o segredo é memorizado pode ser esquecido, o que normalmente leva à escolha de segredos simples, que facilitem a respectiva memorização.

Assim, existe a necessidade de complementar os métodos existentes de autenticação com um local de armazenamento seguro e um factor inerente ao sujeito autenticado. É assim que surgem no contexto da autenticação, os Smart Cards e a autenticação biométrica.

2- Smart Cards

Genericamente, dizemos que um Smart Card é um cartão com as dimensões de um cartão de crédito, munido de um chip com ou sem microprocessador. As dimensões de um Smart Card estão normalizadas pela norma ISO 7816. Fora destas dimensões encontram-se os cartões SIM (Subscriber Identification Module), utilizados pelo sistema de comunicações móveis GSM (Global System Mobile Communication). No entanto, alguns autores consideram estes cartões como um tipo de Smart Card. No contexto deste trabalho apenas consideramos os Smart Cards equipados com processador.

Um Smart Card possui três tipos de memória: *Random Access Memory* – RAM – volátil; EEPROM – Electric Erasable Programmable Read Only Memory – permanente e alterável após o fabrico do Smart Card; e Read Only Memory – ROM – gravada no processo de fabrico do cartão e não alterável. A capacidade de armazenamento e processamento de um Smart Card é reduzida e limita as suas funcionalidades, apesar de a sua configuração ter evoluído ao longo dos últimos anos, num processo semelhante à evolução dos pequenos computadores no final dos anos oitenta. A limitação imposta pelo hardware do Smart Card é habitualmente contornada através da repartição do processamento necessário entre o cartão e o terminal a que ele vai ser ligado – *host* – que pode ser de diversos tipos, desde que esteja equipado com um CAD (Card Acceptance Device).

Existem diversas tecnologias para programar Smart Cards, orientadas, frequentemente, para situações tipo e que de seguida são sumariamente descritas, com base numa compilação exaustiva efectuada por [Chen 2000]

A empresa SUN desenvolveu a Java Card Virtual Machine, uma Java Virtual Machine (JVM) limitada, capaz de interpretar um subconjunto da linguagem Java e o protocolo de comandos específicos suportados pelos Smart Cards.

GSM é o nome genérico de um conjunto de normas publicadas pelo European Telecommunications Standard Institute destinadas à utilização em sistemas de comunicações envolvendo sistemas telefónicos. Esta norma tem um nível de aceitação cada vez maior, não só na Europa onde surgiu, como na Ásia e, mais recentemente, no continente Americano. Esta especificação recorre à utilização de um tipo específico de Smart Card, já referido, o SIM card .

A especificação EMV – Europay, Mastercard & VISA - é baseada na norma ISO 7816 e foi desenvolvida de modo a incluir extensões adequadas às necessidades das empresas financeiras.

A especificação OP (Open Platform) foi inicialmente desenvolvida pela VISA e, mais tarde, transferida para a GlobalPlatform. Esta especificação tinha como objectivo a uniformização das implementações em tecnologias ligadas a Smart Cards. A especificação OP exige que os leitores sejam compatíveis com as normas ISO e com a especificação EMV (também desenvolvida pela VISA) e define características que uma aplicação deverá possuir para ser uma tecnologia independente do fabricante do leitor e dos cartões.

As especificações PC/SC (Personal Computer/Smart Card) propõem uma arquitectura para a utilização de Smart Cards em computadores pessoais. De acordo com esta especificação, os programas executados no sistema anfitrião (um computador pessoal) são construídos sobre um ou mais fornecedores de serviços e um gestor de recursos. O fornecedor de serviços transforma as especificidades de cada fabricante, tornando-as transparentes para o utilizador. O gestor de recursos, como o nome indica, gere os recursos necessários para o acesso do sistema ao CAD – aqui denominado Interface Device – e, a partir daí, a um cartão. Este gestor de recursos deverá: detectar os leitores existentes e, consequentemente, os tipos de cartões disponíveis; gerir os acessos concorrentes a um cartão: e detectar a inserção e remoção dos cartões de modo a identificar e informar as aplicações dos cartões e serviços disponíveis a cada instante. As PC/SC estão essencialmente dirigidas para o sistema Windows e, neste Sistema Operativo, qualquer aplicação desenvolvida segundo o Opencard Framework consegue aceder ao dispositivo leitor de cartões através do gestor de recursos do PC/SC.

O consórcio OpenCard (www.opencard.org) foi criado pelas principais empresas ligadas aos Smart Cards, com o objectivo de criar plataformas normalizadas que permitam a interoperabilidade de aplicações independentemente do produtor do cartão/leitor. Apesar de não haver ainda uma norma que permita programar para qualquer aparelho, é já possível, em muitos casos, programar o acesso ao cartão sem a preocupação de programar explicitamente os acessos à porta física. Ao atingir níveis de abstracção mais elevados, com a consequente facilidade de integração e programação, é admissível uma clara afirmação desta tecnologia. De notar ainda

que esta especificação foi desenhada tendo em vista o funcionamento em redes informáticas e é implementada em linguagem Java.

3- A autenticação biométrica

O termo biometria deriva do grego *bios* (vida) + *metron* (medida) e, na autenticação, refere-se à utilização de características próprias de um indivíduo para proceder à sua autenticação e/ou identificação perante um SI de uma organização.

Existem hoje muitas características utilizadas, isoladamente ou em conjunto, para autenticar e/ou identificar um sujeito. Cada um dos métodos pode ser avaliado através de vários parâmetros: grau de fiabilidade, nível de conforto, nível de aceitação e custo de implementação. [Liu et al. 2001].

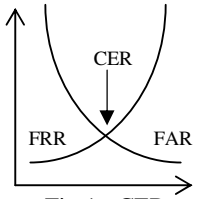

Fig.1 - CER

O grau de fiabilidade pode ser aferido tendo em atenção os valores FAR (False Acceptance Rate – Taxa de Falsas Aceitações) e o FRR (False Rejection Rate – Taxa de Falsas Rejeições). Infelizmente estas variáveis são mutuamente dependentes, não sendo possível minimizar ambas. Assim, procura-se o ponto de equilíbrio (fig.1) a que chamamos CER (Crossover Error Rate – Taxa de Intersecção de Erros). Quanto mais baixo for o CER mais preciso é um sistema biométrico [Liu et al. 2001].

O nível de conforto é um padrão de certa forma subjectivo e está profundamente ligado ao público utilizador do sistema.

Outro padrão subjectivo é o nível de aceitação. De um modo geral o sistema é tanto melhor aceite pelos utilizadores quanto menos intrusivo for.

O custo de implementação é um factor fundamental e abrange diversos factores, alguns dos quais frequentemente descurados [Liu et al. 2001]:

- Hardware;
- Software;
- Integração com hardware/software existentes;
- Formação dos utilizadores;
- Pessoal de manutenção de Bases de Dados;
- Manutenção do sistema;

A escolha do(s) método(s) a utilizar depende da análise de risco que necessariamente deve ser feita, relativamente à informação/infra-estrutura que se pretende proteger. Por exemplo,

o aeroporto Narita (Tóquio) pretende implementar um processo de autenticação que inclui o reconhecimento de rosto e o reconhecimento da íris em conjunção. A Central Intelligence Agency (CIA), o Federal Bureau of Investigation (FBI) e a National Aeronautics and Space Administration (NASA) utilizam leitores de retina para proteger o acesso a zonas sensíveis. No entanto, seria excessivamente dispendioso e desajustado utilizar leitores de retina ou de íris para autenticar/identificar o utilizador de um computador pessoal no laboratório de informática de uma universidade.

4- Tecnologias de autenticação biométrica

4.1 Reconhecimento facial

No reconhecimento facial os problemas são essencialmente provocados por diferentes orientações da cabeça [Poh et al. 2001].

O processo tem início com a captura de uma imagem, seguida da detecção de um rosto que será comparada com modelos armazenados numa base de dados, complementada com a análise da cor da pele, detecção de linhas ou ainda de um modelo híbrido [Thian 2001].

Os processos baseados neste tipo de biometria são limitados pelo facto de o utilizador ter que ser enquadrado com o modelo, dada a dificuldade (processamento necessário) em adaptar o modelo à sua cara, isto para além da necessidade de adaptar o modelo a todas as condições que podem alterar a aparência de um indivíduo, como o uso de óculos, envelhecimento, barba, etc.. Este processo baseia-se essencialmente na localização de pontos fixos como os olhos, nariz e boca [Poh et al. 2001][Thian 2001].

Os casinos têm utilizado esta tecnologia com sucesso para criar uma base de dados de faces de burlões, de modo a facilmente serem identificados pela segurança [Liu et al. 2001].

4.2 Geometria da mão

O reconhecimento da geometria da mão resulta de uma análise das características da mão como a forma, o comprimento dos dedos e as suas linhas características. Podemos ter diferentes níveis de segurança neste sistema consoante se utilizem as características em si, a posição das características relativamente a um ponto fixo ou a fixação de vários pontos e as distâncias das características relativamente a todos eles.

De realçar que não existe nada que indique que a geometria da mão (tal como os algoritmos de hoje a interpretam) é uma característica própria de cada indivíduo.

Por outro lado, a geometria da mão, comparada com outras biometrias, não produz um grande conjunto de dados. Portanto, dado um grande número de registos, a geometria da mão

pode não ser capaz de distinguir um indivíduo de outro com características da mão semelhantes [Thian 2001].

4.3 Impressão digital

É, sem dúvida, a tecnologia biométrica mais utilizada actualmente. Esta biometria tem um nível de aceitação muito satisfatório, provavelmente devido ao facto de a impressão digital ser há muito tempo utilizada nos registos civis e em investigações criminais.

Esta tecnologia é, de entre as biometrias físicas, a de menor fiabilidade. Os equipamentos normalmente utilizados para a captura dos padrões não distinguem, eficientemente, um dedo vivo de um dedo morto (separado do utilizador legítimo ou replicado sinteticamente). Aliás, é muito fácil produzir uma impressão digital sintética com ou sem a colaboração do seu proprietário. Os passos necessários para criar uma impressão digital sem colaboração do seu proprietário são descritos em [Putte et al. 2000]:

- Obter um objecto, como por exemplo um copo, onde o proprietário tenha deixado a sua impressão digital.
- Espalhar delicadamente qualquer tipo de pó fino sobre a zona onde se encontra a impressão utilizando um pincel.
- Colar uma banda de fita cola (fina e transparente) sobre o pó e remove-la.
- Colar a fita-cola no lado fotossensível de um negativo fotográfico e fotografar uma fonte de luz difusa.
- Depois de revelado, o negativo é colocado sobre uma placa fotossensível (como as usadas nos circuitos impressos) e exposto a luz ultravioleta. Retira-se então o negativo.
- Utilizando um banho de gravura com água-forte, as partes da placa expostas à luz ultravioleta são removidas.
- Um último banho de água-forte cauteriza a camada de cobre resultando num perfil muito fino (cerca de 35μ) que é uma cópia "exacta" da impressão original.
- Após aprofundar as marcas de modo a assemelhar-se a uma impressão digital pode ser feito um carimbo de cimento de silicone à prova de água para substituir a impressão digital original.

Existem leitores que tentam ultrapassar o "efeito dedo morto" recorrendo a sensores de tensão arterial, condutividade, temperatura e leitura de padrões existentes em camadas inferiores à epiderme. No entanto, estas tecnologias são caras e ainda não atingiram o nível de maturidade desejado.

4.4 Leitura de Íris

Esta tecnologia envolve a análise do anel colorido que cerca a pupila do olho humano e é a menos intrusiva de todas, funcionando mesmo com óculos postos [Liu et al. 2001].

A leitura de íris possui padrões de comparação com eficácia acima da média e é uma das poucas tecnologias biométricas que pode ser adequada para identificação. No entanto, a dificuldade de utilização e integração com os sistemas existentes é um obstáculo à sua utilização [Liu et al. 2001].

O baixo custo de implementação é uma vantagem, já que uma câmara normal pode ser utilizada no processo. No entanto, a qualidade da imagem a utilizar no processo é uma questão importante a ter em conta [Thian 2001].

4.5 Leitura de retina

Os sistemas biométricos baseados na leitura de retina analisam a camada de vasos sanguíneos situada na parte de trás do olho, através da utilização de uma fonte de luz de baixa intensidade para opticamente reconhecer padrões únicos. Esta tecnologia pode atingir altos níveis de precisão, mas requer que o utilizador olhe para dentro de um receptáculo e foque um determinado ponto, o que não é conveniente para utilizadores que usem óculos ou que receiem o contacto próximo com o leitor [Liu et al. 2001].

O custo do equipamento necessário para a implementação desta tecnologia é, sem dúvida, um factor limitativo.

4.6 Reconhecimento de voz

Os processos de autenticação que recorrem ao reconhecimento da voz baseiam-se no facto de as características físicas de cada indivíduo proporcionarem à sua voz características únicas. No entanto, a informação capturável não possui informações suficientes para garantir o reconhecimento em larga escala de indivíduos [Jain et al. 2000].

Estes processos fundamentam-se nas técnicas de processamento de voz e na biometria e o envolvimento do utilizador pode passar pela introdução (oralmente) no sistema de uma palavra/frase chave ou pela leitura de um conjunto de caracteres que, combinados, fornecem um conjunto de características suficientes para permitir a autenticação ou a identificação do indivíduo. [Markowitz, 2000]

O potencial destes sistemas é grande devido ao baixo custo do hardware necessário que, aliás, está já presente em grande parte dos computadores existentes: um microfone. No entanto,

a sua aplicação está limitada, actualmente, a aplicações com um baixo nível de segurança, em virtude das grandes variações na voz de um indivíduo e na baixa precisão dos actuais sistemas de autenticação por reconhecimento de voz.

4.7 Keystrokes dynamics

A tecnologia denominada Keystrokes dynamics, também conhecida por dinâmica de digitação, é baseada na monitorização dos padrões comportamentais do utilizador ao digitar palavras/frases passe e/ou texto durante uma sessão. Regra geral, o sistema requer que o utilizador, na primeira utilização, digite a mesma frase um determinado número de vezes. Contudo, teoricamente um sistema pode na primeira utilização recolher a informação necessária para encontrar um padrão sem o conhecimento do utilizador.

É também possível ao sistema adaptar o modelo do padrão ao longo do tempo, de forma a ajustar-se à nova informação recolhida.

4.8 Assinatura manual recolhida de modo digital

A assinatura tem sido utilizada como um elemento de identificação largamente disseminado. É utilizada para comprometer indivíduos e organizações em contratos e para realizar pagamentos através de, por exemplo, cartões de crédito. A assinatura manual pode ser utilizada como uma biometria para autenticação/identificação desde que se possua um painel que capture a velocidade e a pressão dos movimentos que geram a assinatura, bem como a sua forma.

5- Níveis de precisão das tecnologias biométricas

Perceber os níveis de precisão das tecnologias biométricas é uma tarefa difícil, não só pela complexidade dos testes necessários para os conhecer, mas pela dificuldade de obter esses dados do universo de empresas fabricantes destes dispositivos de autenticação. No entanto, é de presumir que as empresas dispostas a fornecer esses dados e/ou sujeitar-se a teste governamentais, como é o caso do "Facial Recognition Vendor Test" do Counterdrug Technology Development Program Office do Departamento de Defesa dos Estados Unidos da América, serão aquelas que se encontram nos níveis mais avançados de precisão.

De modo a estruturar esta comparação, parece preferível analisar comparativamente produtos do mesmo tipo de tecnologia biométrica, seleccionar em cada grupo o(s) mais preciso(s) e, por fim, concluir da maturidade, em termos comparativos, das várias classes de tecnologias biométricas.

5.1 Reconhecimento facial

O *Counterdrug Technology development Program Office* do Departamento de Defesa dos Estados Unidos da América promoveu o *Facial Recognition Vendor Test 2002* num esforço internacional de colaboração com diversas entidades governamentais como, por exemplo, o FBI, o Canadian Passport Office, o Australian Customs e o United Kingdom Biometric Work Group. Participaram dez algoritmos neste teste de grupo.

Da informação disponibilizada, pode-se concluir que a autenticação/identificação com recurso a esta classe de tecnologias é mais precisa em indivíduos do sexo masculino do que em indivíduos do sexo feminino. Ainda assim, a maturidade actual destas tecnologias parece estar ao nível em que se encontravam em 1998 as tecnologias biométricas baseadas na impressão digital [Phillips, 2003].

Os valores exactos de FAR e FRR não se encontram disponíveis. No entanto, por observação dos gráficos, podemos obter valores aproximados. A tabela 1 sistematiza os melhores desempenhos.

FAR	FRR	
0,0001	0,725	**Masculino**
	0,71	**Feminino**
0,001	0,91	**Masculino**
	0,88	**Feminino**
0,01	0,91	**Masculino**
	0,89	**Feminino**
0,1	0,96	**Masculino**
	0,95	**Feminino**

Tabela 1- Fiabilidade do reconhecimento facial

5.2 Geometria da mão

São poucos os dados técnicos relativos a sistemas biométricos baseados na geometria da mão. No entanto, foi recentemente apresentado um sistema misto que divulgou os valores de FRR e FAR obtidos para o sistema de geometria da mão isoladamente. A FRR obtida foi de 8,34%, enquanto que a FAR foi de 5,29% [Kumar et al, 2003].

Estes valores mostram que, isoladamente, esta tecnologia está longe da maturidade. Quando combinada com outros factores inerentes à mão, como as linhas da palma, os valores melhoram consideravelmente, não pela precisão da representação mas por factores ligados aos algoritmos de decisão.

5.3 Impressão digital

O FVC2002 (Fingerprint Verification Competition) é um teste de grupo organizado pela Universidade de Bolonha, pela Universidade Estadual San Jose e pela Universidade Estadual do Michigan, que contou com a participação de trinta e um algoritmos, entre produtos académicos, industriais e anónimos [Maltoni et al, 2003]. Embora ainda só existam informações relativas ao relatório preliminar, é já possível tirar algumas conclusões da informação disponibilizada por [Maio et al, 2002] e [Maltoni et al, 2003].

Devido ao grande número de métricas utilizadas, que dificultam a percepção da precisão dos sistemas avaliados, é preferível ter em conta apenas as dez melhores taxas de intersecção de erros denominada, no relatório, por *Equal Error Rate*.

Produto	EER (%)
Bioscrypt Inc.	0,19
Anónimo	0,33
Anónimo	0,41
Bioscrypt Inc.	0,77
Siemens AG	0,92
Neurotechnologija Ltd.	0,99
SAGEM	1,18
Andrey Nikiforov (independente)	1,31
SAGEM	1,42
Deng Guoqiang (independente)	2,18

Tabela 2 - Fiabilidade do reconhecimento da impressão digital facial

É possível observar na tabela 2 que esta tecnologia tem já um grau de maturidade bastante elevado. No entanto, existem sistemas (mesmo comerciais) muito distantes dos valores desejados, com taxas de intersecção de erros superiores a 5%, isto é, taxas vinte e cinco vezes mais alta do que o produto melhor classificado.

Os leitores de impressão digital vêm, muitas vezes, incorporados em hardware de utilização comum como, por exemplo, o teclado. Torna-se então necessário conhecer o nível de precisão destes dispositivos. A única empresa que respondeu a esta questão indicou que a FAR é menor que 1% e a FRR é inferior a 2%.

5.4 Leitura de Íris

Esta tecnologia é considerada como uma das tecnologias biométricas mais precisas. [Wang 2003] apresenta um trabalho em que combina esta tecnologia com o reconhecimento facial e indica, entre outros, os valores de FRR e FAR para o reconhecimento da íris apresentados na tabela 3.

FAR	FRR
0	0,002
0,2	0,0014
0,6	0,0008

Tabela 3 - Fiabilidade do reconhecimento por leitura da íris

5.5 Leitura de retina

Os sistemas biométricos de leitura de retina actualmente implementados são soluções proprietárias desenvolvidas especificamente para as entidades que as utilizam. Assim, não existem no mercado soluções *pret-a-porter*. No entanto, as patentes norte-americanas número 5673097 e 6453057 apresentam soluções de alta portabilidade que poderão revolucionar este mercado. A *Retinal Technologies, LLC* anunciou recentemente que se prepara para colocar no mercado leitores de padrões de retina a um custo extremamente baixo e de alta precisão. Quando questionada quanto aos valores de FRR e FAR, a empresa apresentou um relatório técnico de onde se extraiu a tabela 4 que sistematiza os valores de FRR e FAR em função do valor definido de tolerância.

Tolerância (t)	**FAR**	**FRR**
0.37	2.38E-5	0.000271
0.41	3.38E-6	0.00081
0.44	4.17E-7	0.0022
0.48	4.48E-8	0.0055

Tabela 4 - Fiabilidade anunciada de um sistema leitor de retina

Estes valores representam um nível de precisão incomparável com qualquer outra tecnologia biométrica.

5.6 Biometrias comportamentais

São poucos os estudos publicados no que respeita à precisão das tecnologias biométricas de carácter comportamental, como a dinâmica de digitação ou a assinatura captada de modo digital. No que respeita à primeira, os poucos estudos conhecidos utilizam um conjunto de dados demasiado pequeno para serem significativos. Quanto à assinatura digital, a única informação fiável que pôde ser recolhida foi que, embora tenha uma precisão razoável, não é uma tecnologia adequada para identificação em larga escala [Jain 2000].

Assim sendo, a análise comparativa que se segue refere-se apenas a biometrias de carácter físico.

5.7 Análise comparativa (por classes) da precisão das tecnologias biométricas

De modo a facilitar a comparação, a tabela 5 sintetiza os valores encontrados para FRR e FAR das várias tecnologias. Para a impressão digital considerou-se o valor EER, por ser o único disponível.

FAR	Íris	Impressão digital	Face (M)	Face (F)	Retina	Geometria da mão
0	0,002					
4,48E-08					0,0055	
0,00000417					0,0022	
0,00000338					0,00081	
0,0000238					0,000271	
0,0001			0,725	0,71		
0,001			0,91	0,88		
0,01			0,91	0,89		
0,1			0,96	0,95		
0,19		0,19				
0,2	0,0014					
0,33		0,33				
0,41		0,41				
0,6	0,0008					
0,77		0,77				
0,92		0,92				
0,99		0,99				
5,29						8,34

Tabela 5 - FRR vs FAR das várias tecnologias estudadas

O gráfico 2 não considera os valores relativos à geometria da mão, porque estes são muitos desfasados de todos os outros e porque, assim, é mais legível a distribuição em causa.

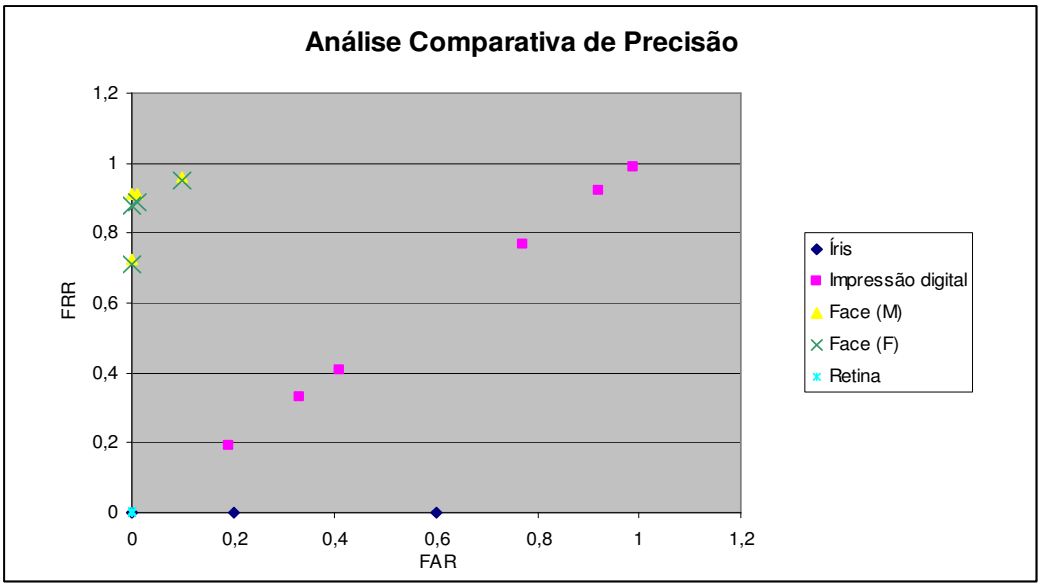

Gráfico 2 - FRR vs FAR das várias tecnologias estudadas

6- Impacto da autenticação biométrica nas organizações

No final do século passado, com a proliferação das tecnologias informáticas (nomeadamente o *PC*) e o avanço das tecnologias biométricas, tornou-se viável a implementação de autenticação por biometria no acesso a informação. No entanto, esta metodologia, além das dificuldades técnicas, acarretava algumas dificuldades de carácter social.

Países como a Austrália, Canadá, Estados Unidos e Nova Zelândia testemunharam uma inquietação pública quanto aos esquemas de identificação. Entre os vários receios citados incluem-se [Davies 1994] :

- Que as pessoas sejam desumanizadas ao serem reduzidas a códigos;
- Que o sistema potencie o poder sobre os indivíduos de determinadas organizações e do estado;
- Que a identificação de alta integração envolva a inversão da apropriada relação entre o cidadão e o estado;
- Que o sistema seja conduzido por uma burocracia tecnologicamente assistida, ao invés de por governos eleitos;
- Que isenções e excepções existam para organizações e indivíduos poderosos;
- Que estes esquemas de identificação sejam os mecanismos previstos em profecias religiosas como, por exemplo, a *Marca da Besta*;

Com a generalização de equipamentos leitores de características biométricas e com a sua divulgação em filmes de grande sucesso, o cidadão comum encara hoje a autenticação biométrica como algo que lhe é familiar, embora a associe em grande parte à ficção científica.

Por outro lado, o medo provocado pelo terrorismo, nomeadamente o atentado de 11 de Setembro de 2001 ao World Trade Center, leva o indivíduo a encarar qualquer tecnologia que aumente os níveis de segurança como uma contribuição para o seu bem-estar. Ainda assim, é preciso que a organização use de bom senso ao proteger a sua informação pois, como já foi referido, é necessário equilibrar o valor da informação a proteger, com o custo de implementação da solução que a irá proteger.

7- Autenticação com Smart Cards

De uma forma simples, podemos afirmar que qualquer técnica biométrica assenta na recolha de um conjunto de características próprias de um indivíduo, sendo a autenticação o resultado (positivo ou negativo) da comparação dessas características com um padrão

armazenado. Se a recolha deve ser um processo fiável, ao mesmo nível de exigência deve estar a segurança do armazenamento e da operação de comparação.

Os Smart Cards garantem hoje esse requisito de armazenamento e, com a capacidade de processamento actual, podem ainda efectuar a comparação de padrões, naturalmente com algumas limitações, mas dentro de um ambiente bastante seguro. A tecnologia Java Card, como uma das mais amadurecidas, permite explorar níveis de programação já bastante elevados e garante a portabilidade do processo entre Sistemas Operativos.

Do ponto de vista de sistema existe uma limitação imposta pela separação física entre o subsistema biométrico e o subsistema de suporte ao Smart Card que, habitualmente, se encontram interligados através de um computador pessoal. Esta arquitectura introduz algumas vulnerabilidades na comunicação, que poderão ser ultrapassadas recorrendo a técnicas de encriptação. Contudo, numa evolução previsível, é natural que os leitores biométricos venham a incorporar leitores de Smart Cards, conferindo ao conjunto interessantes capacidades de identificação e autenticação.

Numa política de segurança global, será ainda interessante garantir a integração da função do identificador/autenticador com outros eventuais serviços de segurança existentes num sistema de informação. Esta integração poderá ser feita eficientemente utilizando o protocolo LDAP (Lightweight Directory Access Protocol), bastante utilizado para acesso a repositórios de informação estruturada, como é o caso dos servidores de certificados nas infra-estruturas de chave pública, ou do próprio *registry* que o Windows implementa. Este protocolo, que pode ser seguro quando associado à criptografia, permite interoperabilidade entre sistemas operativos diferentes permitindo, por exemplo, uma autenticação única para Windows e Linux [Swanson et al. 2002]**.** Estes repositórios aparecem então com elo de ligação entre subsistemas independentes de identificação/autenticação e serviços de segurança que exigem essa função.

Matryoshka é uma arquitectura em desenvolvimento pelos autores e que procura explorar esta linha de desenvolvimento. Do ponto de vista da tecnologia exige a criação de uma camada de interface no Smart Card (já concluída), do ponto de vista da biometria exige a investigação de técnicas biométricas adequadas a um determinado nível de segurança e dentro das capacidades de processamento disponíveis. Tal como foi demonstrado, apesar do domínio das soluções ser alargado, as restrições impostas pela limitada capacidade de processamento dos Smart Card e por eventuais políticas de segurança, podem inviabilizar uma solução, obrigando à investigação de algoritmos optimizados e/ou técnicas biométricas alternativas.

8- Conclusões

Existem hoje algumas tecnologias biométricas com um grau de maturidade que permite considerá-las como uma ferramenta de autenticação indispensável quando utilizados em conjunto com os Smart Cards que, potenciados pela tecnologia Java materializada na plataforma Java Card, representam uma forma portátil, segura e resistente de amplificar as funções de autenticação existentes, nomeadamente as de carácter biométrico. Contudo, a conjugação de ambas as tecnologias implica compromissos importantes com naturais reflexos ao nível dos algoritmos a utilizar, o que justifica a investigação em curso.

9- Bibliografia

Chen, Z., *Java Card Technology for Smart Cards*, Addison Wesley, U.S.A., 2000

Davies, S.: *Touching Big Brother – How biometric technology will fuse flesh and machine*, Information Technology & People, Vol 7, No. 4, 1994.

Jain, A., Hong, L e Pankanti, S.: *Biometric Identification*, Comunications of the ACM, Vol. 43, No. 2, 2000.

Kumar, A., Wong, D. C. M., Shen, H. C. e Jain, A. K., *Personal Verification using Palmprint and Hand Geometry Biometric*, Proc. of 4th Int'l Conf. on Audio- and Video-Based Biometric Person Authentication (AVBPA), Guildford, UK, 2003.

Liu, S. e Silverman, M.: *A Practical Guide to Biometric Security Technology*, IEEE Computer Society, www.computer.org/itpro/homepage/Jan_Feb/security3.htm (Dezembro de 2002), 2001.

Maio, D., Maltoni, D., Cappelli, R., Wayman, J.L. e Jain, A. K.: *FVC2002: Second Fingerprint Verification Competition*, Proceedings of the International Conference on Pattern Recognition – ICPR2002, 2002

Maltoni, D.Maio, D., Jain, A. K. e Prabhakar, S.: *Handbook of fingerprint recognition*, Springer, New York, 2003.

Markowitz, J.: *Voice Biometrics*, Comunications of the ACM, Vol. 43, No. 9, 2000.

Phillips, P. J., Grother, P., Micheals, R. J., Blackburn, D. M., Tabassi, M. e Bone, M.: *Face Recognition Vendor Test 2002: Evaluation Report*, www.frvt.org , (Abril 2003), 2003

Putte, T. e Keuning, J.: *Biometrical fingerprint recognition: don´t get your fingers burned*, Proceedings of IFIP TC8/WG8.8 Forth Working Conference on Smart Card Research and Advanced Applications, Kluwer Academic Publishers (2000), 289-303.

Poh, N. e Korczak, J.: *Hybrid Biometric Person Authentication Using Face and Voice Features*, Proceedings of the Third International Conference, Audio- and Video--based Biometric Person Authentication AVBPA 2001, Halmstad, Sweden, 2001, 348-353.

Swanson, C. E Lung, M.: *OpenLDAP everywhere*, Linux Journal, Vol. 2002, No. 104, 2002.

Thian, N.: "Biometric Authentication System", Tese de mestrado, USM, Penang, Malásia, http://hydria.u-strasbg.fr/~norman/BAS/publications.htm (Fevereiro 2003), 2001.

Wang, Y., Tan, T. e Jain, A. K., *Combining Face and Iris Biometrics for Identity Verification,* Proc. of 4th Int'l Conf. on Audio- and Video-Based Biometric Person Authentication (AVBPA), Guildford, UK, 2003.