BIOMETRIA E E-LEARNING:
UM CASO DE USO DO MOODLE COM *KEYSTROKE*

Aracaju – SE – maio de 2012

M. Sc. Mário Vasconcelos Andrade – TECNED – Tecnologias Educacionais – mario@tecned.com.br

M. Sc. Rodolfo Botto de Barros Garcia – SIA – Software com Inteligência Artificial – rodolfo@sia.eti.br

João Paulo de Mendonça Barroso – SIA – Software com Inteligência Artificial – jp@sia.eti.br

Lucas Luan Bomfim Menezes – SIA – Software com Inteligência Artificial – lucas@sia.eti.br

Dr. Jugurta Montalvão - Universidade Federal de Sergipe – jmontalvao@ufs.br

Categoria: C - Métodos e Tecnologias

Setor Educacional: 5 - Educação Continuada em Geral

Classificação das Áreas de Pesquisa em EaD
Macro: C. Sistemas e Instituições de EAD / Meso: H. Tecnologia Educacional / Micro: N. Interação e Comunicação em Comunidades de Aprendizagem

Natureza do Trabalho: B - Descrição de Projeto em Andamento

Classe: 2 - Experiência Inovadora

RESUMO

Este trabalho apresenta uma experiência inovadora quanto à autenticação de usuários em sistemas de educação a distância via Internet (*e-learning*). Foram aplicadas tecnologias de baixo custo e de fácil utilização, assim viabilizando o acesso de um grande número de usuários ao produto deste trabalho. O artigo

apresenta o problema da autenticação, faz uma breve conceituação da biometria por *Typing Dynamics,* apresenta a solução proposta de integração com o *Moodle* e relata os resultados até agora encontrados.

Palavras chave: biometria; segurança; autenticação; *typing dynamics*; *keystroke*.

1 - Introdução

Apesar do uso crescente do e-learning, alguns problemas ainda não têm solução clara, especialmente quando as avaliações são realizadas *online*. Este é um problema de autenticação que se manifesta desde o primeiro ingresso do aluno no ambiente virtual, ou seja, tipicamente, não se sabe como comprovar, remotamente, que a pessoa que está matriculada é realmente aquela que fez o *login* no sistema e que o está efetivamente utilizando. Algumas soluções já foram propostas e vão desde a realização de avaliações presenciais até a utilização de soluções biométricas, como é o caso do leitor de impressões digitais, porém essas soluções implicam a utilização, por parte do usuário, de um equipamento especial para leitura biométrica, que na maioria das vezes não está acessível ao aluno. Neste artigo, apresentaremos uma solução que independe de equipamentos especiais ou de procedimentos pouco comuns aos alunos. Utilizaremos apenas teclado e a digitação para autenticar os alunos em um ambiente de *e-learning* utilizando o *Moodle*.

2 – Typing Dynamics (ou *Keystroke*)

O *keystroke* (jargão de biometria computacional) é uma modalidade da biometria comportamental, através da qual um indivíduo pode ser identificado (identificação), ou ter sua identidade verificada (verificação) pelo seu padrão rítmico de utilização de um teclado.

Embora ainda pouco conhecida, a biometria via ritmo de digitação vem se firmando gradualmente como uma solução de segurança comparável àquelas que já ocuparam lugar na indústria e junto ao público em geral. De acordo com o texto publicado por Prof. Anil K. Jain[1], responsável pelo Biometrics Research Group[2], o reconhecimento pelo ritmo de digitação é, em média, melhor que o reconhecimento facial ou reconhecimento por voz, ficando

apenas um pouco atrás da biometria pelo reconhecimento de impressões digitais, em termos de taxas de erros.

Esta modalidade biométrica, embora não possa ser classificada entre as mais precisas, é muito conveniente em aplicações envolvendo sistemas *via* Internet, como o *e-learning*, pois grande parte da comunicação na rede é feita por meio do teclado. Além disso, esta modalidade biométrica, ao contrário de outras mais populares como as baseadas em impressões digitais ou reconhecimento de íris, não exige o uso de nenhum dispositivo (*hardware*) particular.

O reconhecimento de indivíduos pela maneira como esses digitam num teclado comum (de computador) é ainda mal compreendido pelo público em geral. Não é raro que um programa que usa o *Keystroke* desperte questões/comentários como:

"como pode funcionar sem um sensor biométrico? Só usa o teclado mesmo?"

"o teclado tem que ser especial?"

"e se eu mudar de teclado ou computador?"

Todas essas questões são pertinentes, e já foram respondidas (estatisticamente) através de modelos de probabilidade e, não menos importante, do uso e ajuste fino de protótipos ao longo de anos de pesquisa sobre a "biometria do comportamento", mais especificamente o "*typing dynamics*".

De fato, embora desconhecida do grande público, o estudo do *keystroke* teve início há décadas. Um dos pioneiros foi o trabalho de R. Gaines, S. Press, W. Lisowski e N. Shapiro, "Authentication by keystroke timing: some preliminary results"[3]. Relatório técnico da Rand Corporation, publicado em 1980. Nele os autores mostraram que *keystroke typing* pode caracterizar um indivíduo tanto quanto uma assinatura manuscrita (assinatura em cheque, por exemplo). Nesse trabalho pioneiro, os experimentos foram feitos com apenas sete secretárias, que escreveram, cada uma, três páginas de texto.

Desde então, muito se progrediu, em particular, na quantidade de texto necessária à verificação da identidade, pois poucas pessoas estariam dispostas a digitar três páginas de texto para uma única autenticação. Atualmente bastam poucas palavras para que os sistemas identifiquem os usuários.

No Brasil, o *BioStroke* (software que utilizamos neste experimento) é o primeiro sistema de verificação biométrica comercial baseado em *keystroke*. Ele foi desenvolvido numa parceria entre universidade/empresa, partindo de um protótipo inicial, em 2005[4], testado e ajustado originalmente com estudantes e professores da universidade, esse protótipo ganhou formato e robustez suficiente para se tornar, alguns anos depois, um produto comercial. Hoje, suas funcionalidades podem ser livremente testadas através da internet, no site www.biostroke.com.br.

2.1 - Mas como funciona e qual a precisão?

Enquanto um usuário digita num teclado comum, os intervalos de tempos entre-tecladas são registrado localmente pelo computador. A essa sequência de intervalos de tempos chamamos de *''Assinatura Rítmica do Usuário''*. Isso porque tem sido demonstrada de forma consistente, desde a década de 80, que, com exceção dos iniciantes no uso dos teclados, cada pessoa desenvolve uma característica pessoal no ritmo de digitação, análoga à caligrafia.

Esses tempos, ou essa *"Assinatura Rítmica"* é então codificada e criptografada, antes de ser enviada ao módulo (remoto ou local, mas tipicamente remoto) responsável pela verificação dessa "caligrafia" rítmica.

Em todo sistema biométrico, dois tipos de erros são mais importantes:

- **Alarme falso (FAR)**: quando um usuário com assinatura cadastrada não é reconhecido pelo sistema.
- **Falsa Aceitação (FRR)**: quando um intruso (falsário) se faz passar por um usuário cadastrado e é aceito, erradamente, pelo sistema.

Ainda no estudo apresentado por Prof. Anil K. Jain[1], realizado com 63 usuários, com assinaturas rítmicas coletadas ao longo de 11 meses, apenas com textos fixos (como nomes próprios), em diversos teclados, essas duas taxas ficaram abaixo de 3% (isto é, menos de 3 erros a cada 100 tentativas), o que é um resultado bem melhor que o da biometria baseada em reconhecimento facial.

Por outro lado, o *BioStroke*, desde seus primeiros protótipos, datados a partir de 2005, tem sido fundamentado num método original, parcialmente publicado em 2006, em que consegue melhorar os resultados obtidos por métodos tradicionais [4].

Em testes realizados com o *BioStroke*, induzindo ao treinamento de falsificadores, o que corresponde ao pior caso, obtivemos uma média de 4 erros (seja FRR ou FAR) em cada 100 tentativas, usando apenas 3 repetições da digitação do nome completo do usuário.

Apesar de o sistema permitir a verificação de identidade através de textos livres, como o texto de um *e-mail* pessoal, ou de uma resposta subjetiva a uma questão de prova, esse não foi o objetivo deste trabalho. Portanto, os testes foram feitos apenas na autenticação do usuário no momento da entrada no sistema. Mais recentemente, uma base com dezenas de digitações de nomes próprios (digitações genuínas) e respectivas tentativas de falsificações minuciosamente treinadas (*skilled forgeries*) foi gerada e novos testes foram realizados com o *BioStroke*, fornecendo taxas de FRR e FAR aproximadas entre 4% e 5%. Além disso, há resultados novos relacionados ao método de equalização de tempos, o mesmo usado como parte importante do *BioStroke*, que serão apresentados no CBA2012 [5].

3 – A biometria no Moodle

Para os testes da biometria em sistemas de *e-learning,* utilizamos o Ambiente Virtual de Aprendizagem – AVA - *Moodle* (www.*moodle.org)*. A escolha do *Moodle* se deu pelo fato de ser uma aplicação *web* de código aberto, com vasta utilização no meio acadêmico o que facilitou a integração com a solução biométrica.

Para instalar a solução biométrica *Biostroke* no *Moodle* foi modificado o módulo de autenticação padrão para que, além do login e senha, o sistema solicitasse também a digitação de uma assinatura biométrica (figura 1). A integração e comunicação entre as aplicações foram feitas utilizando um “*Web Service*”, assim foi possível fazer com que as duas aplicações tivessem instalações, banco de dados e ambientes diferentes, aumentando a segurança da solução proposta e facilitando a integração.

Figura 1. Tela de *login* do *Moodle* com a inclusão do campo de biometria

Dessa forma, todos os usuários, quando foram cadastrados, tiveram que cadastrar também a suas assinaturas biométricas (figuras 2 e 3). Conforme já mencionado, para o cadastro biométrico, foram solicitadas três assinaturas, porém para o *login* apenas uma assinatura é solicitada (campo Chave Bio da figura 1).

Figura 2. Cadastro das assinaturas biométricas do usuário.

Figura 3. Tela de cadastro efetuado com sucesso.

4 – Resultados e Comentários finais

Nos testes realizados houve uma perfeita integração entre o *Moodle* e o *Biostroke*, não identificamos nenhum problema de performance ou compatibilidade. Nos testes de massa, foram acionados dois grupos de voluntários, a saber: o **grupo A** tinha por tarefa usar o *BioStroke* naturalmente, se cadastrando e consultando o sistema durante dias., e o **grupo B,** que tinha por tarefa observar indivíduos do **grupo A** usando o sistema, estudar sua forma de digitar (olhando para o teclado e escutando os sons – ritmo – produzidos pelas teclas) e tentar burlar o sistema, falsificando as assinaturas do **grupo A**. Este tipo de falsificação é considerada a mais arriscada, pois o potencial falsificador é treinado. Os membros dos **grupos A e B** se intercambiaram, de forma que todos conheciam bem o funcionamento do sistema.

O resultado de desempenho do *BioStroke* obtido nesse caso extremo pode ser sumarizado como segue:

Os erros de falsa aceitação de falsificadores treinados ou falsa rejeição de usuários cadastrados foram aproximadamente iguais, ambos menores que 4 em cada 100 tentativas (pior caso, com falsificadores treinados).

O *BioStroke* é um sistema biométrico e, como tal, deve tolerar erros de verificação, da mesma forma que há falhas de autenticação via rubricas, em cheques bancários tradicionais, por exemplo.

Para o *e-learning* identificamos que este tipo de aplicação poderá se beneficiar com o uso da biometria por *keystroke* através de:

- Maior segurança em sistemas informatizados que necessitem de autenticação, sejam eles AVA, Sistemas de Matrícula e Pagamento ou sistemas de avaliação;
- Redução do número de invasões de sistemas por conta de falhas de segurança, especialmente aquelas ligadas ao roubo ou perda de senhas. No *e-learning* isso significa redução de compartilhamento de senhas e consequente redução de perdas financeiras, aumento da confiabilidade por parte dos usuários e aumento nas possibilidades de avaliação de aprendizagem;

- Por se tratar de uma tecnologia que não necessita de equipamentos especiais, muitas vezes caros e que demandam manutenções/ajustes periódicos, essa tecnologia permite que mais pessoas tenham acesso a serviços mais seguros e confiáveis.

Referências

[1] A. K. Jain. “Biometric Authentication based on Keystroke Dynamics”. Disponível em http://www.cse.msu.edu/cse891/Sect601/KeystrokeRcg.pdf (data de acesso: 16/07/2012).

[2] WebSite do Biometrics Research Group, disponível em http://biometrics.cse.msu.edu (data de acesso: 16/07/2012).

[3] R. Gaines, “Authentication by keystroke timing: some preliminary results.” / R. Stockton Gaines ... [et al.] Rand, Santa Monica, CA, 1980.

[4] J. Montalvão, E. O. Freire. “On the equalization of keystroke timing histograms.” Pattern Recogn. Lett. 27, 13, pp. 1440-1446. Outubro 2006.

[5] M. A. Bezerra Junior, J. Montalvão, E. O.Freire. "Equalização de intervalos adaptada à dinâmica da digitação (Keystroke) de senhas curtas", aceito para publicação nos anais do XIX Congresso Brasileiro de Automática, 2012.