DETECÇÃO DE INTRUSÕES BASEADA EM USER PROFILING E REDES NEURAIS

Paulo Henrique Pisani[1], Silvio do Lago Pereira[2]
[1]Aluno do curso de Especialização em Análise e Projetos de Sistemas da FATEC-SP
[2]Prof. Dr. do Curso Tecnologia da Informação da FATEC-SP
paulohpisani@yahoo.com.br, slago@ime.usp.br

Resumo

Na era atual, as pessoas possuem um ativo chamado *identidade*. Identidades são usadas para autenticação em diversos contextos envolvendo sistemas informatizados, desde acesso a sistemas de suporte ao trabalho até a contas bancárias e comunidades de relacionamento. Há diversos métodos de autenticação de identidade; contudo, em geral, após uma autenticação inicial, um intruso está livre para acessar e usar o sistema assim como um usuário legítimo o faria. Neste trabalho, mostramos como evitar fraudes de identidade usando um método de detecção de intrusões baseado em *user profiling* e redes neurais que, analisando o comportamento do usuário, permite a constante autenticação de sua identidade.

1. Introdução

Identidade pode ser definida como um conjunto de características e circunstâncias que distinguem uma pessoa [1]. Identidades são usadas para autenticação em diversos contextos envolvendo sistemas informatizados [2], desde acesso a sistemas de suporte ao trabalho até a contas bancárias e comunidades de relacionamento.

Contudo, em geral, após a autenticação inicial, um intruso está livre para acessar e usar o sistema assim como um usuário legítimo o faria [3]. Conforme as pesquisas mostram [4], mesmo com o uso de mecanismos de autenticação inicial, a cada ano, mais de 10 milhões de pessoas são afetadas pela fraude de identidade. Isso indica que uma forma mais efetiva de evitar fraudes de identidade requer a constante autenticação do usuário.

Neste artigo, mostramos como *user profiling* [5] e redes neurais [6] podem ser usados, de forma integrada, para o desenvolvimento de um sistema de detecção de intrusões [7] que monitora continuamente o comportamento do usuário e sinaliza qualquer desvio de seu comportamento padrão como uma possível intrusão.

O restante desse artigo está organizado do seguinte modo: na Seção 2, introduzimos os fundamentos de *user profiling* e redes neurais; na Seção 3, descrevemos o sistema desenvolvido; na Seção 4, discutimos os resultados dos experimentos realizados com esse sistema; e, finalmente, na Seção 5, apresentamos nossas conclusões.

2. Fundamentos

A evolução dos sistemas informatizados e dos mecanismos de comunicação levou ao surgimento da chamada *identidade digital* e também de uma maior exposição dos dados pessoais, o que contribuiu para o crescimento de um crime conhecido como *roubo de identidades* [8].

O uso do termo "roubo de identidades" é na verdade um equívoco, pois a identidade de uma pessoa é algo que não pode ser roubado. De qualquer forma, este termo é comumente usado para referir-se ao crime de utilizar as informações pessoais de uma pessoa fazendo passar-se ilegalmente por esta.

Atualmente, utilizamos credenciais para comprovar identidades e assim ter acesso a locais físicos, sistemas informatizados e outros serviços. Como exemplos destas credenciais podemos citar o RG e o usuário e senha para acesso ao e-mail.

A autenticação de identidades em sistemas informatizados pode ser feita por meio de diversos métodos [9]:

- o que o usuário *sabe* (e.g. senha);
- o que o usuário *possui* (e.g. cartão); ou
- o que o usuário *é* (e.g. biometria);

sendo este último considerado o mais robusto ou, equivalentemente, o menos sujeito a fraudes.

2.1. User Profiling

A partir do monitoramento do usuário e da observação de suas características comportamentais é possível gerar modelos que representem o comportamento normal deste usuário. O processo de geração destes modelos para a criação do *perfil* de um usuário é denominado *perfilamento de usuário* (*user profiling*) [5].

Um perfil pode ser:

- *estático*, neste caso, após a sua definição, ele não é mais alterado, a menos que seja recriado; ou
- *dinâmico*, neste caso, ele adapta-se automaticamente ao longo do tempo.

Perfis estáticos podem se tornar imprecisos ao longo do tempo e, por isso, necessitam ser renovados periodicamente. Perfis dinâmicos, em contrapartida, pelo fato de adaptarem-se a pequenas alterações ao longo do tempo, não necessitam ser renovados.

A partir do perfil representando o comportamento normal do usuário, gerado no *período de treinamento*, um sistema de detecção de intrusão (*Intrusion Detection System* – IDS) pode detectar anomalias de comportamento [10]. Para tanto, o IDS efetua uma comparação entre o perfil e os eventos observados, indicando aquilo que desvia do perfil como uma possível fraude.

A maior vantagem dos IDSs baseados em detecção de anomalias é fato de eles serem bastante efetivos na detecção de ameaças ainda não conhecidas [10].

2.2. Dinâmica da Digitação

Uma das características comportamentais que podem ser monitoradas é a dinâmica da digitação, cuja análise permite reconhecer usuários pelo seu ritmo de digitação. Pesquisas em dinâmica da digitação focam atributos tais como tempos entre o pressionamento de teclas e tempos de pressionamento de teclas. Outra característica bastante informativa é a pressão exercida nas teclas durante a digitação, entretanto, a monitoração dessa característica necessita de *hardware* especializado e, por esse motivo, não é muito usada em aplicações práticas [11]. A dinâmica de digitação no contexto de segurança é considerada um tipo de *biometria comportamental* [11].

Normalmente, o desempenho de sistemas biométricos é avaliado em relação às seguintes taxas [11]:

- Taxa de Falsa Aceitação (*False Acceptance Rate* - FAR), que mede quanto um sistema biométrico reconhece um conjunto de características falsas como verdadeiras. Em segurança, isso equivale a reconhecer um intruso como um usuário legítimo.
- Taxa de Falsa Rejeição (*False Rejection Rate* - FRR), que mede quanto um sistema biométrico reconhece um conjunto de características verdadeiras como falsas. Em segurança, isso equivale a reconhecer um usuário legítimo como intruso.

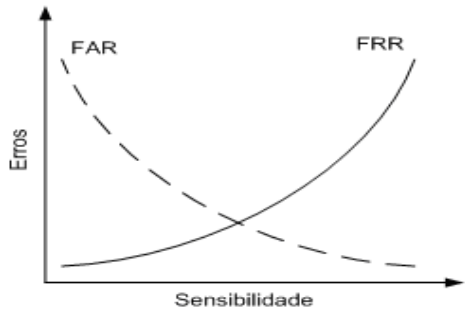

Figura 1 – Taxas FAR e FRR

Como regra geral, a diminuição do valor de qualquer uma das duas taxas gera um aumento na outra. O gráfico da figura 1 mostra uma relação hipotética entre as taxas FAR e FRR. O ajuste de sensibilidade é um dos fatores que influencia na alteração do valor das taxas. Quanto menores os valores destas taxas, maior a precisão do sistema biométrico.

2.3. Redes Neurais Artificiais

Uma ferramenta bastante poderosa para a tarefa de reconhecimento de padrões são as *redes neurais artificiais* (RNAs) [6]. Redes neurais artificiais são comuns em aplicações de Inteligência Artificial (IA), cujo objetivo é desenvolver sistemas computacionais que simulem comportamento inteligente, tais como aprendizado, percepção, raciocínio e adaptação [12].

RNAs, que têm como inspiração as redes neurais biológicas, possuem a capacidade de operar com dados incompletos e com ruídos, oferecendo assim grande robustez no reconhecimento de padrões [6].

Para melhor compreensão das redes neurais artificiais, apresentamos na figura 2 (adaptado de [13]) um neurônio biológico, que pode ser dividido, basicamente, em três partes:

- *dendritos*, que recebem impulsos de entrada;
- *soma*, que processa os impulsos de entrada;
- *axônio*, que envia um impulso de saída (podendo possuir ramificações em sua extremidade).

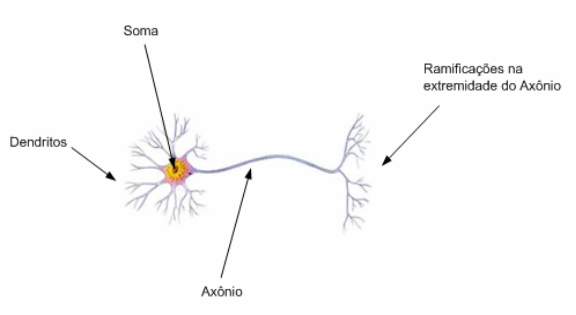

Figura 2 – Partes de um neurônio biológico

Inspirados no neurônio biológico, *McCulloch* e *Pitts* desenvolveram um modelo matemático de um neurônio artificial conhecido como neurônio MCP [14].

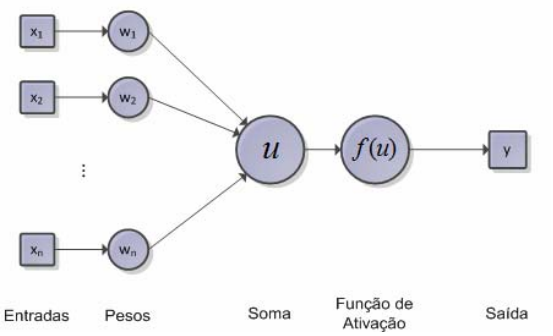

Figura 3 – Neurônio Artificial (MCP)

O neurônio MCP possui as seguintes partes:

- *entradas*: valores de entrada;
- *pesos*: valores que representam o nível de influência de cada valor de entrada no neurônio;
- *soma*: é o resultado da soma ponderada dos valores de entrada com os respectivos pesos;

$$u = \sum_{i=1}^{n} w_i \cdot x_i \qquad (1)$$

- *função de ativação*: a função de ativação é uma função matemática que recebe o valor da soma como entrada;
- *saída*: resultado da função de ativação.

Com a evolução dos estudos das redes neurais, verificou-se que um neurônio isoladamente possui capacidade limitada, mas um agrupamento de neurônios pode solucionar problemas bastante complexos. Os neu-

rônios são ligados uns aos outros através de sinapses. A sinapse ocorre com a conexão do axônio de um neurônio ao dendrito de outro. As diversas sinapses que ocorrem entre os neurônios formam as redes neurais.

Um dos primeiros modelos de RNAs desenvolvido foi o *perceptron simples*. O *perceptron simples* possui restrições com relação aos problemas que pode solucionar. Com o passar do tempo, foi criado o *perceptron multicamada* que cobriu as restrições verificadas no *perceptron simples*. Além do *perceptron*, outros modelos de redes foram desenvolvidos como os Mapas Auto-organizáveis, *Cognitron* e *Neognitron*, entre outros [6].

O aprendizado das redes neurais artificiais ocorre por meio do ajuste de seus pesos w_1, ..., w_n (inicialmente aleatórios) por um mecanismo denominado *treinamento* [6]. O treinamento consiste em apresentar um conjunto de dados para a RNA de modo que esta se adapte a estes. O conjunto dos valores dos pesos após o treinamento é chamado de *conhecimento* adquirido pela rede neural.

Uma RNA passa por duas fases:

- *treinamento*: quando adquire conhecimento; e
- *operação*: quando utiliza o conhecimento adquirido para gerar as saídas.

Alguns pontos comuns entre as RNAs e as redes neurais biológicas são:

- processamento paralelo e distribuído;
- comunicação entre as unidades de processamento por meio de conexões sinápticas;
- capacidade de generalização;
- redundância.

Neste trabalho, focamos no *multilayer perceptron*, ou MLP, que é formado por camadas intermediárias de neurônios com funções de ativação sigmóide. Uma rede MLP com uma camada intermediária tem a capacidade de aproximar qualquer função contínua [15] e com duas camadas intermediárias pode aproximar qualquer função [16].

3. Aplicação

Utilizando redes neurais artificiais, desenvolvemos um sistema simples para detecção de intrusões (IDS) baseado em *user profiling* [7]. As RNAs foram usadas para identificar desvios no comportamento dos usuários.

Para a definição do comportamento do usuário, bem como para a detecção de desvios, escolhemos características relativas ao seu ritmo de digitação.

Uma das aplicações da dinâmica da digitação é na verificação contínua de palavras-chave específicas. Utilizamos este conceito para monitorar uma lista de comandos cadastrados. A proposta do sistema é de que sejam cadastrados comandos considerados sensíveis. Citamos a seguir alguns exemplos para o caso do *Microsoft Windows*. Além destes, poderia ser cadastrado também o valor de algum *login* utilizado na máquina.

- `regedit`: permite acesso ao editor do registro do sistema operacional;
- `command`: permite acesso ao *prompt* de comando;
- `control`: permite executar comandos do sistema operacional.

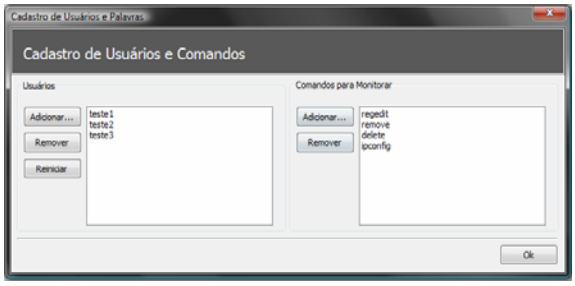

Figura 4 – Cadastro de usuários e comandos

A tela de cadastro de comandos sensíveis à monitoração é apresentada na figura 4. Após o cadastramento, o sistema monitora os comandos cadastrados para detectar um padrão de uso, permitindo detectar anomalias no comportamento que podem ser classificadas como possíveis intrusões. Pelo fato de capturar dados de uma estação de trabalho ou computador específico, este sistema é classificado como um *host-based* IDS [10] no item monitoração e, por ser baseado na detecção de anomalias a partir de *profiles* armazenados, a detecção é do tipo *anomaly-based detection* [10].

A extração de características de uma palavra gera um vetor que intercala valores de duas informações de acordo com a figura 5:

Figura 5 – Vetor de características

Em que:

- n, TA e TB são calculados de acordo com as equações (2), (3) e (4).

$$n = (quantidades\ de\ caracteres) - 1 \quad (2)$$

$$TA_i = P_{(i+1)} - P_i \quad (3)$$

$$TB_i = P_{(i+1)} - S_i \quad (4)$$

- P_i e S_i representam os instantes em que uma tecla é pressionada e solta, respectivamente, e i é o índice da tecla, conforme ilustrado na figura 6.

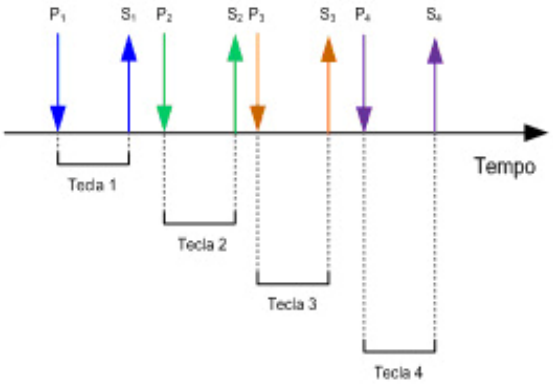

Figura 6 – Exemplo de captura da digitação

O vetor de características final é resultado da transformação dos valores de TA e TB para a faixa [-1; +1], conforme ilustrado na figura 7, através do uso da seguinte regra: calculamos TAT e TBT de acordo com as equações (5) e (6). Caso o valor obtido para TAT ou TBT seja maior que 1, consideramos este como 1 e, caso seja menor que -1, como -1.

O valor de TD é um fator de sensibilidade que é ajustado de acordo com o público aplicado. Usamos o valor 300 em nossos testes.

$$TAT_i = \left(\frac{TA_i}{TD}\right) * 2 - 1 \quad (5)$$

$$TBT_i = \left(\frac{TB_i}{TD}\right) * 2 - 1 \quad (6)$$

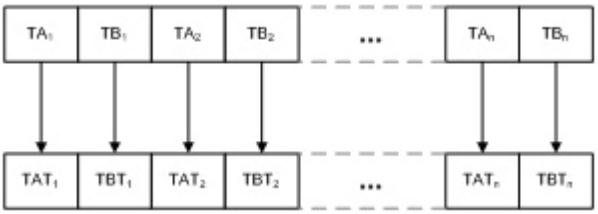

Figura 7 – Vetor de características processado

O vetor de características final, resultante do processo descrito acima, é utilizado como entrada para a rede neural que, neste caso, serve como ferramenta para o reconhecimento de padrões. Escolhemos o *perceptron multicamada* (MLP) por ser bastante efetivo nesta tarefa e pelo fato de já ter sido utilizado em outros trabalhos relacionado à dinâmica da digitação [11].

O MLP utilizado varia o número de entradas de acordo com o comando, pois, conforme definido anteriormente, o número de itens no vetor de características é função do número de caracteres do comando. Devido a isso, foi necessário criar dinamicamente uma rede para cada palavra. O modelo destas redes é apresentado na figura 8. Cada rede MLP criada possui 6 neurônios na camada intermediária e 1 neurônio na camada de saída. Usamos 5000 épocas no treinamento com taxa de aprendizado 0,75 e valor α do termo *momentum* igual a 0,1.

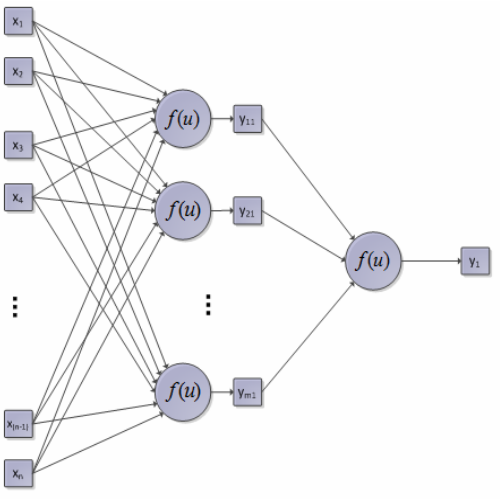

Figura 8 – Modelo do MLP utilizado

A tela principal do sistema desenvolvido (disponível em *http://br.geocities.com/php_rna/default.htm*) é apresentada na figura 9.

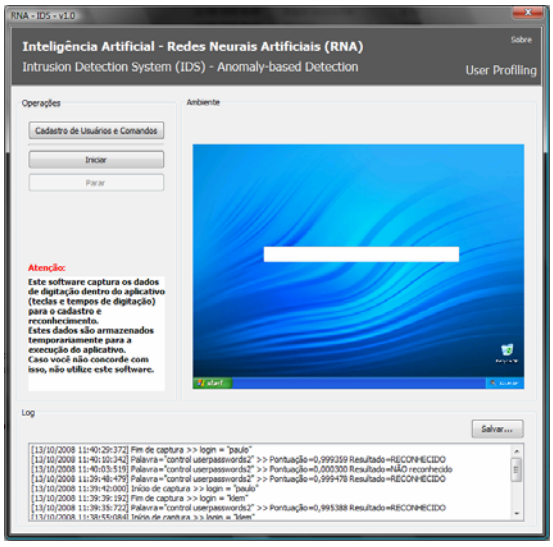

Figura 9 – Tela principal do aplicativo

4. Resultados

Os testes iniciais foram realizados com 12 pessoas e obtivemos taxas de falsa aceitação (FAR) de 22,5% e de falsa rejeição (FRR) de 23,5%, em média, sendo que para comandos com maior quantidade de caracteres estas taxas foram de 10% e 15%, respectivamente. Os comandos maiores permitiram melhores resultados pelo fato de oferecerem mais informações sobre o ritmo de digitação do usuário, o que melhorou o desempenho da rede neural na diferenciação.

5. Conclusões

Com aumento significativo da exposição de dados e do uso de identidades, bem como das fraudes relacionadas ao mau uso destas, mecanismos de segurança adicionais ao uso de senhas passaram a ser fundamentais. Um destes mecanismos é o *user profiling* [5]. De fato, conforme observamos com os testes realizados, *user profiling* baseado em redes neurais artificiais é um mecanismo bastante efetivo e robusto para o reconhecimento de fraudes de identidade.

Porém, uma aplicação de *user profiling* mais completa necessita de um conjunto maior de características para atingir resultados mais precisos. Algumas dessas características poderiam ser a velocidade de movimentação do cursor, os tempos de clique do *mouse*, a quantidade de cliques, programas usados e consumo de tempo de CPU e memória. Tais características adicionais são objetos de estudo para trabalhos futuros.

Referências Bibliográficas

[1] Houaiss, Instituto Antônio, **Dicionário Eletrônico Houaiss da Língua Portuguesa**. Editora Objetiva, 2004.

[2] **Taking control of your digital ID**, BBC News, 1 nov. 2006.

[3] D. J. Marchette, **Computer Intrusion Detection and Network Monitoring**, Springer, 2001.

[4] **Identity Theft Focus of National Consumer Protection**, Week 2005. Federal Trade Commission, Fev. 2005.

[5] T. Goldring, **User Profiling for Intrusion Detection in Windows NT**, In Proc. of the 35th Symposium on the Interface, 2003.

[6] A. P. Braga et. al. Redes Neurais Artificiais. LTC, 2007.

[7] P. H. Pisani, **User Profiling com Redes Neurais**, http://br.geocities.com/php_rna/default.htm, Acesso em: 11 ago. 2008.

[8] USLAW.COM, **Identity Theft**. http://www.uslaw.com/us_law_dictionary/i/Identity+Theft. Acesso em: 10/Outubro/2008.

[9] IBM, **The Need for Authentication and Authorization**. IBM Redbooks, 2003. http://www.redbooks.ibm.com/abstracts/tips0266.html?Open. Acesso em: 10/Outubro/2008.

[10] K. Scarfone & P. Mell, **Guide to Intrusion Detection and Prevention Systems (IDPS)**, National Institute of Standards and Technology (NIST), 2007.

[11] P. Elftmann, **Secure Alternatives to Password-based Authentication Mechanisms**, Lab. for Dependable Distributed Systems, RWTH Aachen Univ., 2006.

[12] S. Russell & P. Norvig, **Artificial Intelligence – A Modern Approach**, 2nd ed., Prentice-Hall, 2004.

[13] **O Sistema Nervoso Humano**. http://www.portaltosabendo.com.br/index.php/assuntos_quentes/visualizar/o_sistema_nervoso_humano.wsa. 20/Setembro/2008.

[14] W.S. McCulloch & W. Pitts, **A logical calculus of the ideas immanent in nervous activity**. Bulletin of Mathematical Biophysics, 5:115–137, 1943.

[15] G. Cybenko, **Approximation by superpositions of a sigmoid function**. Mathematics of Control, Signal and Systems, 2:303-314, 1989.

[16] R. Duda et. al., **Pattern classification**. John Wiley and Sons. 0-471-05669-3, 2001.