Autenticação contínua para smartphones baseada em assinatura acústica

Marcelo da Luz Colomé, Raul Ceretta Nunes

Departamento de Computação Aplicada – Centro de Tecnologia

Universidade Federal de Santa Maria, Santa Maria – RS – Brazil

{marcelocolome, ceretta}@inf.ufsm.br

Abstract. *With the increasing of data and sensible information stored in smartphones, control the access to this devices is essential in order to mitigate risks. In this sense, a variety of authentication mechanisms has been explored, as the use of passwords and gestures. However, users tend to set weak password combinations or gestures that are easy to reproduce. This fact has been stimulating the research for continuous authentication methods, based on the user's interaction, which also run in background. The purpose of this paper is a new continuous authenticating method based on acoustic signature that is produced by the user-smartphone's interaction.*

Resumo. *Com o aumento de dados e informações sensíveis armazenados nos smartphones, controlar o acesso aos dispositivos é essencial para redução de riscos. Neste sentido diferentes mecanismos de autenticação tem sido explorados, tal como o uso de senhas ou gestos. Entretanto, os usuários costumam utilizar combinações ou gestos facilmente reproduzíveis, o que têm estimulado a perquisa por métodos de autenticação contínua baseados na interação do usuário e que executam em background. Este artigo propõe um novo método de autenticação contínua baseado em assinatura acústica produzida a partir da interação usuário-smartphone.*

1. Introdução

No cenário atual, *smartphones* são largamente utilizados, sendo estes dispositivos capazes de armazenar dados e informações importantes (sensíveis). Porém, estes dispositivos estão suscetíveis a uma variedade de riscos, tais como perda, roubo ou invasões, o que pode resultar em um acesso não permitido aos dados e informações. Dentre os principais tipos de autenticação de smartphones estão a autenticação por senha e a autenticação baseada em gestos, mas segundo [Frank et al. 2013] os usuários geralmente definem senha fracas, ou até mesmo desativam este tipo de proteção, deixando o dispositivo suscetível a ataques. Isto é um claro indicativo que apenas este tipo de autenticação não oferece uma boa solução para resolver a autenticação em smartphones.

Uma técnica de autenticação alternativa, chamada de autenticação contínua (*continuous authentication*), consiste em verificar continuamente, em background, se o usuário é autentico, oferecendo uma segunda barreira de proteção em complemento à

autenticação convencional [Frank et al. 2013]. Sem interromper o usuário, este tipo de autenticação costuma ser baseada em dados biométricos que podem ser captados do usuário que interage com o dispositivo pelos sensores presentes no mesmo. No caso dos *smartphones*, estas informações podem ser captadas através da tela sensível ao toque, ou com sensores presentes em grande parte dos *smartphones* atuais como o giroscópio, o acelerômetro, o magnetômetro e o microfone. Uma vez captadas, as informações podem ser usadas para a criação de um perfil individual de cada usuário, uma espécie de assinatura biométrica que é usada para identificar, de uma maneira não obstrutiva, se o usuário do sistema é autêntico.

Alkilani e Shirkhodaie (2013) propuseram uma técnica de reconhecimento de assinaturas acústicas para interações humano-objeto e que foi aplicada em sistema de vigilância. O desafio foi identificar o padrão de som (assinatura) emitido pela manipulação de objetos de diferentes materiais, como metal, plástico e madeira, em diferentes situações, mas a solução é computacionalmente complexa. No caso dos smartphones, oferecer um novo método de autenticação contínua baseado no som proveniente da interação humana com o dispositivo ainda é uma tarefa não resolvida. Há de se considerar que os smartphones são dispositivos com limitações de processamento e de consumo de energia, o que demanda soluções específicas.

Este trabalho apresenta uma solução para a autenticação contínua em smartphones, a qual é baseada no processamento em background dos sons capturados pelo microfone do dispositivo e na identificação de uma assinatura acústica que permita detectar o uso por usuário legítimo ou por usuário não autorizado (intruso).

2. Solução Proposta

Visando solucionar o problema da autenticação contínua baseada em sons provenientes da interação usuário-dispositivo, este trabalho alia estratégias já aplicadas à autenticação contínua com técnicas usadas para a identificação de padrões de som (assinatura acústica).

Na autenticação contínua, diferentes técnicas de seleção de atributos são utilizadas para reduzir o espectro das informações de interesse. Alguns autores como Song et al. (2013) preferem a técnica Fisher de seleção de atributos [Duda e Stork 2001], uma das técnicas supervisionadas mais utilizadas devido ao seu bom desempenho em geral, enquanto outros como Govindarajan, Gasti e Balagani (2013) utilizam a seleção não supervisionada baseada na derivação da mediana absoluta (MAD). Por não utilizar informação de referência, a seleção não supervisionada pode facilitar a escalabilidade por não exigir que o processo de seleção de atributos seja refeito quando um novo usuário do dispositivo é considerado, tal como pode acontecer em dispositivos empresariais.

Para a fase de seleção de atributos, considerando que os dados provenientes do microfone podem resultar numa classe de dados não balanceada, neste trabalho optou-se pela utilização dos algoritmos *Random Forests* [Liaw and Wiener 2002] e *k-d-tree* para classificar os atributos mais significativos. Baseado nesta classificação, um perfil do usuário pode ser construído a partir das informações extraídas do áudio proveniente da interação do usuário com o *smartphone*.

A obtenção de uma assinatura acústica depende de técnicas de identificação de padrões de som similares as usadas para a extração de atributos dos arquivos de áudio, tal como a Transformada de Fourier (*Fast Fourier Transform – FFT)* usada em [Alkilani and Shirkhodaie 2013]. Por isto, o primeiro passo do nosso método é a extração dos atributos de áudio presentes nos arquivos que podem ser gravados a partir do microfone padrão do *smartphone*.

A primeira interação do usuário é usada para o treinamento do modelo de autenticação e subsequente para teste. O processo de extração é seguido do processo de seleção, que tem como objetivo identificar os atributos mais discriminativos, isto é, os que irão proporcionar uma maior chance de obtenção de padrões de som significativamente distintos.

Na fase de extração, o arquivo de áudio gerado durante a interação do usuário com o *smartphone* é dividido em pequenos pedaços contendo apenas os momentos sonoros onde há informação relevante, tal como em [Alkilani and Shirkhodaie 2013]. A técnica empregada nesta etapa é determinar quando ocorrem os toques na tela do smartphone através do sensor de toque existente no dispositivo [Frank et al. 2013], pois estes toques geram eventos, como quando uma ligação está sendo efetuada pelo usuário. Posteriormente então, divide-se o arquivo em várias partes baseado na informação temporal dos eventos captados. Assim a tarefa de determinar o momento exato deste tipo de interação é facilitada, necessitando apenas o ajuste de sincronia do arquivo de áudio com os dados provenientes do sensor de tela. Um script que lê as informações de quando os toques ocorreram no dispositivo, divide o arquivo principal em arquivos menores que contém apenas o som proveniente da interação do usuário com este dispositivo. Após esta etapa, o *software* JAudio [JAudio 2013] é usado para a extração de valores de domínio de frequência através da Transformada Fourier. A partir deste valor encontrado para cada pequeno arquivo de áudio calcula-se o valor mínimo, máximo, médio, desvio padrão e mediana. Todos estes valores farão parte do vetor que representa o perfil do usuário.

Construído o perfil do usuário, a próxima etapa é a comparação dos perfis de usuários. Usa-se a distância Manhattan e a distância Euclideana para comparar a distância entre os vetores que representam os perfis de usuário (construídos na etapa anterior). Compara-se assim os perfis do próprio usuário consigo mesmo e os perfis de usuário entre si. Quanto menor a distância entre o próprio usuário e maior a distância entre os usuários diferentes, menor é a probabilidade de autenticação com falsa aceitação (*False Acceptance Rate*) e falsa rejeição (*False Rejection Rate*) do modelo de autenticação [Govindarajan, Gasti and Balagani 2013].

O produto final do método de autenticação proposto é um modelo de autenticação que pode ser aplicado a um *smartphone* convencional, sem a necessidade de implantação de *hardware* adicional, e que permite verificar continuamente o usuário baseado no som produzido pela sua interação com o dispositivo, isto é, sua assinatura acústica. Quando o sistema de autenticação está ativo no *smartphone*, ele capta o áudio proveniente da interação e o compara com a assinatura acústica previamente gravada no dispositivo. Portanto, se a assinatura acústica não corresponder com o perfil acústico do usuário pode-se enquadrar o usuário como intruso e a autorização de acesso pode ser negada.

É importante ressaltar que os testes estão em desenvolvimento e que a precisão do método ainda não foi computada. Além disto, salienta-se que o método deve ser utilizado em conjunto com outros métodos de autenticação para melhor garantia na cessão de diretos de acesso, dado que os métodos de autenticação contínua não substituem métodos de autenticação convencionais.

3. Considerações finais

Conforme exposto neste trabalho, autenticação de smartphones requer uma abordagem diferente das técnicas utilizadas na segurança de outros dispositivos como os computadores pessoais. A autenticação contínua oferece esta abordagem diferenciada, na qual o usuário é autenticado com base em seu comportamento, e não na informação que ele carrega consigo, como uma senha ou um padrão de gestos. A autenticação contínua baseada em sons produzidos pela interação entre o usuário e o dispositivo é uma técnica promissora de autenticação contínua, porém ao que alcança o conhecimento dos autores, é algo ainda não explorado fora deste trabalho.

A solução apresentada neste trabalho utiliza técnicas de extração de atributos de som, técnica usada com sucesso em [Alkilani and Shirkhodaie 2013] para a elaboração de um perfil de sons provenientes da interação humano-objeto, juntamente com estratégias de autenticação contínua usadas em [Frank et al. 2013], [Serwadda and Phoha 2013], [Govindarajan, Gasti and Balagani 2013], [Song et al. 2013].

4. Referências

Frank, M., Biedert, R., Ma, E., Martinovic, I. and Song, D. (2013). Touchalytics: On the applicability of touchscreen input as a behavioral biometric for continuous authentication. *IEEE Transactions On Information Forensics And Security*, 8(1):136-148, January.

Alkilani, A. and Shirkhodaie, A. (2013). Acoustic signature recognition technique for Human-Object Interactions (HOI) in persistent surveillance systems. *Proc. SPIE 8745, Signal Processing, Sensor Fusion, and Target Recognition XXII*, May, doi:10.1117/12.2018627.

Serwadda, A. and Phoha, V. V. (2013). When kids toys breach mobile phone security. *ACM SIGSAC conference on Computer & communications security (CCS '13)*.

Govindarajan, S., Gasti, P. and Balagani, K. S. (2013). Secure privacy-preserving protocols for outsourcing continuous authentication of smartphone users with touch data. *Biometrics: Theory, Ap- plications and Systems (BTAS), IEEE Sixth International Conference on*, vol., no., pp.1-8, doi: 10.1109/BTAS.2013.6712742.

JAudio 1.0 (2013). http://jaudio.sourceforge.net, Acesso em Julho.

Song, Y., Salem, M. B., Hershkop, S. and Stolfo, S. J. (2013). System level user behavior biometrics using fisher features and gaussian mixture models. *Security and Privacy Workshops (SPW), 2013 IEEE*, pages 52-59, May.

Duda, P. E. H. R. O. and Stork, D. G. (2001). Pattern Classication. Wiley-Interscience Publication.

Liaw, A. and Wiener, M. (2002). Classification and Regression by randomForest. R News, v.2, n.3, December, pp.18-22.

