Sistematização do Contexto como Fator de Autenticação de Usuários de Dispositivos Móveis

Márcio A. S. Correia[1,2], Pablo Ximenes[1], Rossana M. C. Andrade[1,2]

Universidade Federal do Ceará (UFC)
[1]Mestrado e Doutorado em Ciência da Computação (MDCC)
[2]Grupo de Redes de Computadores, Engenharia de Software e Sistemas (GREat)
Fortaleza, CE – Brasil

{marcio,rossana}@ufc.br, pablo@ximen.es

Abstract. *The need to protect mobile devices from unauthorized access is growing. On the other hand, conventional mechanisms currently used for authentication represent an obstacle that users need to overcome every time they want to use their devices. This problem is exacerbated in mobile devices because of their differences in the use dynamics. In this scenario, many authors propose solutions based on implicit, transparent and continuous authentication focused mainly on the use of biometric factors. Unlike other studies, we propose the use of context as a user authentication factor together with a systematization of this strategy on mobile devices. In order to achieve this goal our proposal makes use of the context acquisition framework LoCCAM and Hidden Markov Models (HMM) techniques.*

Resumo. *A necessidade de proteger os dispositivos móveis de acessos não autorizados é crescente. Por outro lado, os mecanismos convencionais de autenticação utilizados hoje representam um obstáculo difícil que os usuários precisam vencer sempre que desejam utilizar seus dispositivos. Essa problemática é agravada nos dispositivos móveis por conta das suas diferenças na dinâmica de utilização. Nesse cenário, muitos autores propõem soluções baseadas em autenticação implícita, transparente e contínua focadas principalmente no uso de fatores biométricos. Diferente dos outros trabalhos, propomos o uso do contexto como fator de autenticação dos usuários e uma sistematização do seu uso nos dispositivos móveis, utilizando para isso o framework de aquisição de contexto LoCCAM e Cadeias de Markov Ocultas (Hidden Markov Model - HMM).*

1. Introdução

Para Crawford (2014), a autenticação em dispositivos móveis não deve ser pensada da mesma forma que nos computadores pessoais (*desktop* e *laptop*). Para ele, a principal diferença está na forma como interagimos com esses dispositivos. Usamos os dispositivos móveis em "rajadas", isto é, buscamos eles com maior frequência, mas por curtos períodos de tempo. Nesse caso, ao oferecer mecanismos de autenticação impróprios para dispositivos móveis, podemos importunar os usuários ao ponto deles desativarem a autenticação ou usarem códigos de acesso inseguros.

Segundo Regina Dugan[1] da Motorola, estudos revelam que um usuário leva em média 2,3 segundo para desbloquear o seu telefone e faz isso cerca de 39 vezes por dia.

1 http://motorola-blog.blogspot.com.br/2013/08/hello-skip-goodbye-pin-introducing.html

Quando analisamos apenas usuários avançados, o número de desbloqueios chega perto de 100 vezes por dia. Isso pode representar para eles um grande desperdício de tempo com uma tarefa que deveria ser trivial. É um processo tão lento e repetitivo que muitos usuários entrevistados durante esses estudos relataram preferir usar códigos fáceis (e.g. "0000") ou, simplesmente, não se preocupar com autenticação. Assim, podemos concluir que esses mecanismos, na prática, não agregam segurança para uma grande parcela dos usuários de dispositivos móveis.

Para Wiedenbeck (2006), outra questão importante é que os dispositivos móveis, por serem muito utilizados em locais púbicos, são mais vulneráveis a ataques de observação direta, tais como olhar por cima do ombro de alguém (*shoulder-surfing*) para obter informações sigilosas (e.g. códigos de acesso). Portanto, os mecanismos de autenticação oferecidos nas plataformas móveis precisam ser mais resistentes a essa ameaça.

Na tentativa de superar as limitações de utilização de técnicas tradicionais de autenticação nos dispositivos móveis, vários autores têm proposto o uso de autenticação implícita (Jakobsson et al., 2009), transparente e contínua (Clarke, 2011). Contudo, ao focar nos aspectos biométricos, eles deixam de lado um rico conjunto de elementos relevantes na interação entre usuário e sistema, denominado por Dey (2001) de contexto. Por isso, propomos a seguir uma investigação que vai além dos elementos biométricos e busca a sistematização do uso de elementos de contexto como fator de autenticação de usuários para sua ampla utilização junto aos dispositivos móveis.

2. Proposta

O contexto é formado por pedaços de informação que podem ser usados para caracterizar a situação de um elemento que é relevante para a interação entre o usuário e o sistema, incluindo como elementos os próprios usuário e sistema (Dey, 2001). Ele pode ser entendido como uma visão estruturada e unificada do mundo em que o sistema opera, dentro de um processo de constante mudança (Coutaz el al., 2005). Os elementos que compõem o contexto dependem da sua relevância para o sistema e da possibilidade de observá-los, fazendo com que o contexto seja dinâmico e evolua ao longo da execução do sistema (Viana, 2010). Baseado nestas visões de contexto, podemos perceber que os fatores de autenticação tradicionalmente utilizados – o que o usuário sabe, tem ou é – nada mais são do que elementos do contexto, pois, sem dúvida, são considerados relevantes na interação entre o usuário e um sistema que requer controle de acesso. Entretanto, para que o contexto possa ser usado como fator de autenticação, ele deve atender a alguns requisitos importantes como, por exemplo, a unicidade.

Alguns outros estudos já propuseram o uso do contexto durante a autenticação dos usuários. Discutiremos aqui dois deles que mais bem ilustram as abordagens já propostas. O primeiro é o *Smart Lock*[2] que está presente na plataforma Android L. Ele permite selecionar alguns elementos de contexto que manterão o dispositivo móvel desbloqueado, como por exemplo, locais e dispositivos confiáveis. Essa abordagem busca usar o contexto para avaliar o risco e requerer ou não autenticação do usuário, evitando que ele precise repetir essa operação múltiplas vezes em situações onde não existe um risco tão elevado. O outro estudo é o *framework* CASA (Hayashi et al., 2013). Nesse estudo, os autores buscam modular a técnica de autenticação explícita exigida pelo dispositivo com base em múltiplos elementos do contexto com o objetivo de

2 http://get.google.com/smartlock/

manter um balanceamento entre segurança e usabilidade. Essa abordagem permite, da mesma forma que a anterior, manter o dispositivo desbloqueado em situações de baixo risco, mas permite também, por exemplo, requerer autenticação baseada em senha alfanumérica em situações que o risco é alto e o usuário teoricamente pode digitar uma senha usando o teclado virtual. Permite ainda, por exemplo, requerer código de acesso baseado em padrão gráfico em situações que o risco é intermediário e isso adicionar mais conveniência para o usuário.

Diferente desses estudos, neste trabalho entendemos haver forte ligação entre os fatores de autenticação e os elementos do contexto e, por isso, propomos a utilização do contexto de forma semelhante a um sistema biométrico. Segundo Costa, Obelheiro e Fraga (2006), o modelo conceitual simples de um sistema biométrico típico está dividido nos processos de aquisição de exemplar, extração de atributos, registro de perfil e comparação. Assim, propomos a sistematização do uso do contexto como fator de autenticação seguindo esse mesmo modelo.

Para alcançar esse objetivo, o *framework* de aquisição de contexto LoCCAM (Maia et al., 2013) será adaptado para os processos de aquisição de exemplar e extração de atributos. A utilização do LoCCAM busca tirar proveito da sua arquitetura componentizada e adaptativa, que facilita a inclusão de suporte a aquisição de novos elementos de contexto e otimiza o desempenho da ferramenta. A arquitetura componentizada é especialmente importante para o suporte a aquisição de múltiplos elementos de contexto, pois é esperado que essa multiplicidade aumente a confiabilidade do sistema assim como ocorre nos sistemas biométricos (Costa; Obelheiro; e Fraga, 2006)

Além disso, serão utilizadas também Cadeias de Markov Ocultas (*Hidden Markov Models* – HMM) para as etapas de registro de perfil e comparação. Para Rabiner e Juang (1986), um HMM é um processo duplamente estocástico, composto por um processo estocástico subjacente que não é observável diretamente, pois está escondido, mas que pode ser observado através de outro conjunto de processos estocásticos que produzem sequências de símbolos observáveis. A utilização de HMM nessas etapas visa permitir a captura de padrões de interação de um usuário baseado na obtenção de elementos observáveis de contexto.

Nossa estratégia adiciona uma camada de abstração, passando a considerar todo o contexto onde antes tinha-se foco apenas na biometria, incluindo agora também o ambiente e não somente o indivíduo. Desta forma, a combinação de vários outros elementos ligados não apenas ao usuário será vista pelo modelo como uma assinatura contextual que pode ser usada para autenticação.

A avaliação da proposta será feita por meio de experimento, onde será criado um protótipo de sistema. Esse protótipo será instalado em dispositivos de um grupo representativo de usuários escolhidos aleatoriamente e servirá para coletar um conjunto selecionado de dados contextuais. A partir desses dados, será gerado um perfil contextual para cada usuário. Cada perfil será comparado com os dados contextuais coletados de todos os usuários envolvidos no experimento, o que nos permitirá calcular e comparar as taxas de falso positivo (*False Accept Rate* – FAR) e falso negativo (*False Reject Rate* – FRR), da mesma forma que Costa, Obelheiro e Fraga (2006) propõem para avaliação de sistemas biométricos.

Por fim, embora nossa proposta apresente uma estratégia diferente das demais, nada impede que ela seja utilizada de forma combinada com as outras, servindo, nesse

caso, como técnica de autenticação alternativa, a ser aplicada quando for mais apropriado.

3. Considerações Finais

Conforme apresentado, este trabalho estabeleceu um paralelo entre os fatores comumente utilizados para autenticação e o contexto que envolve a interação do usuário com o sistema. Em seguida, propôs uma sistematização do uso dos elementos do contexto para autenticação de usuários em dispositivos móveis baseada no modelo de sistemas biométricos, fazendo uso do *framework* de aquisição de contexto LoCCAM e Cadeias de Markov Ocultas (HMM).

Referências

CLARKE, Nathan. (2011) Transparent User Authentication: Biometrics, RFID and Behavioural Profiling. Springer Science & Business Media.

COSTA, Luciano R.; OBELHEIRO, Rafael R.; FRAGA, Joni S. (2006) Introdução à Biometria. Livro texto dos Minicursos do VI Simpósio Brasileiro de Segurança da Informação e de Sistemas Computacionais (SBSeg2006), v. 1, p. 103-151. SBC: Porto Alegre.

COUTAZ, J. et al. (2005) Context is key. Communications of the ACM, v. 48, n. 3, p. 49-53. ACM.

CRAWFORD, Heather (2014) Adventures in Authentication – Position Paper. In: Symposium on Usable Privacy and Security (SOUPS).

DEY, A.K. Understanding and using context. Personal and ubiquitous computing, v. 5, n. 1, p. 4-7, 2001.

HAYASHI, Eiji et al. (2013) CASA: Context-Aware Scalable Authentication. In: Proceedings of the Ninth Symposium on Usable Privacy and Security (SOUPS'13), p. 3. ACM.

JAKOBSSON, Markus et al. (2009) Implicit Authentication for Mobile Devices. In: Proceedings of the 4th USENIX Conference on Hot Topics in Security. USENIX Association.

MAIA, M.E.F. et al. (2013) LOCCAM – Loosely Coupled Context Acquisition Middleware. In: Proceedings of the 28th Annual ACM Symposium on Applied Computing, p. 534-541. ACM.

RABINER, L. R.; JUANG, Biing-Hwang. (1986) An Introduction to Hidden Markov Models. ASSP Magazine, v. 3, n. 1, p. 4-16. IEEE.

VIANA, W. C. (2010) Mobilité et sensibilité au contexte pour la gestion de documments multimédias personnels: CoMMediA. Tese (Doutorado) — Université Joseph-Fourier – Grenoble. Disponível em: <http://hal.archives-ouvertes.fr/tel-00499550/>.

WIEDENBECK, Susan et al. (2006) Design and Evaluation of a Shoulder-Surfing Resistant Graphical Password Scheme. In: Proceedings of the Working Conference on Advanced Visual Interfaces, p. 177-184. ACM.

