Uma Survey em Autenticação de Usuários em *Smart Devices*: Defesas e Ataques

Artur L. F. Souza, Leonardo Cotta, Lucas Goulart Grossi
Antonio A. F. Loureiro, Leonardo B. Oliveira

[1]Universidade Federal de Minas Gerais (UFMG)
Belo Horizonte – Minas Gerais – Brasil

Abstract. *The smart device market has been growing rapidly along with the great technological advances from the past decades. Those devices have high computing power and storage, with increasingly more users keeping in them a great amount of information, many of them sensible. In this scenario, the user to device authentication has an extreme importance. In this paper, we survey the most relevant/recent authentication methods and known attacks in smart devices. Finally, we present a comparative analysis of them, along with the future directions of research in the area.*

1. Introdução

A autenticação de um usuário em um dispositivo compõe grande parte da segurança dos dados contidos naquele equipamento. Ela provê também a autorização e consequentemente a prestação de contas do usuário, conceitos apresentados em [Conrad 2012]. Normalmente, o dispositivo define um método a ser utilizado em que o usuário, ao requisitar acesso ao dispositivo, deve prover a devida autenticação. Caso o usuário seja autenticado, ele está autorizado a utilizar o dispositivo com determinados privilégios.

Smart devices são caracterizados principalmente por seu poder computacional e de armazenamento. Na medida em que a tecnologia provê maiores poderes aos dispositivos, os usuários aumentam a quantidade de informação armazenada neles e, consequentemente, o uso malicioso se torna mais perigoso. Juntamente a isso, o fato de grande parte dos *smart devices* serem móveis, sujeitos a ambientes com presenças desconhecidas, tornam a autenticação usuário-dispositivo imperativa. Geralmente, a autenticação é feita a cada uso, o que torna a usabilidade um fator de extrema importância em dispositivos com alta demanda de uso, como *smartphones* e *tablets*.

O objetivo desta *survey* é apresentar as principais e mais recentes tendências em técnicas de defesa e ataque no contexto de autenticação de usuários em *smart devices*.

2. Defesas

Mecanismos de autenticação comumente se dividem em três categorias: (i) algo que você sabe, (ii) algo que você é, (iii) algo que você possui. Na primeira categoria, o usuário se autentica através de um segredo compartilhado com o dispositivo (PINs e senhas). Na segunda, o usuário se autentica através de fatores biométricos (digital, voz, rosto). Por fim, algo que você possui inclui os mecanismos baseados em um autenticador externo físico (Token, smart cards).

Nesta seção, apresentamos algumas frentes de trabalho recentes na área de autenticação entre usuário e dispositivo, com trabalhos publicados em importantes conferências internacionais.

2.1. Algo que você sabe

Nessa categoria, o usuário se autentica mostrando que tem conhecimento de um segredo previamente definido. Os mecanismos mais comuns incluem PINs, senhas e, em dispositivos Android, o conhecido *Pattern Lock*. Esses mecanismos são conhecidos por serem simples e fáceis de usar, porém, vulneráveis a diversos ataques, alguns igualmente simples. Devido à imensa popularidade desses mecanismos, muitos autores, como Arif e Mazalek [Arif and Mazalek 2013], buscam formas de torná-los mais seguros, mantendo a usabilidade e simplicidade.

2.2. Algo que você é

Nesta categoria o usuário se autentica através de uma característica inerente e única ao indivíduo, como suas digitais, voz ou rosto. Esses mecanismos de autenticação tem se popularizado à medida que a tecnologia necessária avança e se torna mais precisa e acessível. Trabalhos mais recentes, como o trabalho de [Mock et al. 2012], buscam por novos fatores biométricos que sejam mais facilmente reconhecidos ou por técnicas melhores para reconhecer os fatores já utilizados.

2.3. Novas estratégias

Existem ainda mecanismos de autenticação que não se encaixam bem nas categorias existentes. Tais mecanismos se aproveitam dos sensores e de características particulares de alguns *smart devices* (a mobilidade, por exemplo) para a autenticação. Jakobsson *et al.* em [Jakobsson et al. 2009], propõem um trabalho nessa linha, concebendo um mecanismo de autenticação implícita, usando sensores e analisando o uso cotidiano do usuário para criar um padrão de uso e a partir deste determinar se o usuário é legítimo.

3. Ataques

A ampla disseminação de *smart devices* e o aumento constante de informações pessoais armazenadas neles tornam seu uso malicioso um problema. Além da grande quantidade de *malwares* disponíveis atualmente, os adversários contam com uma nova classe de ataques aos métodos de autenticação existentes baseados em visão computacional. Nessa seção, vamos classificar os ataques aos métodos de autenticação em três categorias: (i) identificação de textos da tela ou de reflexos da mesma, (ii) utilização de resíduos deixados na tela, (iii) reconhecimento da entrada quando o adversário não possui, ou possui parcialmente, visão da tela.

Todas as três categorias apresentam ataques eficazes com grandes percentuais de acerto, comprometendo a segurança do usuário (dados apresentados na tabela 1 ao final da seção). As duas primeiras categorias dependem de um contato direto com a tela do usuário. A terceira categoria não exige visualização completa da tela, o que representa uma vantagem sobre as demais.

3.1. Análise de textos da tela ou seus reflexos

Nessa categoria, o adversário faz uma abordagem direta de textos da tela do usuário ou de reflexos da mesma. Se enquadram nessa sessão técnicas que consistem na observação direta da tela do usuário e seus reflexos, exemplificados em [Maggi et al. 2011] e [Raguram et al. 2011], respectivamente.

3.2. Análise de resíduos deixados na tela

Os ataques dessa categoria são comumente chamados de *smudge* e consistem na análise direta da tela do *smartphone* para identificação de resíduos, como óleo corporal e digitais, deixados pelo toque do usuário. Em [Andriotis et al. 2014] há a descrição de um ataque do tipo *smudge* para identificação de esquemas de autenticação por inserção de padrão.

3.3. Reconhecimento de entradas com visibilidade comprometida da tela

Nos ataques dessa categoria, o adversário não precisa ter acesso direto a tela do dispositivo alvo. Técnicas de visão computacional são aplicadas para detecção da senha do usuário em situações em que o adversário não consegue ver diretamente textos, popups, reflexos ou traços corporais presentes na tela do usuário. Os ataques contemplados nessa categoria gravam o usuário digitando sua senha e utilizam algoritmos que estimam a posição do toque do usuário na tela para descobrir sua senha.

Um ataque deste tipo é apresentados em Shukla *et al.* [Shukla et al. 2014]. Nele técnicas de visão computacional são utilizadas para determinar quais pontos da tela foram tocados pelo usuário e, assim, descobrir seu segredo.

3.4. Outros Ataques

Há uma gama de ataques difícil de se classificar e que não se encaixa nas categorias anteriores. Todavia, é de considerável importância para os estudos de autenticação entre usuário e dispositivo no que diz respeito ao conhecimento e aprimoramento de técnicas de autenticação. Esses ataques utilizam uma abordagem peculiar para revelar o segredo do usuário, uma vez que visam utilizar recursos do próprio dispositivo alvo como som, câmera, microfone e sensor de luz, para obter a informação. Um exemplo desses ataques é contemplado em [Simon and Anderson 2013].

A tabela 1 relaciona os ataques mencionados nessa seção, os mecanismos atacados por eles e suas respectivas taxas de acerto.

Ataque	**Mecanismo Atacado I**	**Taxa de Acerto**	**Mecanismo Atacado II**	**Taxa de Acerto**
Smudge	*Pattern Lock* Incompleto	92.0%	*Pattern Lock* Completo	68.0%
Análise da Tela (Direto)	Inserção de Caracteres	98.85%	-	-
Análise da Tela (Reflexos)	Inserção de Caracteres	92.0%	Inserção de textos	35%
Visão Computacional	*PIN* 4 a 7 dígitos	94.0%	-	-
Outros Ataques	*PIN* 4 dígitos	50%	*PIN* 8 dígitos	45%

Tabela 1. Mecanismos atacados e respectivas taxas de acerto para cada ataque.

4. Direções Futuras

Além de mecanismos mais resistentes à ataques, fatores biométricos e comportamentais permitem a criação de mecanismos com maior usabilidade. Como por exemplo, nas propostas de Jakobsson *et al.* [Jakobsson et al. 2009] e Mock *et al.* [Mock et al. 2012]. Por

essa combinação de usabilidade e segurança, os autores deste trabalho acreditam que futuras pesquisas na área se concentrarão em criar mecanismos de autenticação cada vez mais precisos e simples, usando esses fatores intrínsecos ao indivíduo.

Porém, acreditamos também que ainda há espaço no estado da arte para avanços nos mecanismos de autenticação baseados em "algo que você sabe", principalmente trabalhos que tornem os mecanismos mais seguros e resistentes à ataques, enquanto mantém a usabilidade e simplicidade características desses mecanismos.

5. Conclusão

Em um mundo ubiquamente conectado por *smart devices*, a autenticação de usuário para dispositivo se torna um dos principais meios de se garantir a segurança de um sistema. Como mostrado, há diversos métodos disponíveis na literatura, em sua maioria baseados na entrada de senhas, padrões ou biometria. Ao passo que algumas soluções se estabelecem como padrões entre os usuários, novos ataques são projetados para elas. Isso abre espaço para propostas de métodos mais seguros de autenticação, mas por muitas vezes coloca em risco a usabilidade do método. Assim, caracterizamos um *trade-off* comum nesse cenário de autenticação, entre segurança e usabilidade.

Referências

Andriotis, P., Tryfonas, T., and Yu, Z. (2014). Breaking the android pattern lock screen with neural networks and smudge attacks. In *Poster session presented at Conference on Security and Privacy in Wireless and Mobile Networks*.

Arif, A. S. and Mazalek, A. (2013). A tap and gesture hybrid method for authenticating smartphone users. In *International Conference on Human-Computer Interaction with Mobile Devices and Services (MobileHCI'13)*, pages 486–491.

Conrad, Misenar, F. (2012). *CISSP study guide*. Elsevier Inc., 1st edition.

Jakobsson, M., Shi, E., Golle, P., and Chow, R. (2009). Implicit authentication for mobile devices. In *4th USENIX Conference on Hot Topics in Security*, pages 9–9.

Maggi, F., Volpatto, A., Gasparini, S., Boracchi, G., and Zanero, S. (2011). Poster: Fast, automatic iphone shoulder surfing. In *18th ACM Conference on Computer and Communications Security*, pages 805–808.

Mock, K., Hoanca, B., Weaver, J., and Milton, M. (2012). Real-time continuous iris recognition for authentication using an eye tracker. In *2012 ACM Conference on Computer and Communications Security*, pages 1007–1009.

Raguram, R., White, A. M., Goswami, D., Monrose, F., and Frahm, J.-M. (2011). ispy: Automatic reconstruction of typed input from compromising reflections. In *18th ACM Conference on Computer and Communications Security*, pages 527–536.

Shukla, D., Kumar, R., Serwadda, A., and Phoha, V. V. (2014). Beware, your hands reveal your secrets! In *2014 ACM SIGSAC Conference on Computer and Communications Security*, pages 904–917.

Simon, L. and Anderson, R. (2013). Pin skimmer: Inferring pins through the camera and microphone. In *Third ACM Workshop on Security and Privacy in Smartphones & Mobile Devices*, pages 67–78.