Proposta de Implementação de uma Aplicação de Mobile Payment com suporte a Dupla Autorização

José Carlos Ferreira Cavalcanti[1], **Luciano Ignaczak**[1]

[1]Universidade do Vale do Rio dos Sinos (UNISINOS) – São Leopoldo, RS – Brazil

contato@carloscavalcanti.com,lignaczak@unisinos.br

Abstract. *The use of mobile devices has been growing in last years and this allows the development of new forms to perform some activities. An activity transformed by the use of mobile devices is the payment of products or services, due to the growth of the mobile payment. However, mobile payment is facing some problems related to the security of transactions, creating risks to the users and virtual stores. In this context, this paper proposes a way to mitigate these risks: a mobile payment application that implements a dual authorization protocol.*

Resumo. *O uso de dispositivos móveis vem crescendo nos últimos anos, permitindo o desenvolvimento de formas alternativas para realizar algumas atividades. Um das atividades impactadas pelo uso de dispositivos móveis é o pagamento de produtos ou serviços, pois o mobile payment vem se destacando como opção no momento de realizar uma compra. No entanto, o mobile payment enfrenta problemas relacionados com a segurança da autorização de uma transação, trazendo riscos aos usuários e às lojas virtuais. Diante desse contexto, este trabalho propõe uma forma de mitigar esses riscos: a implementação de uma aplicação de mobile payment com suporte a dupla autorização.*

1. Introdução

O mundo digital começou a transformar o modo como os consumidores realizam seus pagamentos. Com a presença do *smartphone* em toda parte, ele se tornou um dispositivo essencial para o consumidor, com isso ficou claro que ele poderia ser utilizado também para realização de pagamentos [Mantri and Feng 2011]. Nas experiências no Brasil, destacou-se o Paggo Participações S/A em seu sistema de transação de crédito via telefone celular, onde o funcionamento ocorria através de trocas de SMS entre o consumidor e o lojista. Em 2006, a Oi lançou o OiPaggo, cartão de crédito vinculado à linha do telefone celular [MARTINS 2008]. De acordo com a pesquisa do terceiro trimestre de 2014 da Nielsen sobre *mobile payment*, 40% dos usuários já utilizam dispositivos móveis como principal modo de pagamento [nielsen 2014].

Os avanços do *e-payment* oferecem várias contribuições, como privacidade, conveniência, integridade, mobilidade, eficiência e baixo risco, além de um custo atraente [Keck 2010]. Com essas evoluções tecnológicas começam a aparecer novos modelos de negócios, mudando assim o modo que as pessoas realizam seus pagamentos. Com isso, as grandes empresas que possuem uma imensa influência no mercado como Google, Visa e Paypal, passam a oferecer também seus próprios serviços de *e-payment*. O modelo *m-payment*, que também é um tipo de *e-payment*, vem para facilitar o cotidiano das pessoas

e movimentar mais a economia [Lerner 2013]. Para realizar um pagamento é possível utilizar o *Near Field Communication* (NFC) como meio para concretizar uma transação, onde esta tecnologia tem obtido uma considerável atenção no meio do *m-payment*, devido a sua facilidade para uso e segurança [Li et al. 2008].

A grande facilidade no uso dos dispositivos móveis para pagamentos eletrônicos também pode gerar problemas, entre estes a possibilidade de pessoas não autorizadas realizarem transações. Existem casos nos Estados Unidos onde crianças realizaram compras sem a autorização do seu responsável [Altit 2014]. Devido a esses problemas de *in-app purchases* realizados por crianças, a Apple teve que devolver US$ 32,5 milhões em 2014 [AppleInsider 2014]. Segundo a [Engadget 2014], o mesmo ocorreu com a Google, que foi obrigada a reembolsar os usuários no valor de US$ 19 milhões no mesmo ano.

Devido às fraquezas amplamente conhecidas do método de usuário e senha, os sistemas que fazem uso dele não possuem elementos que possibilitam garantir, com alto grau de certeza, a identidade de um usuário [Harn and Ren 2011]. Segundo [Stallings 2008], existe uma falta de confiança nas trocas de informações, fazendo com que seja necessário uma segurança além da autenticação, através do certificado digital é possível verificar sua procedência e autenticidade afim de diminuir o risco de um terceiro não autorizado tentar realizar algum procedimento sem as devidas permissões.

O objetivo deste trabalho é elaborar um protocolo de *m-payment* baseado em dupla autorização para transações financeiras entre um consumidor e uma loja virtual, utilizando certificados digitais para identificação das partes e autorização do pagamento. O protocolo é composto por quatro entidades: usuário dependente, usuário autorizador, loja virtual e sistema de pagamento. O usuário dependente é o consumidor que realiza compras de serviços ou produtos de uma loja virtual, já o usuário autorizador aprova ou rejeita a transação através de uma solicitação exibida pelo aplicativo. Diante da aprovação do usuário autorizador, a transação é realizada pelo sistema de pagamento.

O artigo está dividido em cinco seções distintas. A segunda seção apresenta os conceitos relacionados a este artigo. A seção três demonstra o protocolo elaborado. Na seção quatro é descrita a proposta de implementação e na seção cinco são apresentadas as considerações finais.

2. Trabalhos relacionados

As pessoas utilizam os dispositivos móveis para diversos propósitos, desde acesso a redes sociais até a sistemas de *internet banking* para efetuar pagamentos [Felt et al. 2011]. Segundo [Furnell et al. 2008], a medida que a gama de serviços se expande é cada vez mais desejável que os usuários utilizem meios de protegerem seus serviços e aplicativos. Com a finalidade de restringir e evitar acessos indevidos a familiares, normalmente filhos, existem aplicativos capazes de filtrar e bloquear conteúdos acessados através do *smartphone* como, por exemplo, o *K9 Web Protection*, o *MetaCert* e o *Norton Family*. Porém, esses aplicativos se limitam a bloquear conteúdos e *sites* pré-definidos em suas configurações, ou seja, não há um bloqueio de ações diretamente, como a realização de um pagamento [Buratto and Glanzmann 2016].

A segurança no meio de pagamento é bastante importante, porém os usuários agem de forma a trazer riscos para eles mesmos. Segundo [Aloul et al. 2009], grande

parte dos sistemas na atualidade dependem de senhas estáticas para verificar a identidade do usuário. Porém, essas senhas provocam grandes preocupações relacionadas à segurança, onde a maioria dos usuários possuem o hábito de aumentar essa insegurança, como por exemplo, definir senhas de fácil adivinhação e utilizar as mesmas senhas em diferentes contas. Segundo [Felt et al. 2011], as atitudes que os usuários tomam para aumentar o risco fazem com que eles se tornem um alvo fácil, dando brecha para um terceiro não autorizado obtê-las. Além disso, o meio eletrônico ainda precisa lidar com alguns problemas, como as fraudes nas transmissões de dados e problemas de confiabilidade dos próprios sistemas. Segundo [Nag et al. 2015], a autenticação é a defesa fundamental contra qualquer acesso ilegítimo e, devido as ameaças, utilizá-la através de um único fator não é confiável para fornecer uma proteção adequada. Com esses problemas de segurança, os sistemas na atualidade já estão utilizando a autenticação através de múltiplos fatores com o propósito de minimizar os riscos à segurança.

Algumas das maiores empresas de tecnologia já possuem sistemas para realizar pagamentos utilizando dispositivos móveis. A Apple (2016) implementou a tecnologia chamada Apple Pay, disponível a partir do iPhone 6, que possibilita vincular os principais cartões de crédito e débito do mercado para realizar uma transação de pagamento. Para executar um pagamento é necessário somente uma aproximação do aparelho ao leitor usando a tecnologia NFC e um toque no Touch ID, sem a necessidade de abrir um aplicativo ou desbloquear o aparelho. Já o Google (2016) desenvolveu o Android Pay, semelhante ao Apple Pay, que também permite o armazenamento dos cartões e a utilização do NFC para realizar o tráfego de informações. Com o Android Pay é necessário desbloquear o aparelho e aproximá-lo do terminal, mas sem a necessidade de abrir um aplicativo. A Samsung (2016) desenvolveu o Samsung Pay que está disponível em alguns dispositivos da marca, entre eles os aparelhos da linha S6 e Note5. O Samsung Pay segue a mesma ideia do Apple Pay e Android Pay, com ele é possível adicionar os cartões desejados para efetuar as transações. Assim como a tecnologia da Apple, para efetuar uma compra é necessário tocar no leitor biométrico e aproximar o aparelho ao leitor, porém é necessário abrir o aplicativo do Samsung Pay.

Este trabalho está relacionado com os sistemas Apple Pay (Apple, 2016), Android Pay (Google, 2016) e Samsung Pay (Samsung, 2016), nos quais, utilizam o dispositivo móvel como meio para realizar uma transação financeira de forma prática e eficiente. No caso da Apple, houveram muitos problemas devido a facilidade das crianças realizarem compras dentro dos aplicativos (*in-app purchases*), com isso, foi implementado um controle parental para bloquear a possibilidade de realizar transações financeiras e podendo ser desbloqueado somente através de um PIN especifico da área de controle parental. Porém, é necessário estar em posse do aparelho a ser controlado para configurar este bloqueio. No projeto proposto não haverá necessidade de configurar o aparelho para evitar as transações. Para que isso ocorra foi adicionada uma camada, onde esta terá a responsabilidade de aprovar ou reprovar uma transação em tempo real, ou seja, no momento que a transação for requisitada.

3. Protocolo baseado em dupla autorização

Dentre as atividades previstas neste trabalho está a elaboração de um protocolo baseado em dupla autorização para transações financeiras entre um consumidor e uma loja virtual utilizando dispositivos móveis. O protocolo definiu uma terceira parte, denominada

usuário autorizador, que fará uso de um certificado digital para incrementar a segurança da autorização de uma transação. O protocolo elaborado possui 4 componentes, os quais são detalhados a seguir:

- Usuário dependente: o usuário que irá realizar a compra de um produto ou serviço de uma loja virtual, mas que não possui autonomia para autorizar o pagamento. A transação será iniciada pelo usuário dependente, porém somente o usuário autorizador poderá dar continuidade a ela.
- Usuário autorizador: o usuário responsável por aprovar ou rejeitar os pagamentos solicitados pelos usuários dependentes vinculados a ele.
- Loja virtual: responsável pela comunicação entre todas as entidades: o usuário autorizador, usuário dependente e o sistema de pagamento. Através da loja virtual o usuário dependente irá adquirir um produto ou serviço, após isso a própria loja virtual se comunicará com o usuário autorizador para que o mesmo realize a aprovação ou rejeição da transação. Se a transação for aprovada, a loja virtual irá proceder a autorização com o sistema de pagamento.
- Sistema de pagamento: entidade responsável por realizar a transferência do pagamento entre a conta do usuário autorizador e a conta da loja virtual.

Figura 1. Fluxo de pagamento móvel baseado em dupla autorização

Na Figura 1 é possível visualizar as ações ocorridas no protocolo. O processo começa através do usuário dependente, onde ele inicia a transação de pagamento para a loja virtual (passo 1), que por sua vez, realiza a pergunta ao usuário autorizador se o processo deve ser aprovado ou rejeitado pelo usuário autorizador (passo 2). Ao receber a resposta do autorizador (passo 3), se a transação for aprovada, a loja virtual irá requisitar ao sistema de pagamento a efetivação do pagamento (passo 4). O sistema de pagamento deverá retornar a situação à loja virtual (passo 5), a qual informará o usuário dependente (passo 6).

4. Implementação

A proposta da aplicação que implementará o protocolo elaborado pelo autor fará uso de diversas tecnologias disponíveis para o sistema operacional Android, as quais deverão ser utilizadas para assegurar que o protocolo atenda aos requisitos de segurança necessários para o funcionamento do sistema. O protocolo não tem como objetivo garantir a confidencialidade das informações, mas de garantir a autenticação das partes envolvidas. Para atingir este propósito será utilizado certificados digitais para assinar digitalmente a autorização, oferecendo elementos que permitem detectar alterações nas informações de uma compra. Abaixo são apresentadas as tecnologias que irão ser utilizadas:

- *Push notification*: o *push notification* é o responsável por notificar as partes sobre as transações. Para o usuário autorizador é utilizado para requisitar a aprovação da transação, já no usuário dependente é usado para informar o sucesso ou não da transação.
- *Web service*: *web service* é a solução que possibilita a integração entre sistemas, estabelecendo uma comunicação entre as partes envolvidas no protocolo. Através dos *web services*, a loja virtual e o sistema de pagamentos disponibilizam seus serviços, possibilitando que a loja virtual interaja com os usuários autorizador e dependente através dos *smartphones*; já o sistema de pagamentos faz uso de *web services* para integração com a loja virtual. Para a implementação do *web services* será utilizado o paradigma RESTful, responsável por ditar a arquitetura e o funcionamento da comunicação entre todos os envolvidos no sistema.
- Certificado digital: o intuito do certificado digital é realizar a assinatura digital da aprovação ou rejeição de uma transação, garantindo assim a autenticação do usuário autorizador e, consequentemente, a segurança do processo.
- *Near Field Communication* (NFC): para agilizar o inicio da transação de pagamento, o projeto prevê utilizar a tecnologia NFC para realizar a troca de informações entre o usuário dependente e a loja virtual. A partir desta troca de informação inicia-se o processo da transação definida no protocolo.
- Sistema de pagamento: o sistema de pagamento adotado é o PayPal, onde o mesmo disponibiliza serviços que podem ser consumidos com o intuito de realizar transações financeira através de serviços de terceiros.

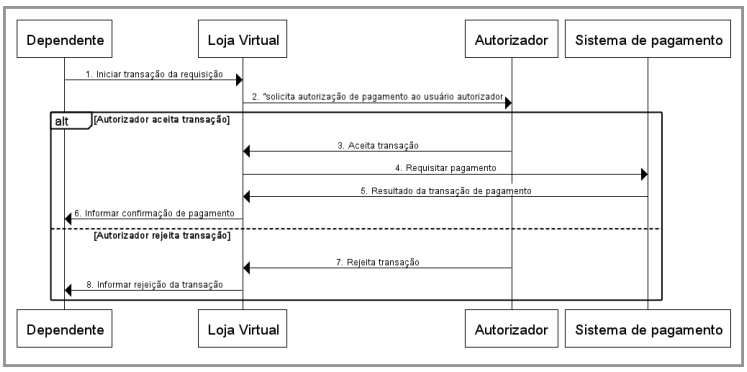

Figura 2. Processo de pagamento

Na Figura 2 é apresentado o diagrama de sequência. No diagrama são representados os fluxos de mensagens relacionados com a aprovação e rejeição de uma transação.

- Passo 1: o usuário dependente irá selecionar os serviços e/ou produtos e realizar a troca de informação com a loja virtual através da tecnologia NFC para que a transação seja iniciada.
- Passo 2: a loja virtual irá disparar um *push notification* para o usuário autorizador e será requisitado a ele que aprove ou rejeite a transação. Caso a transação seja rejeitada o fluxo seguirá para o passo 7.
- Passo 3: o usuário autorizador aprova o pagamento, selecionando o certificado digital para garantir sua identificação, assina a transação e envia à loja virtual.

- Passo 4: a loja virtual irá realizar o pedido da efetivação da transação junto ao sistema de pagamento (PayPal).
- Passo 5: o sistema de pagamento irá retornar o resultado da transação, podendo ser uma confirmação ou não do pagamento.
- Passo 6: a loja virtual irá notificar ao usuário dependente se a transação foi realizada com sucesso ou não, caso tenha tido algum tipo de problema irá conter o motivo.
- Passo 7: caso o usuário autorizador rejeite a transação, ele informa a loja virtual.
- Passo 8: o usuário dependente é notificado através de um *push notification* sobre a rejeição do usuário autorizador.

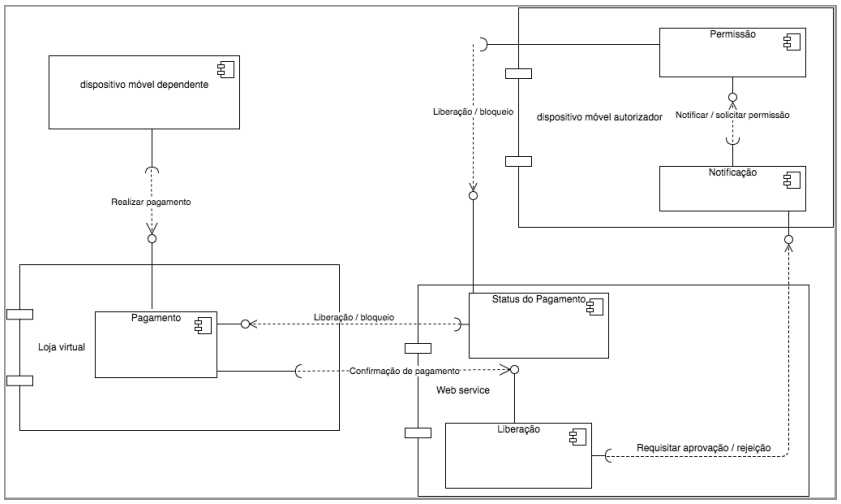

Figura 3. Diagrama de componentes da proposta de aplicação

Na Figura 3 é apresentado o diagrama de componentes, composto pelo dispositivo móvel do dependente, loja virtual e o dispositivo móvel autorizador. O processo é iniciado através do dispositivo dependente que realiza uma compra à loja virtual através do componente pagamento, que por sua vez, solicita a aprovação ou rejeição no componente liberação para o dispositivo autorizador junto ao componente notificação, onde conterão as informações da transação. Após o autorizador responder, a loja virtual irá receber a resposta através do componente permissão e realizar uma comunicação com o componente status de pagamento, que irá encaminhá-lo ao componente pagamento.

A Figura 4 apresenta três propostas de telas do aplicativo, criada através da plataforma Android Studio. A Figura 4a, representa a tela do usuário dependente onde ele visualiza as informações da transação a ser iniciada e dispõe de um botão para realizar o pagamento. A Figura 4b é a representação de uma notificação disparada para o usuário autorizador, contendo as informações da transação que foi iniciada pelo usuário dependente. Na Figura 4c são exibidos os dados da transação a ser aprovada ou rejeitada pelo próprio usuário autorizador.

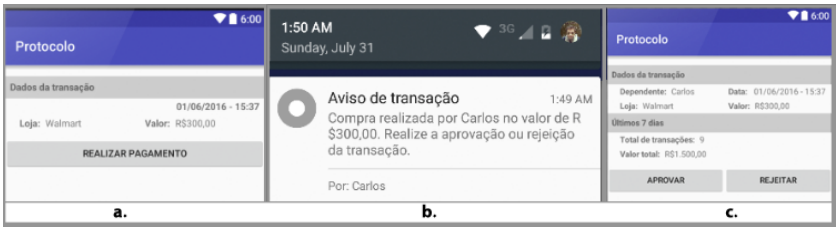

Figura 4. Notificação e tela de aprovar ou rejeitar transação

5. Considerações finais

Este trabalho realizou o desenvolvimento de uma aplicação de *mobile payment* com suporte a dupla autorização. O uso de dispositivos móveis por usuários com pouca compreensão do processo de pagamento móvel (ex. crianças) torna necessário uma confirmação para a efetivação de uma compra. A aplicação desenvolvida busca ocupar este espaço, possibilitando que pais entreguem dispositivos aos filhos e permita que eles façam compras em lojas virtuais sem extrapolar um valor pré-estipulado.

A necessidade de uso de um certificado digital pelo autorizador do pagamento oferece garantia à loja virtual que a compra foi autorizada por uma parte que detém privilégios para tal. Além disso, a assinatura digital impede que o responsável negue a aprovação de um pagamento, pois o mesmo assegura o requisito de não-repúdio.

Como trabalho futuro a aplicação desenvolvida poderá ser incrementada para o uso de outros sistemas de pagamentos, onde inicialmente foi utilizado o PayPal. Implementar uma área de configuração para usuário, onde poderá ser informado um limite pré-aprovado para os dependentes, com o intuito de aumentar a agilidade, onde caso este limite exceda, o usuário autorizador deva agir através de aprovação ou rejeição da transação.

Referências

Aloul, F., Zahidi, S., and El-Hajj, W. (2009). Two factor authentication using mobile phones. *IEEE*.

Altit, M. (2014). The freemium approach to children in the ios app market economy.

AppleInsider (2014). *Apple agrees to pay $32.5M in refunds, settling App Store in-app purchase lawsuit with US government*. AppleInsider. Disponível em: <http://appleinsider.com/articles/14/01/15/apple-settles-app-store-in-app-purchase-lawsuit-with-us-government>. Acesso em: 28 jul. 2016.

Buratto, R. P. and Glanzmann, J. H. (2016). Controle parental: uma análise das principais ferramentas para monitoramento e controle dos filhos na internet. *Seminários de Trabalho de Conclusão de Curso do Bacharelado em Sistemas de Informação*, 1(1).

Engadget (2014). *Google is refunding the $19 million your kids spent on in-app purchases*. Engadget. Disponível em: <https://www.engadget.com/2014/12/10/google-in-app-purchase-ftc-refund/>. Acesso em: 28 jul. 2016.

Felt, A. P., Finifter, M., Chin, E., Hanna, S., and Wagner, D. (2011). A survey of mobile malware in the wild. In *Proceedings of the 1st ACM workshop on Security and privacy in smartphones and mobile devices*, pages 3–14. ACM.

Furnell, S., Clarke, N., and Karatzouni, S. (2008). Beyond the pin: Enhancing user authentication for mobile devices. *Computer fraud & security*, 2008(8):12–17.

Harn, L. and Ren, J. (2011). Generalized digital certificate for user authentication and key establishment for secure communications. *Wireless Communications, IEEE Transactions on*, 10(7):2372–2379.

Keck, J. A. (2010). *Benefits & Risks of Electronic Payment Systems*. http://www.weltman.com/publications/articles/?i=200.

Lerner, T. (2013). *Mobile payment*. Springer.

Li, Q., Zhang, X., Seifert, J.-P., and Zhong, H. (2008). Secure mobile payment via trusted computing. In *Trusted Infrastructure Technologies Conference, 2008. APTC'08. Third Asia-Pacific*, pages 98–112. IEEE.

Mantri, R. and Feng, J. (2011). Exploring the key challenges: Adaptability, sustainability, interoperability and security to m-payment. *International Journal of Interactive Mobile Technologies (iJIM)*, 5(2):34–40.

MARTINS, G. S. e. a. (2008). Competitividade da tecnologia de pagamento via telefonia celular na cadeia brasileira de cartÃ£o de crÃ©dito. *XXXII Encontro da ANPAD*.

Nag, A. K., Roy, A., and Dasgupta, D. (2015). An adaptive approach towards the selection of multi-factor authentication. In *Computational Intelligence, 2015 IEEE Symposium Series on*, page 472. IEEE.

nielsen (2014). The modern wallet: Mobile payments are making life easier.

Stallings (2008). *Criptografia e segurança de redes: princípios e práticas*. Pearson Prentice Hall.