Um Sistema Móvel de Compras Rápido e Seguro via QR Code e Vitrine Virtual

Eduardo R. Costa, Karin S. Komati

Coordenadoria de Informática, Instituto Federal do Espírito Santo (IFES) Campus Serra
Rodovia ES-010, Km 6.5 – 29.164-231 – Serra – ES – Brasil

erigamonte@gmail.com, kkomati@ifes.edu.br

Abstract. *This work aims to present a sales system for mobile devices that is safe and agile. Particularly, the issue of safety was a major concern of this work. Our proposed solution is based on the use of QR Code to direct the user to the web store through their mobile devices; a strategy that we call virtual showcase. Unfortunately, this strategy potentially exposes the user of our system to different kinds of attack. We propose the use of symmetric key cryptography as a way to prevent these attacks. In this way we expect to guarantee, by the use of cryptography, that the information read from the QR Code is indeed valid.*

Resumo. *O objetivo deste trabalho é apresentar um sistema de compras para dispositivos móveis que seja rápido e seguro. Em particular, o quesito segurança foi a maior preocupação do trabalho. A solução proposta se baseia na utilização de QR Code para direcionar os usuários, através de seus dispositivos móveis, para o site de venda, estratégia que chamamos de vitrine virtual. Entretanto, esta estratégia expõe os usuários do sistema a diversos tipos de ataques. Propomos o uso de criptografia baseada em chaves simétricas como uma forma de evitar tais ataques. Desta forma buscamos garantir, através do uso de criptografia, que a informação lida do QR Code seja válida.*

1. Introdução

O comércio eletrônico *mobile* (*m-commerce*) está ganhando cada vez mais espaço. Segundo o instituto de pesquisas IDC [G1, 2012], até o ano de 2017 as compras feitas pelo celular chegarão a um montante de US$ 1 trilhão. A maior parte das compras inclui músicas, filmes e aplicativos, e recentemente, mercadorias, como: eletrônicos, roupas e alimentos. No entanto, muitas vezes a navegação em diversas páginas pode ser comprometida pelo tamanho da tela, ou as pessoas não possuem a destreza de digitar textos extensos nestes aparelhos. Para facilitar e agilizar o uso dos celulares, temos a tecnologia denominada de QR Code (*Quick Response Code*), que foi desenvolvido pela Denso Wave, lançado em 1994 e padronizado com o ISO/IEC 18004 [Denso Wave Corporation, 2012].

O QR Code é uma imagem, um código de barras 2D, em duas cores, que pode ser lido e interpretado pelos *smartphones*. Quando a informação contida pelo QR Code for uma URL, direciona-se automaticamente para o endereço fornecido na internet, tornando o acesso fácil e rápido [Komati, Costa e Andrade, 2012]. Uma característica visível é a presença de três quadrados nos vértices do código, chamados de padrões de localização. Esses padrões de detecção de posição garantem a leitura estável, evitando os efeitos negativos da interferência de fundo e possibilitando a leitura de 360º em alta

velocidade. Enquanto os códigos de barras convencionais armazenam no máximo 107 dígitos, o QR Code pode armazenar até 7089 dígitos.

Nesse contexto, o objetivo deste trabalho é apresentar um sistema de compras, o **Mobile Market**, rápido e seguro, utilizando a tecnologia QR Code e a ideia de vitrine virtual. Uma vitrine virtual pode ser uma revista, folheto ou encarte, que em geral é distribuído gratuitamente ou; pode estar na forma de cartazes dispostos em lugares públicos. O importante é que cada produto tenha um QR Code associado. A Figura 1 mostra o funcionamento do processo de compra: a vitrine virtual nesse caso é um encarte, onde o usuário aponta a câmera do celular para o símbolo QR Code do produto que deseja comprar. O aplicativo faz a leitura do código, decodifica-o, e comunica-se com o site, e vai enchendo o carrinho de compras.

Figura 1. Funcionamento de leitura do módulo Mobile, mostrando a leitura do QR Code e o acesso do produto no sistema da loja.

Já existem soluções similares no mercado como a da Multinacional Tesco [Estadão, 2012]. Esta empresa modificou a estrutura do QR Code original, pois os códigos apresentados mostram um padrão com 4 estruturas nos cantos do QR Code ao invés das 3 comumente usadas, programas genéricos de leitura de código QR Code não conseguem ler o conteúdo destes códigos. A grande motivação do uso de um código modificado se deve aos problemas quanto à segurança. Seres humanos não conseguem diferenciar entre imagens de QR Codes válidos ou aquelas que foram maliciosamente alterados. Um incidente aconteceu na Rússia [Wasserman, 2011], onde um QR Code adulterado enganou os consumidores que pensavam estar baixando um aplicativo Android chamado Jimm. O código continha um *malware* que enviou códigos SMS para um número de telefone que cobrava por cada mensagem enviada.

Assim, um diferencial deste trabalho é a inclusão da informação gravada no QR Code de forma cifrada. Diferente da solução da Tesco que alterou a estrutura do QR Code, este trabalho propõe criptografar a informação e manter a estrutura padrão do QR Code. Com o uso de criptografia de chave simétrica, garante-se que o QR Code lido é exatamente o mesmo QR Code gerado pela mesma empresa que está vendendo os produtos.

2. Solução Proposta: Mobile Market

O sistema terá dois módulos: a parte **Desktop**, e o aplicativo **Mobile**. A parte **Desktop** é

responsável pela criação do QR Code para estar associado a cada produto na vitrine virtual. O QR Code deverá conter as seguintes informações: URL do produto no *site* para localizar o produto desejado no *site* da loja, a data de validade do preço que se encontra na vitrine virtual e o preço tal qual na vitrine.

Uma das funcionalidades do módulo **Desktop** é a encriptação das informações e criação dos QR Codes, que serão associados na vitrine para a identificação no sistema do supermercado. Esse módulo foi feito em Java usando a API QRGen [Gullaksen, 2012] para a geração do QR Code. Os dados do QR Code estarão cifrados usando a técnica de criptografia de chave simétrica [cert.br, 2012], conforme a parte esquerda da Figura 2, denominada de "Geração".

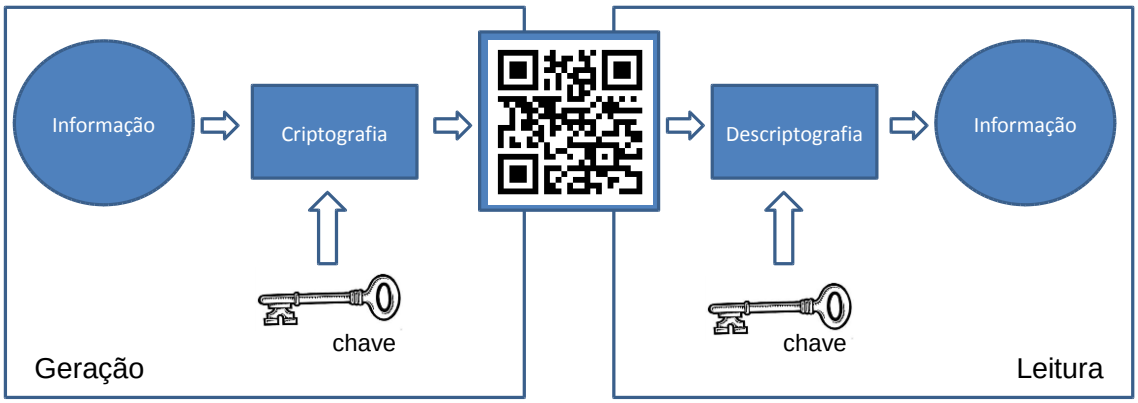

Figura 2. Fluxograma que mostra o passo a passo do processo de encriptação e desencriptação da informação contida no QR Code.

O aplicativo **Mobile** faz a leitura do código, decodifica-o, e comunica-se com o site, conseguindo as informações disponibilidade (ou quantidade em estoque), uma pequena imagem do produto e o preço atual do *site*. De forma fácil, o usuário poderá identificar quantos produtos ele deseja comprar ou mesmo se deseja retirar algum item do carrinho de compras. Ao finalizar o pedido, o usuário informará o endereço de entrega e uma forma de pagamento. Se a data de validade do preço, constante no QR Code, estiver expirada, o sistema irá alertar o usuário de que o produto teve seu preço reajustado e qual é o novo preço de acordo com o *site*.

Como é o aplicativo **Mobile** que fará a decodificação da informação gravada no QR Code e os dados no QR Code estarão cifrados, o usuário só conseguirá fazer as compras se usar o módulo **Mobile** fornecido, conforme a parte direita da Figura 2, denominada de "Leitura". Há o inconveniente de se fazer o *download* deste aplicativo no celular, mas será apenas uma vez.

O módulo **Mobile** foi desenvolvido na linguagem Java, utiliza a API Zxing [ZXING, 2012], que é um código aberto de leitura de códigos de barras, incluindo o QR Code. Além disso, o modulo **Mobile** utiliza a *API Mobile Payment* [PayPal, 2012], que é uma biblioteca muito simples para que vendedores possam integrar pagamentos diretamente de suas aplicações.

3. Considerações Finais

Apresentamos o sistema **Mobile Market**, que é um sistema de compras móvel rápido e seguro que utiliza as tecnologias QR Code e chaves simétricas. Uma vantagem deste sistema é o uso de criptografia de chave simétrica, que é uma técnica simples e

computacionalmente eficiente, para garantir que o QR Code lido é exatamente o mesmo QR Code gerado pela empresa que está vendendo os produtos, futuramente planeja-se testar o software com outras técnicas de criptografia, como a de chave assimétrica e com uma que é um misto entre a técnica anterior e a simétrica.

De acordo com Kieseberg et. al.(2010), é possível se prevenir ataques à processos automatizados e ataques à interação humana. Ataques à processos automatizados são: injeção SQL, injeção de comandos e fraudes. Os ataques à interação humana são: *phishing and pharming*, fraudes, leitor de software malicioso e engenharia social. Um exemplo de uma ação mal intencionada seria o de substituir ou sobrepor o QR Code original na vitrine (fraude), e com isso, redirecionar o usuário para outro site, que não o original. Todos os tipos de ataque se fiam na possibilidade de se criar QR Code com conteúdo malicioso. Na solução **Mobile Market**, todos os tipos de ataque são prevenidos via criptografia/descriptografia da informação, a não ser que o autor do ataque tenha conhecimento da chave.

Esta solução ainda está em desenvolvimento e já se efetua toda a operação de compra, no entanto, necessita de um aperfeiçoamento da interface com o usuário visando uma melhor atratividade. Para estender ainda mais as possibilidades, planeja-se futuramente, desenvolver o sistema **Mobile** para as plataformas Windows Phone e iOS.

Referências

cert.br (2012). “Cartiha de Segurança para Internet”. http://cartilha.cert.br/criptografia/, Junho.

Denso Wave Incorporate. (2012) “About QRCode.com”. http://www.qrcode.com/en/index.html, Outubro.

G1 (2012). “Compras com celulares chegarão a US$ 1 trilhão em 2017, diz pesquisa”. http://g1.globo.com/tecnologia/noticia/2012/11/compras-com-celulares-chegarao-us-1-trilhao-em-2017-diz-pesquisa.html, Novembro.

Estadão. (2012) "A estratégia dos grandes: rede de supermercados inova ao colocar prateleira virtual no metrô". http://pme.estadao.com.br/noticias/noticias,a-estrategia-dos-grandes-rede-de-supermercados-inova-ao-colocar-prateleira-virtual-no-metro,1708,0.htm, Abril.

Gullaksen, K. (2012). “QRGen”. http://kenglxn.github.com/QRGen, Outubro.

Kieseberg, P.; Leithner, M.; Mulazzani, M.; Munroe, L.; Schrittwieser, S.; Sinha, M. e Weippl, E. (2010) “Qr Code Security”. In: Proc. of The International Workshop on Trustworthy Ubiquitous Computing (TwUC’10), Paris, France.

Komati, K. S.; Costa, E. R. e Andrade, J. O. (2012). "Gerenciamento de Informações com QR Code e Código Hash Criptográfico". Em: Anais do XIX Simpósio de Engenharia de Produção (SIMPEP), 2012, Bauru.

PAYPAL. (2012). “Mobile Payment Libraries”. https://www.paypal-brasil.com.br/x/xblog/2012/02/15/mobile-payment-libraries, Fevereiro.

Wasserman, T. (2011) "New Security Threat: Infected QR Codes", http://mashable.com/2011/10/20/qr-code-security-threat/, October.

ZXING. (2012) “ZXing - Zebra Crossing”. http://code.google.com/p/zxing, Outubro.