Marque a opção do tipo de trabalho que está inscrevendo:

(X) Resumo **( ) Relato de Caso**

Autenticação de dispositivos NFC para sistema de pagamentos

AUTOR PRINCIPAL: Jhônatan de Lima de Souza
CO-AUTORES:
ORIENTADOR: Prof. Me. Carlos Adriani Lara Schaeffer
UNIVERSIDADE: Universidade de Passo Fundo

INTRODUÇÃO

Uma das tecnologias de comunicação que tem sido utilizada é a Comunicação por Campo de Proximidade, do inglês Near Field Communication ou NFC. Esta tecnologia permite a troca de informações sem fio entre dispositivos que estejam próximos um do outro. Estas informações são trocadas de maneira automática e instantânea sem a necessidade de maiores configurações. (NFC Forum, 2015).

O principal empecilho no que diz respeito ao uso dessa tecnologia está na segurança dos dados que estão sendo transferidos. Mesmo com a pouca distância exigida para que haja a comunicação, se nada impedir que um dispositivo invasor esteja camuflado entre a comunicação, será possível observar os dados transferidos na transação. Este trabalho busca descobrir vulnerabilidades e propor possíveis soluções para este problema através da autenticação dos dispositivos envolvidos durante a transação eletrônica.

DESENVOLVIMENTO:

Ao pensar no processo de autenticação dos dispositivos, seria possível a utilização do NFC presente num smartphone para realização de pagamentos, sendo então uma alternativa ao cartão de crédito. A proposta é desenvolver um software capaz de realizar a trasanção de maneira segura utilizando de métodos simples para autenticação.

Numa primeira etapa, é necessário gerar uma chave simétrica que será utilizada na criptografia dos dados que vão trafegar pelo meio inseguro. Para tanto, deve ser usado o algoritmo de troca de chaves Diffie-Hellman. No modelo apresentado ele funciona da seguinte maneira (Aldeia Numaboa, 2005): o computador do caixa, ao detectar a proximidade do smartphone, deve gerar dois números aleatórios denominados N e G com as seguintes premissas: N e (N-1)/2 devem ser primos e N maior de 512 bits. G deve ser menor que N, maior que 1 e raiz primitiva do módulo de N. Os valores gerados são enviados ao smartphone. Logo após, ambos os

dispositivos devem gerar um número aleatório grande e realizar o cálculo de módulo. Em seguida, devem trocar o resultado e realizar o modulo novamente, obtendo, desta forma, a chave simétrica denominada K.

Tendo realizadas estas etapas, o caixa e o smartphone têm a chave que é resultado do cálculo do segundo módulo. Através destes cálculos foi possível que ambos obtivessem a chave sem a necessidade de que ela trafegasse pelo meio inseguro. Ambos de posse da chave, os dispositivos podem prosseguir com a segunda etapa, onde é realizada a autenticação dos dispositivos e finalização da compra.

Na segunda etapa, o computador deve gerar um número aleatório e enviá-lo ao smartphone junto ao preço da compra. O smartphone, ao recebê-los, exibe na tela o valor e pede ao usuário que confirme. Caso haja a confirmação, o smartphone utiliza o número aleatório recebido e a chave K para aplicar o algoritmo de Hashing. Feito isso, o smatphone gera um novo número aleatório e o envia ao computador, junto com o HashCode gerado. O computador de posse do HashCode recebido faz o mesmo processo, utiliza o número aleatório que ele gerou e também aplica o algoritmo de Hashing neste número e a chave K, comparando se o HashCode recebido é igual ao gerado. Caso seja, o smartphone está autenticado pelo computador. No segundo passo da autenticação, o computador gera um HashCode com o número aleatório recebido do smartphone e envia para o mesmo. De posse do HashCode recebido, o smartphone utiliza o número aleatório gerado e também aplica o algoritmo de Hashing neste número e a chave K, e compara se o HashCode recebido é igual ao gerado. Caso sim, o computador está autenticado pelo smartphone. Ambos autenticados, podem finalizar a compra.

Desta forma, obtêm-se uma comunicação segura que torna viável a utilização de um smartphone para realizar pagamentos, tendo assim uma nova alternativa ao cartão de crédito.

CONSIDERAÇÕE S FINAIS:

O estudo de formas de autenticação entre dispositivos NFC é importante pois pode trazer à realidade uma forma nova e fácil de realizar pagamentos através do smartphone com segurança. Ficou observado que é algo de fácil implementação e que torna segura e viável este tipo de operação.

REFERÊNCIAS

Aldeia Numaboa – Criptografia Numaboa - O algoritmo Diffie Hellman. Disponível em: <http://www.numaboa.com.br/criptografia/chaves/353-diffie-hellman//>. Acesso em: 16 set. 2015.

NFC Forum – Whats Is NFC? Disponível em: <https://www.nfc-forum.org/what-is-nfc//>. Acesso em: 16 set. 2015.

QUINCOZES, S. E.; KAZIENKO, J. F. . Identificação Segura das Partes na Comunicação por Campo de Proximidade. In: Congresso Brasileiro Regional de Iniciação Científica e Tecnologia em Engenharia, 2014, Alegrete, Brasil. CRICTE, 2014. v. 1. p. 1-4.

NÚMERO DA APROVAÇÃO CEP OU CEUA (para trabalhos de pesquisa):

ANEXOS

Esquema de troca de mensagens: