Available online at www.sciencedirect.com

ScienceDirect

Procedia Computer Science 83 (2016) 685 – 689

Procedia Computer Science

The 7th International Conference on Ambient Systems, Networks and Technologies (ANT 2016)

A Study of Anonymous Purchasing Based on Mobile Payment System

Jieling Wu[a], Chenglian Liu[b,*], Donald Gardner[a]

[a]*Department of Economics and Management, Huizhou University, Huizhou 516007, China*
[b]*Department of Computer Science, Huizhou University, Huizhou 516007, China*

Abstract

"Anonymous purchasing" has been in use for about a decade. While we have been able to use anonymous purchasing to buy goods and services from home based desk-top computers for many years, it has only been within the last few years that anonymous purchasing has been used on a mobile platform. This has enabled the buyer to use anonymous purchasing almost anywhere such as restaurants where it had not been possible before. Now shoppers can easily use their Wechat account for purchasing goods using their mobile phone and do it anonymously. This has added to the privacy and security of the purchaser. This anonymity in purchasing is increasingly being demanded by more people. In this paper the authors will examine an anonymous purchasing system using digital signature techniques of cryptographic and mobile payment systems.

Peer-review under responsibility of the Conference Program Chairs

Keywords: Digital Signature; Anonymous; Hash Function; Mobile Payment;

1. Introduction

Many young people in China purchase goods and services online from popular websites such as meituan.com, lashou.com, and diaping.com. On these websites, shoppers can purchase goods, services, entertainment and travel. In the past, when shoppers made purchases on the internet, they would usually use a credit or debit card, which obviously, has no anonymity. For some people this is fine, but a growing number of customers are demanding anonymous purchasing because of spam and other security issues. More recently, shoppers are making purchases using e-cash through "Wechat" (or the Chinese application "Weixin"). Wechat is an instant mobile messaging application that is a Location Based Service (LBS) technology which provides a function called "Searching for the nearby". These applications have obvious privacy threats because users may send personal information to everyone surrounding them through the wifi system. In this paper, the authors will examine an anonymous payment system, using a mobile payment platform such as Wechat, where three entities are used to keep the buyer anonymous and keep the information secret: the purchaser, merchant, and issuer (usually the bank). These three entities are combined using verification

* Corresponding author. Tel.: +86-18850899538.
E-mail address: chenglian.liu@gmail.com

Peer-review under responsibility of the Conference Program Chairs
doi:10.1016/j.procs.2016.04.152

codes, in such a way, as to keep the buyer' information secret. Wechat, and other mobile systems, have been studied by Gao and Ying on the iPhone[1]. Lien and Cao[2] studied how shoppers use Wechat in China. Mao[3] did a more detailed study of purchasing patterns of Chinese undergraduate students using WeChat. There is some related literature about mobile payment systems in[4,5,6,7], but they are out of the scope of this article.

2. Analysis of Three Player Anonymous E-Cash Systems

2.1. System Overview

This purchasing system operates as follows: 1) Buyer transfers his cash to issuer (bank). 2) Issuer (bank) sends receipt of cash to buyer. 3) Buyer uses e-cash in shop. 4) Seller checks the verification code by issuer (bank). 5) Issuer transfers e-cash to shop. 6) Seller confirms this transaction with buyer.

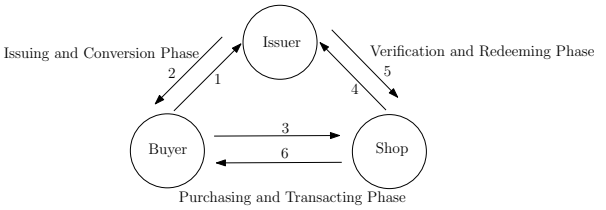

Figure 1. The role of three parties

2.2. Security Issues

Why would a shopper choose anonymous purchasing? The following are some important reasons: 1) To prevent the seller from collecting user data through transaction software such as the website. 2) It is confidential to purchaser. 3) To prevent advertising harassment. The main advantage of the system is that consumers remain anonymous because they do not send any personal information over wifi or other public systems.

3. Our Methodology and Scheme

There are seven phases in our methodology: system initialization, e-cash conversion, fetching, purchasing, verification, redemption and transaction confirmation. The following notations are used in this section:
Notations:
p: a large prime number where $|p|$ is 1204 bits length.
g: an element primitive generator of $\mathbb{Z}_p^*$.
x_i: the secret key.
y_i: the public key.
$h(.)$: a one-way hash function.
t: the e-cash.
m: money amount.
$||$: concatenation. These phases are described in the following subsection.

3.1. System Initialization

During system initialization, the buyer randomly chooses a secret key x_a to compute the public key y_a; the seller also randomly choose a secret key x_b to compute the public key y_b; the issuer randomly choose a secret key x_c to