Secure Micropayment Scheme for Newspaper Subscription - Pay Per Article

J.F. Fasna, M.A.M. Irfan, M.J.M. Rishadhy and M. Sandirigama
Department of Computer Engineering, Faculty of Engineering
University of Peradeniya, Sri Lanka

***Abstract*—Micropayment is the payment of very small amounts online that does not justify high overhead cryptographic techniques. Secure micropayment scheme is to provide a scheme which is more secure and simple.**

In this project, we are developing a micropayment scheme for newspaper industry. It is a subscribing scheme where a reader will not pay for the whole paper, but for the article he reads. To develop this system we need a bank, which acts as a Payment provider for the reader and a Newspaper site. For the payment process, SAS-(Simple and Secure Authentication Protocol) [1] [2] is used. Implementation of this protocol, authentication between user-bank, bank-newspaper and user-newspaper are the components of this system.

***Index Terms*—micropayment, newspaper, subscription, article, secure**

I. Introduction

An online transaction which deals with a small amount of money is called micropayment [3]. Some researches [4] cited that the sales of low priced product will increase in the future. As most of the online users are avoiding subscription plans and switching to individual product payment plans, introducing a new subscription plan for newspaper readers will be also a beneficial one.

Micropayment is used to purchase e-books, smart phone applications, music, and more. Now it is used to pay for newspaper contents which allows users to pay per article rather than subscribing to the entire edition of magazine or newspaper. The Chicago Sun-Times started to accepting micropayments in April 2014. During the first week, 7 out of its 62 subscriptions, or 11%, were paid using Bitcoin, a form of digital micropayment [5].

The purpose of this project is to implement a micropayment based subscription scheme for newspaper industry. This scheme is to produce benefit to the reader. When a reader pay for a monthly subscription plan, he may not read the paper every day and not every article. Therefore, this subscription plan will let the reader to pay only for the article he reads.

To implement the full scheme, we design a banking system where the reader will buy the micropayment tokens to use in the newspaper site, a dummy newspaper site and a secure payment protocol.

II. Literature Survey

We could look the micro payment systems in two stages. Token based micro payment systems were considered as first generation micro payment systems. Here the transaction between the consumer and vendor was happened using the token in place of money.

User interfaces and management were so much unfriendly in the first generation micro payment system, which caused difficulty to the users. Also, users were only able to use the computers which stored their tokens to access the micro payment software.

There were no significant success for the token based micro payment system. The cost of transaction was depend on administering, issuing and validating tokens. Those were too expensive compared to the transaction [6].

The next stage came in the early 2000s. These new generation systems are account based. No more money related details were transmitted through the Internet. It is easier than before. We chose some micropayment systems which are most successful systems for the literature review. They are PayPal, Bitcoin and Flattr.

A. PayPal

PayPal is quick and easy for buyers to use, especially if they already have PayPal account. But if we consider to use this system to magazine industry which is used pay per article, it is not suitable. Because PayPal charges 5 percent of the product cost, plus 5 cents (in dollars) per each transaction, a profit amount below 20 cents is not beneficial to any industry.

Also PayPal is very vulnerable to fraud [7]. If someone cheats the customer, seller need to pay the price when it happens, either by losing your money or getting your account frozen. It is vulnerable to Man in the Browser Attack too.

B. Bitcoin

Bitcoin is an online payment system invented in 2008 by Satoshi Nakamoto. He released the system as a open-source software in 2009. The system is peer-to-peer. There is no individual owner for the Bitcoin network. The users all around the world have control over it. If we look from a user perspective, it is like a computer program.

First, we want to install Bitcoin wallet. Then it will generate bitcoin address based on your computer's public key which is stored in your wallet secretly. Users can own and generate multiple Bitcoin addresses. Generating addresses is similar to generating a public private key pair. Generation of Bitcoin is called mining. We can define a coin as a chain of digital signatures.

Digital currencies and bitcoin are not very popular among people. People need to study about Bitcoin, before using them. The price of one Bitcoin fluctuates according to their market. There is no fixed value for one Bitcoin [8].

C. Flattr

It is similar to the Facebook like and Twitter favorite, users can use this Flattr service to give micro donations [9]. First we have to prepay an amount to Flattr account. Then decide how much we are going to donate for each month. Then go to your favorite sites and click the Flattr button as you wish.

After a month, Flattr divide your monthly subscription amount by number of clicks and send the amount to merchants according to the clicks. It is easy to use and transaction cost is low because of money transaction occur each month.

III. Methodology

A. User Bank Interaction

Here the user will go to the banking system and get registered. While registering, the user have to choose whether he is a reader or newspaper site. When he logged into the system, he will be provided a page where he can add more details to his profile as an user or newspaper industry.

Apart from the profile page, he can buy tokens to use in the newspaper. The tokens have the value of 1. If he buy for Rs.100, he will get 100 tokens. When creating an user account the bank's database will store username and password of the user and the amount he spent. In addition to that, bank will create a key. The key consists the concatenation of user's password and a random number which is hashed by M times. M is the amount user spent on his token purchase.

As soon as the key generated, bank will now transfer the user's username, total amount of tokens, the random number and the key. Now, the bank will go offline.

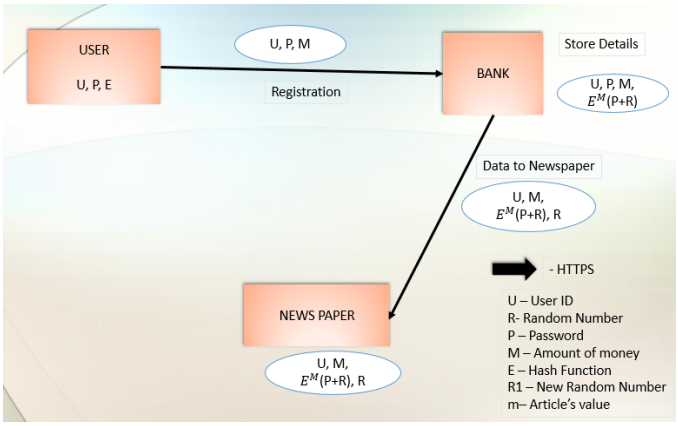

Fig. 1. User Bank Authentication

B. User Newspaper Interaction

Now the user will go to the newspaper site and he will see an integrated button form bank on every article with its price. When he click that, he will be asked to login to the system. A logged user now can read the article by clicking the button. Now the user is the client and newspaper is the server.

Now, the server will send the current amount of tokens and the random number received from bank. Since, client side have the user password, it will concatenate the random number with its password and hash it by the (M-m) times. M - the total amount, m - the article's cost. So, the newspaper now can get the new key and hash it by m times and check it with the key it already had.

Also, the client will send a new random number, new key with the new random number to the newspaper for next transactions. The procedure will go like this for future transactions.

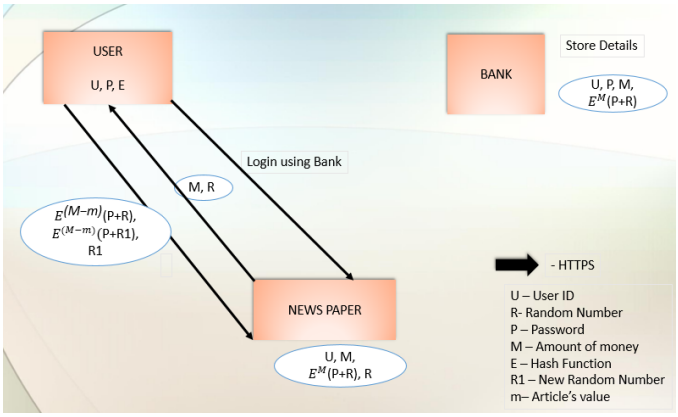

Fig. 2. User Newspaper Authentication

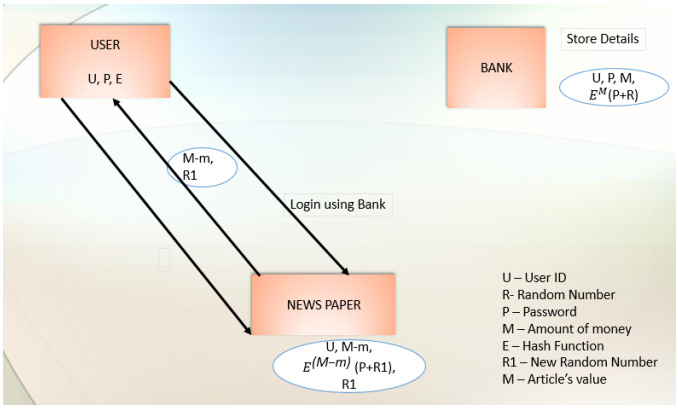

Fig. 3. After First Transaction

When the amount stored in newspaper under a user's account goes to zero, the site will inform the user to buy some

new tokens to spend. Then only the bank will come again to the scene. In the mean time it will remain offline.

IV. Implementation

A. User Bank Interaction

This is the part where the real money transaction happens, therefore we made this interaction more secure. To develop the website of banking system we used, CodeIgniter framework. It has some secure database connection and it won't allow the third parties to view the internal page structure of the project.

In user registration process, we have an indicator to show the strength of the user password. We encourage our users to use strong passwords. We have a human verification Re-Captcha to prevent brute force attacks and email verification to check the user is using a valid email. Only after the email is verified user can login to our system, otherwise he will get an error in login page.

After the user logged in, he will be redirected to a mobile verification process which is optional. User can add it if he wants the transaction to be more secure. If he skip this, he will be asked to do every time he logs in.

Mobile verification is similar to Google verification. The user will be asked to enter his number, and then he will be asked to send a request message for the verify code. Then the system will send the very code to his mobile and he will use it to authenticate himself. For this process, we used Dialog's Ideamart [10] platform.

Now the user is logged in and can buy tokens by providing his payment way to the bank and the amount of tokens. Once he bought the tokens, the detail set of username, amount of tokens, a random number and the key will be transferred to the newspaper. Now the bank will go offline.

B. User Newspaper Interaction

This part is now under implementation process. An e-paper will be shown to the user, where the heading of the article will be in a readable font size and the body will be in very tiny letters. The article body will have a button with the price of article. When user click the button, there will be a popup with login form. Here user have to produce the login credentials he used in the banking system.

Now the user can see his current balance of tokens and he can read the contents now. The details of user credentials, account balance and the new key generations will be handled by AJAX and JQuery.

V. Conclusion

In this project, we have created a secure micropayment scheme for newspaper and magazine industries. The scheme is to reduce the subscription fees and encourage users to pay per article. Up to now in the project, user-bank authentication and a dummy news paper site with integrated read button have been created. newspaper-bank and user-newspaper interaction and authentication are still to be implemented.

Acknowledgment

We would like to thank is Dr. Suneth Namal Karunarathna, who gave us some good advice in using HTTPS protocol and secure network connections.

References

[1] M. Sandirigama, A. Shimizu, and M. Noda, "Simple And Secure Coin(sas-coin) - A practical micropayment system," IEICE Transactions, December 2000.

[2] ——, "Simple And Secure Password Authentication Protocol(sas)," IEICE Transactions, 2000.

[3] Wikipedia. (2014, April) Micropayment. [Online]. Available: http://en.wikipedia.org/wiki/Micropayment

[4] L. Gitman and C. McDaniel, *The Future of Business: The Essentials*. Cengage Learning, 2007.

[5] D. E. Neuts. (2015, July) Micropayments: The hot, new way to pay for digital content. [Online]. Available: http://www.subscriptioninsider.com/public/Micropayments-The-Hot-New-Way-to-Pay-for-Digital-Content.cfm

[6] R. Parhonyi, L. J. Nieuwenhuis, and A. Pras, "Second generation micropayment systems: lessons learned," in *Proceedings of the Fifth IFIP conference on e-Commerce, e-Business, and e-Government, I3E 2005*, Springer, 2005.

[7] S. Gallagher. (2009, October) Transaction costs table for paypal micropayments. [Online]. Available: http://pressbin.com/tools/paypal_micropayments/

[8] CoinReport. (2014, February) What are the advantages and disadvantages of bitcoin? [Online]. Available: https://coinreport.net/coin-101/advantages-and-disadvantages-of-bitcoin/

[9] S. Ltd. Flattr vs paypal. [Online]. Available: https://www.similartech.com/compare/flattr-vs-paypal/

[10] Dialog. (2015) Ideamart-free app builder. [Online]. Available: https://www.dialog.lk/mobile-miscellaneous-idea-mart/