NagASTHRA - A New Look to e-Security

Abstract :

One of the often-cited reasons why B2C e-commerce has not taken off as opposed to its potential, is the lack of trust the consumers have on the security aspect of current payment mechanisms. The common apprehension that a consumer today has is the possibility of *misuse of information*, an issue that is not addressed by the prevailing payment methods. At the same time, the merchants and the banks are dithering to take a plunge because of uncertainties of remittances owing to repudiation/refusal of the consumers regarding the orders in question, and the charge backs ensuing thereof.

There are other reasons, though, which contribute to the stunted growth of e-commerce. They are the meager PC penetration and the lack of internet-literacy. A growing marketplace constricted by absence of patron! A possible workaround to this access-based limitation is to use intermediaries, who offer to combat these limitations by providing their own infrastructure to facilitate e-commerce (by receiving orders over other access media like the telephone and doing intelligent comparisons/searches) and placing the orders on the e-merchants. But again, in the current scheme of things, the payment information will have to pass through these intermediaries, an intimidating prospect which hinders the proliferation in such an approach.

To counter these impediments, there is a need to revisit the basics of card-based payment system, identify the inherent shortcomings, and propose a workable alternative. This paper discusses a new payment model, which provides the user with control of when, with whom, for what and for how long the card can be used. This is proposed to be accomplished by a two pronged approach. Addition of business level security layer in the existing mechanism and execution of this security through a simple process of authentication.

Concept:

Conceptually, this would be accomplished by the division of, what is referred to here as the business security layer, into two parts. The first part, is the virtual credit card number, which is made available to the restricted entities (Order Help Desk and/or Family members and friends) as identified by the credit card owner. The other part is called the d-PIN (Device PIN) that is known to, and used only by the card owner for authorizing the transaction. The implications of such a division of business layer and the ability to share the virtual credit card number with restricted entities will translate into various business models when it comes to implementation, each of which is also discussed.

Setup:

The new setup would entail the credit/debit card owner to establish two codes with his Bank. A user configurable (flexible and sharable) virtual credit card number and d-PIN. Both these can be changed/configured at the bank site by the user at any point of time. The advantage of this flexibility is that it vests lot of authority with the user in terms of reconfiguring the card codes at any point of time without going into the loop of intimating all the participants in the payment system. The benefits of this approach will become clearer as we unravel the system.

Process:

This virtual credit card number is a mapping of the credit card number only, not any other detail, which will be shared by the user with Order HelpDesk/Family Members/Friends, referred to **proxy buyer** hereafter, till we discuss the ramifications of sharing it with other players respectively. Once the user shares this virtual credit card number with the proxy buyer, the proxy buyer can place an order on the half of mPayee (Real Buyer) using his own resources. The proxy buyer searches the net and finds the best merchandise deal meeting the mPayee needs. When it comes to payment, he would enter the virtual credit card number to get the first level authorization from the bank. At the bank, the virtual card code supplied by the proxy buyer is compared with valid card code maintained by the user. If the authorization is successful, the bank will send the details of the order to user's handheld device (the number of the handheld device is also maintained on the bank's database). This is then ratified /authenticated by the user by keying in the d-PIN into the handheld device, confirming/authorizing the order.

1. Introduction

A simple analysis of the present e-commerce statistics, we can pinpoint the deficiencies in the e-commerce set-up, that are arresting its growth. At the same time, the analysis will provide rich insights into requirements, which may catalyze the growth:

- **63%** of web surfers will not purchase over the internet until they are assured of more human interaction (Lack of Personal Touch) (Source: Forrester Group)

  *If somehow, the order is placed through "familiar" intermediaries who can act as **proxy buyer** (Help Desk) or through a more "personal" interaction (by telephone) and the buyer has the last say in approving the order, then such a system will bring in a great deal of reassurance for the buyer*

- **2/3** of all online shopping carts are abandoned before checkout (Waste of Time due to a poorly designed site, Leap of Faith!). (Source: Forrester group). This is because when it comes to finally disclosing the card details, most people balk.

  If somehow, there is a system wherein the buyer just needs tell what he needs to buy and let an proxy buyer do the searching/analysis/comparisons then the buyer will save a lot of time.

  More importantly, if the buyer is assured that he is, at no point in time, exposing his credit card details to the proxy buyer, his apprehensions will be mitigated to a great extent, that he retains the right to say NO to the transaction at any point of time, then .

- At present there are approximately 3.8 million credit cards in India, according to a report in The Hindu (March 15, 2000). So, if my son does not have a credit card, he cannot do Internet based shopping or benefit from Internet based services (booking a room in the hotel, which requires verification of creditworthiness). But if he could use my credit card number, he would be able to do e-commerce and provide the much-needed impetus to e-commerce [a whole new population is good spending power gets added]. But I stand a risk of him misusing my card. I need to be reassured that my card is not misused for some other purpose, which it was not intended for.

  But if the new system ensures that the card is being used for the intended use, by alerting me every time some payment is requested to be made from the card, and giving me the authority to say yes or no to the transaction, then I will have no hassle in giving my credit card information to my son.

- **85%** of online households have only 1 phone line so they can't call and be on the site at the same time (Lack of Infrastructure)

Can we somehow bring-down /remove the time spent on the site and therefore cut down the total transaction time?

- Most selling items on the net are **Books, Software, Music, Stationary** items, which have discreet identification attributes and makes NO difference if someone else buys the item on behalf of the customer.

  These sales in these categories can be subjected to easy surrogate buying!

- The credit card is required not only for the purchase but also as an age proof (entry into Spam sites!). Again, since these Spam sites store this information in their servers, and allocate you a username and password (for entry and for billing you for the use of the content), and there are common instances of the username and passwords getting hacked, (and proudly put up on hacker sites), parting with information is risky. Someone would be using your the username password and surfing the site and you get billed!!

  Even if the site gets hacked, whenever a request for payment is made, the owner for the credit card must be intimated and requested to own the responsibility for the transaction

The crux of the above analysis is that presence of proxy buying, can help e-commerce take off. Also, the credit card owner needs a lot of reassurance that his card is not getting misused.

But proxy buying in today's context is fraught with dangers, which are inherent in the current payment models. Proxy buying in today's context would mean parting with your credit/debit card details, which is the major point of contention of the consumers. This arises due to fear and risk involved in the misuse of Credit Card.

2. How about Giving Business Level Security to Credit Card Payments?

As it flows from the discussion, there is a felt need for a mechanism wherein the user gets alerted whenever there is a money transaction request relating to the card. This is the much-required Business Level Security Layer for payment scenario that this paper seeks to propose.

To understand what is business level security layer, let us try to understand the Internet based security concepts. Basically, there are two levels of security on the net, i.e. one at Business Level (fulfilled by login and password, which establishes your unique identity) and other at transportation level (fulfilled by SSL-Secure Socket Layer, which prevents the manipulation of the data when it is floating through the net).

The irony, which stares in our face, is this lack of implementation of this very understanding for e-commerce. While we find the use of the business level security layer in many applications on the net, surprisingly, we find that the same business level security layer is absent when it comes to payments on the net through credit card.

Since there is no mechanism today which asks us to establish our identity at the time of the use of the card, this is reason enough of our being at peril if someone knows our credit card details.

But if this is so simple, why don't we apply this understanding quickly in the payment mechanisms. So why not apply the same understanding of business level security as done by, say mail servers (remember Yahoo asking for your email id and password before letting you see your mails!) directly on to the credit card transactions.

This is because a direct mapping of user name and password mechanism similar to the sites like Hotmail and yahoo mail will not be possible for the payments. Why? Because the architecture, entities, flow of information and dependencies/interactions are different in each.

In Yahoo mail, primarily, only two machines are involved: One is the server on which the mail contents and the highly sensitive DATABASE of user information reside and other is the client machine, which we use to connect to that server. The client machine can be different each time (as I can access the mail from any computer), but the server machine is always the same or in some special circumstances, can be an authorized machine which has access to the central database machine. (But strictly maintained by Yahoo only.

In contrast, in the payment scenario, there are four entities. A client machine, an e-shop, a payment processor and a bank. During a transaction, the information flows from the client (the buyer) to the e-shop, then on to the payment processor and then to the bank. That is, during this flow, the credit card information would pass through the client

machine, the hosting environment of the e-merchant, the payment processor servers and finally to the bank.

If we do a comparison with the simple mail server kind of architecture and the information flow that we discussed, we see that in the case of a payment transaction, the first three, viz., the client machine can change (needs no explanation!), the e-shop machine can change (since the user can go to any shop to buy a product or a service) and payment processor may change (an e-shop may have tie-ups with more than one payment processor). But, the fourth entity, the Bank does not change, since the transaction authorization has to happen at the DATABASE of the acquiring bank.

We saw that the client, today, can only pass-on the card information to e-shop, e-shop in turn talks to the payment processor, which in turn contacts the card-issuing bank through the payment network (Visa/Master Card Network). The Credit card issuing banks will always be requested for the approval for a payment. But, today, the biggest lacuna is that the client has no direct access to the bank **while** approval request is made to the bank.

For operational and reasons which are fundamental to the transaction payment scenario (Read Trust), there CAN BE NO CENTRAL DATABASE, which is accessible to all the machines. Therefore, in no condition can there be a possibility of the information flowing between any/only two machines as is the case in a simple web mail application. (And therefore we see that the business layer concept implementation is difficult to implement.). Except that, in various scenarios there could be possibilities of the central database residing with the payment processor or with a new service provider entity which performs the similar role of the bank, even though this would be a sub-optimal solution.

The challenge is to implement login mechanism (business layer) for this kind of many computers (e-shop computer, payment processor, and card issuing bank) interactions. The various ways in, which the CENRAL DATBASE EXISTS and the security layer gets integrated, are as follows:

Variations:

Case 1: The login mechanism gets directly integrated with the issuing bank in question, that is the user wishes (and the bank agrees!) to share the information with the issuing bank directly, MEANING THEREBY THAT THE BANK ACTS AS THE CENTRAL DATABASE. This will not call for any major changes in the software systems at the e-shop level or the processor level.

Case 2: The login mechanism gets integrated at Payment Process level (VISA or Master Card Network), which means the Payment Processor acts as the CENTRAL DATABSE. In this scenario, user needs to register with each payment processor. No changes required at the bank but minor changes at processor and e-shop configurations will be required.

Case 3: It can be provided as general service, which can be used either by Card Network or Bank by installing the integration software. User needs to register only with the payment service provider who acts as the CENTRAL DATABASE.

Value added features of such a Mechanism:

1. This new mechanism will extend well beyond the realm of on-line payments. It can find wide acceptance in the off-line payments market as well.

2. Not only for Credit card payment but also Debit card a/c transfer payments. Virtual Card can be mapped either to account number/Credit Card or debit card number etc..

The solution framework, would therefore need that an approval request is fired to the user, whenever an authorization request is received by the CENTAL DATABASE. This can be conveniently achieved by sending the approval request to the credit card owner through a handheld device.

3. The Solution (Using WAP as Technology)

WAP technology is rapidly overshadowing the other Internet related technologies. This is because of the facility it provides by means of easy access to the Internet via any mobile device. This feature of WAP can be exploited to enable WAP enabled cellular phone users to conduct commercial transactions on the Internet, thus entirely eliminating the computer.

As per the new model, the end user who pay's for the goods purchased will be referred to as mPayee. The person/s who will assist him will be called as Order Help Desk. We are discussing the first scenario where the bank holds the CENTRAL DATABASE

Each of the mPayee will have a Virtual Card Number and d-PIN, which he gets by the registering with Card issuing Bank. The mPayee can distribute his Virtual Card to the Order Help Desk who will follow the existing method to place an order. The only difference is that the Order Help Desk will have to enter the Virtual Card instead of the credit card number.

Unlike the current payment gateway, the payment will not be approved on the basis of the Credit card information alone. Even though it appears to the Order Help Desk that his order is being processed directly, the back end processing seeks the approval of the mPayee as described below.

Based on the Virtual Card Number, the payment gateway sends an alert to the corresponding mPayee's WAP phone. The mPayee has to enter his d-PIN to view the pending orders. On authentication of the d-PIN only will one be able to view details such as items being purchased, shipping address and amount to be paid. Based on this information one can either Pay or Decline the Payment. Accordingly the Payment gateway will permit or deny the payment. The final status is intimated to the Order Help Desk and the transaction is completed.

The service given above describes how an asynchronous transaction between people at different locations can be conducted, synchronously by using the "WAP Alerts" technology. This service would go a long way in allaying the fears in the minds of the people regarding e-payments and encourage purchasing on the Internet.

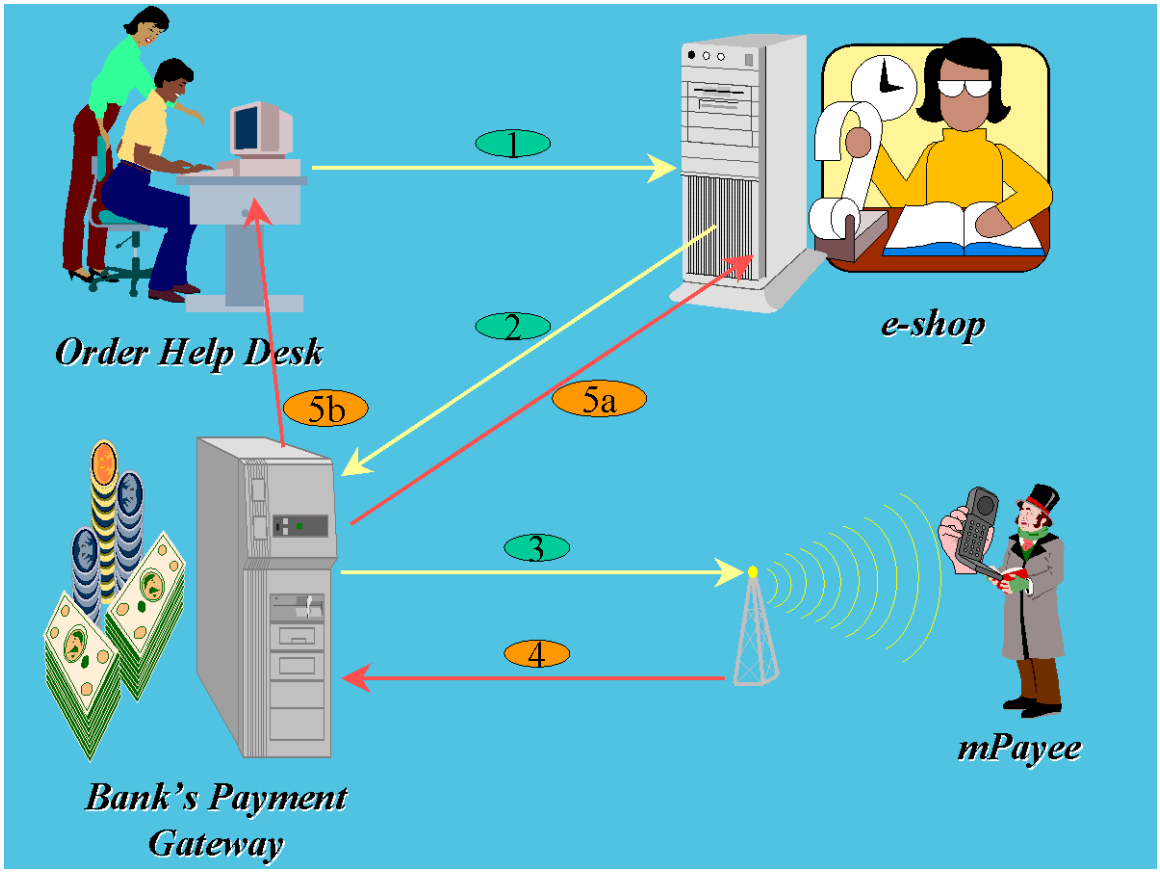

Fig: Proposed e-commerce model

1. mPayee (Real Customer) would call the order help desk and orally share what kind of goods he wishes to purchase and shares the Virtual Card Number.
2. Order Help Desk (Virtual Customer, Proxy Buyer) placing an order using the mPayees Virtual Card Number
3. e-shop taking the approval from the Issuing Bank Payment Gateway
4. Issuing Bank Payment gateway sending an alert to mPayee's WAP phone
5. mPayee's taking decision on the Pending Order
6. Issuing Bank Payment gateway providing the, Payment status to both, the e-shop and the Order Help desk

Advantages:

1. Novice can shop (Digital Civilization is not a necessity)
2. Commerce without surfing as opposed to single click buy
3. No need to have a separate dependent card for the family, as each user can register for more than one Virtual Card Number.
4. No fear that the e-Shop would charge the user every month
5. Order anything from anywhere taking anyone's help (just a phone call away) and still have full control on your e-payments.

6. Valid period for payments can be enforced, by the concept of volatile Virtual Card Numbers.
7. Credit Card can be used as guarantees e.g. age proof .

About the author

Raja Nagendra Kumar (nagendra_r@satyam-infoway.com) is working as **Technical Manager** at **Satyam Infoway**, Bangalore. He has 9 Years of experience, out which $4^1/_2$ years in Java, he holds M.E from Anna University, Chennai, India and B.Tech (Mechanical) from K.S.R.M College of Engg, A.P, India. Master Java 2 Programmer certificate from Brain Bench. He has won the First Prize at WWW.WAPHOTHOUSE.COM contest conducted by NOKIA in the year 2000. Nagendra would like to thank his colleagues **Biplove Belwal, Surekh**, **Annapoorna and Alok Jain** for supporting his efforts to write this article and **Prabhakar Ravoori** for providing a environment for excellence.