Journal of Mobile, Embedded and Distributed Systems, vol. VI, no. 4, 2014
ISSN 2067 – 4074

# Security in Electronic Payment Systems

**Roxana TURCU**
*IT&C Security Master*
*Department of Economic Informatics and Cybernetics*
*The Bucharest University of Economic Studies*
*ROMANIA*
*turcuroxana90@gmail.com*

***Abstract:*** The payment security becomes fundamental in our days. Based on this statement I have decided to deepen this subject and to study the online payment systems and the connection between them. I have observed that this area becomes the hackers' attraction and I have realized how important the security of the ecommerce is. Also I have done a research of the possible attacks and I have searched for the countermeasures of this attacks. The result of my research is my payment gateway solution presented in the following lines.

***Key-Words:*** Payment Gateway, Security, Ecommerce, .NET, Credit Card, Provider, Payment, PayPal

## 1. Introduction

As we can see the present and the future of the informatics world will be the ecommerce. Day by day appears on the internet many businesses that are based on the sale of services or/and products. Of course this fact is benefic to us thanks to the ecommerce advantages, but also we should know the risks of online payments.
When we say ecommerce we say the process of buying and selling products / services over electronic system such as the Internet or another computer networks. But also any form of business transaction conducted over the Internet is ecommerce, such as online shopping, electronic payments, online auctions, internet banking and online ticketing.
In the last century the ecommerce has grown so fast thanks to various advantages that it brings. The facts that it eliminates limitations of time and geographical distance and also that it reduces the costs are the main benefits.
Another advantage of ecommerce can be the online payment because the checks and the currency notes are removed, but this part brings a lot of risks like our personal sensitive data safety. And that is where payment providers and payment gateways come into the picture.

## 2. Online payment systems

An online payment system facilitates the acceptance of electronic payment for online transactions. This system includes all the solutions who are taking part of the payment accomplishment, such as payment gateways solutions, payment providers, payment processors.

### 2.1 Payment Gateway

A payment gateway is an interface between the client and the merchant banks and/or payment providers. His purpose is to authenticate and automate electronic payments made by shoppers. A payment gateway has the following roles: to process a transaction securely, to verify the client identification, to validate the card information and to accept or to reject the transaction. In other words it is the middleman between the bank/payment processor and the merchant.
Regarding the location of the transaction processing code, there exists two types of payment gateways: merchant Side API and A secure order form. In the first type the transaction processing takes place on the merchant's server. For the second type, the customer is redirected to the website of the payment gateway and after the transaction is processed, the customer is returned to merchant site.

## 2.2 Differences between Payment Provider, Payment Processors and Payment Gateway

A payment provider (PSP) offers services for accepting electronic payments by a variety of payment methods like credit card, bank-based payments such as direct debit, bank transfer and real-time bank transfer based on online banking.
This term is close to the payment gateway, but it has more responsibilities than a payment gateway. Besides the offered transaction security, it can connect to multiple acquiring banks, cards and payment networks and fully manage this connections. Furthermore a PSP can offer fraud protection, risk management services for card, fund remittance, transaction payment matching, reporting. Some Payment Providers can process other future payment systems such as wallets, prepaid cards or vouchers, cash payments.
Another term very used in online payment systems is the payment processor. It has the role to handle the credit card transactions for merchant acquiring banks. There exits two types of payment processors: front-end and back-end.
The front-end processors communicate with card associations and supply the authorization status and the settlement services to the merchant's bank. The back-end processors take the settlements from front-end processor and move the money from the issuing bank to the merchant bank, with The Federal Reserve Bank.
Usually the payment processors communicates with payment gateways for sending to the customer the status of transaction and other information.

## 2.3 Online payment system solutions

Below I will introduce the most used payment system solutions for processing and securing the online transactions.
One of the most used payment acquirer is PayPal, who in 2011 processed over $4 billion in payments. The payments are made using users PayPal accounts. It is distinguished by the others acquirers through the feature that allows its users to send money through the service.
The PayPal concurrent on the market is Google Checkout. The payments can be done through an account connected to users Google profile.
Another direct competitor to PayPal is Dwolla who is processing over $1 million per day. The processing procedure is identical to PayPal, but its name is not so known like PayPal.
Another important payment provider is CyberSource who process online payments, simplify the payment security and streamline online fraud management. The most important information is that in 2007 the most widely used payment gateway, Authorized.Net, was acquired by CyberSource.
An excellent payment solution for web developers can be Stripe who integrates a payment system using Stripe's API. It handles all PCI compliance and merchant approval.
Another payment processor that unify a payment gateway and a merchant account into one is 2Checkout. It offers shopping cart stores and allows customers to receive credit card payments and PayPal payments.
Also on the market exists payment system solutions who allow merchants to accept credit card payments through their mobile devices like Square and Intuit's GoPayment.
As we can see the e-payment market offers a multitude of solutions aimed to protect, secure and process our payments.

# 3. Ecommerce Security

Annually billions online transactions are made over the Internet. A transaction involves the use of sensitive data such as credit card information. With this information the bank account can be accessed and an unprotected transaction can leave a huge open door to the bank account to the bunglers. This means a possibility of a large number of attacks.
The ecommerce security is a part of

ISSN 2067 – 4074

information security and has the role to provide the protection of the sensitive account data from possible attacks.
Below I will present the most common ecommerce attacks and some countermeasure of the ecommerce attacks.

## 3.1 Ecommerce Attacks

The ecommerce attacks can be divided in the following categories:

- Intellectual property threats. This category can contain the using of existing assets found on the Internet without owner permission such as software pirating, cybersquatting (domain name).
- Client computer threats. The client computer can be infested with Trojan horse, Viruses, and Active contents.
- Communication channel threats. Between the client and the payment processors can appear a lot of threats like sniffer program, backdoor, spoofing, denial-of-service. The most used practices of the hackers are the Denial of Service, where through the server is overloaded with a large number of automatic requests. This practice can slow down the server or worst, to block the server. Another dangerous attack can be the Phishing. Some hackers build websites who looks exactly like ecommerce websites and try to invite the people to use those websites. With this method is very easy to access the sensitive data like credit card information.
- Server threats. Also on the server we aren't so protected because can be some threats like privilege settings, SSI (Server Site Include), CGI (Common Gateway Interface), File transfer, Spamming, Malware.
- The malware attacks are very dangerous for the ecommerce website servers because they can execute actions such as downloading software without permission.

## 3.2 Ecommerce Security Features

As we can see there are a lot of threats that can attack our payment systems, but also there are a lot of countermeasures.

- Intellectual property protection. Our assets can be protected from intellectual property attacks using Legislature and Authentication.
- Client computer protection. Some known security features against client computer threats can be: Digital certificates, Browser protection, Antivirus software, Cookie blockers and Computer forensics expert.
- Communication channel protection. The communication channel is the most exposed to the ecommerce threats and the encryption techniques, the usage of SSL and S-HTTP protocols, the digital signature availability can be the attack countermeasures.
- Server protection. To protect the server it is necessary to control the user's access and implement the authentication. And also very important is the firewall presence.

# 4. Description of Payment Gateway Solution

Because of importance of ecommerce security I have decided to develop a payment gateway solution, designed to communicate with the shops, to secure and validate the sensitive data and send them to payment providers for finalizing the payment.
To get a clear view of payment system communication I have built an online shop and also I have simulated a payment provider who will communicate with my payment gateway solution.

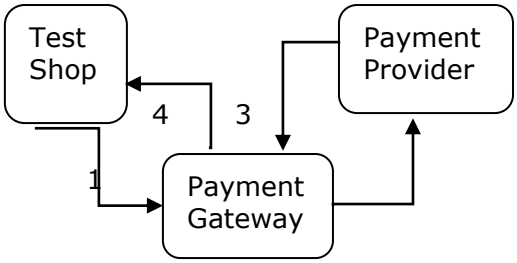


*Figure 1. Payment System model*

1. The user of the shop does a checkout of the products that he wants to order, he will complete the shipping address and the credit card information and he will submit the order. The completed data is encrypted and send to the payment gateway solution.
2. The Payment Gateway solution will decrypt the data, will validate them and if the result of the validation is ok the data will be send to the payment provider. If the result of the validation is not ok, the payment gateway solution will send the response to the shop.
3. The payment provider will validate and process the transaction and will send a response to the payment gateway.
4. The payment gateway will send the response from the payment provider to the shop.

## 4.1 The client application design

The Test Shop is a web application, built using ASP.NET MVC Framework and it contains a login system, a shop page, a user information page and a payment page.

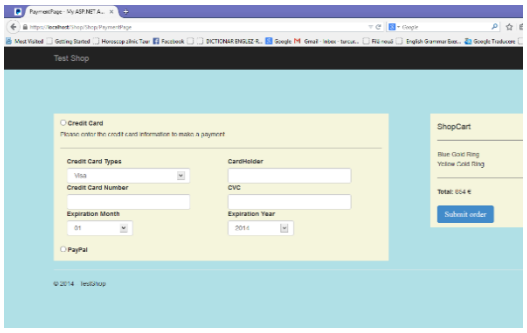

*Figure 2. Payment Page*

Because of the sensitive data usage the data is send over HTTPS protocol who provide the data protection.

The shop page can be accessed only by the users who have an account created because the shop contains also a page with transactions history and status of the transactions made by the user. If a user doesn't have an account, he has the possibility to create one.

The client side is built with new generation technologies such as HTML 5, JQuery and Bootstrap. The server side is developed using C# programming language and for the communication with the database I used EntityFramework.

## 4.2 The architecture of Payment gateway solution

My payment gateway solution is a .NET application, developed with C# programming language. Its objective is to validate the data received from the shops and communicate with the PSPs.

The communication with the shops is made by a web service using WCF. The access of the service can be made with an username and a password that the customers will know.

The interface of the service shows the following methods: Authorize, Refund, Capture, Cancel and GetTransactionInfo. This interface can be updated in time when will be implemented another methods.

Using Authorize method, the shops will send to the payment gateway solution the encrypted data. The payment gateway will decrypt the data and will save the payment in the database. After the save process will be generated a PaymentToken. To complete the authorize process, the payment gateway will validate the data.

Firstly, it will check in the database if the current merchant can perform a payment with the sent currency in the selected country.

Secondly, it will validate the sensitive data. The payment gateway will check if the sensitive data are not empty, the credit card is not expired, the credit card number correspond with the format of VISA/MasterCard/ AMEX card number,

ISSN 2067 – 4074

also the same thing for CVC number.
If the validation process is successful the data will be sent to the payment provider.
At this moment my payment gateway communicates with a simulated payment provider and also with PayPal.
The communication between the payment gateway solution and the simulated payment provider will be made using the XML.
The payment provider will send a response which contains the transaction status, a Boolean value and also an error message in case of the payment failure.
After the payment provider response, the payment gateway will save in the database the transaction with the proper status and the corresponding PaymentToken. This save process will generate a TransactionToken. The Shop will receive the response of the transaction which contains the TransactionToken, the Boolean value if the transaction was successful authorize and the message error in case of failure.
The Capture process can be made by accessing Capture method from service interface. It is necessary that the transaction have the authorized status to do capture on transaction.
To cancel the transaction it is necessary that the status of the transaction is Authorize. This method can be accessed from service interface.
The Refund method has the role to return the captured money or a part of them. This operation can be made only for captured transactions.
All these methods will return the same fields on response: the TransactionToken, if the method was processed successfully and the error message.
The GetTransactionInfo method will return to the shop the information for the TransactionToken sent by the shop.

### 4.2.1 PayPal Integration

The Payment Gateway solution is integrated also with PayPal, bringing an advantage to my payment gateway because this is the most used acquirer in the world. The payment gateway solution is integrated with PayPal using REST API.

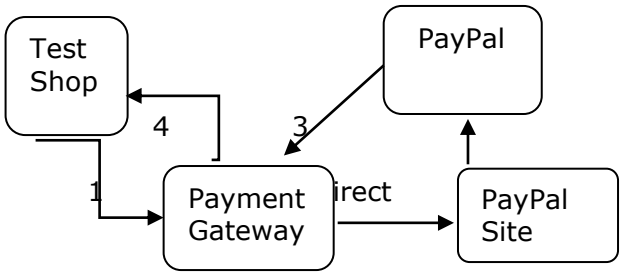


*Figure 3. Payment System with PayPal*

1. The user from the Shop selects to pay with PayPal. He will make an authorized request to my payment gateway.
2. The payment gateway will check which payment type was selected to pay and will validate if the user is authorized to pay with the selected payment method. If the validate is true the user will be redirect to the PayPal page.
3. PayPal will process the payment and will send to the payment gateway a response with the status transaction.
4. The user will be redirect to the shop page and will receive the status of his transaction.

## 4.3 Databases design

For improving the security of the system, the payment gateway has three databases: AdminSettings, Payments and Transactions. The AdminSettings database has a table who contains sensitive information about the merchants such as the private key decryption, the payment matrix (currency-country), the payment types supported. The access of this database can be done with a user and a password.
The Payments database contains the sensitive data of the users and also information about the order. Like AdminSettings, this database can be accessed only by the users who know the user and the password.
The Transactions database contains information about the transactions such as transaction status, the created date, the message from the PSP.

### 4.4 The Implementation of the security system

To avoid a loss of sensitive data between shop and payment gateway, the data are encrypted in the shop using RSA algorithm.
In the payment gateway the data are decrypted with the private key stored in the database.
The shop use HTTPS protocol for a secure payment, and also for the password verification from login page it is used MD5 hash algorithm.
The databases are protected by username and password.

## 5. Conclusion

The payment security becomes fundamental in our days and this article supports this statement. I have exposed the possible e-commerce attacks of a payment system and it is observed that there are a lot of them. So it is very important to know your future system enemies before to develop it. I have introduced my payment gateway system who represent a solution against the existing threats and who can also be integrated with another payment gateways. This solution can be forwards expended by implementing new payment methods and be integrated with another payment providers/processors.

## Acknowledgement

Parts of this paper were presented at The 7th International Conference on Security for Information Technology and Communications (SECITC 2014), Bucharest, Romania, 12-13 June 2014.

## References

[1] Mehdi Khosrow-Pour, E-Commerce Security Advice from Experts, CyberTech Publishing, 2004, pp. 122-135
[2] Vesna Hassler, Security Fundamentals for E-Commerce, Artech House, 2001, pp. 67-79
[3] Jean D Habiyaremye, Jules Miller, E-Commerce Security Threats, GRIN Verlag, 2013, pp. 53-70
[4] Adam Freeman, Allen Jones, Programming .Net Security, O'REILLY, 2003