On the Security of e-commerce

RADUCANU RAZVAN
Department of Mathematics
“Al. I. Cuza” University
Bulevardul Carol I, Nr.11, 700506, Iasi
ROMANIA
razvan@uaic.ro http://www.rraducanu.ro

OMUSORU EDUARD
Edline Design
ROMANIA
eduard@edline.eu http://www.edline.eu

Abstract: - This work has been created as a short guide on e-commerce, offering indications on problems often encountered in this process. It discusses the most attacked places in your commerce platform and the best solutions that can prevent issues in this activity.

Key-Words: - e-commerce, risk assessment, threats, security solutions

1 Introduction
The commerce is an act of trade defined by a relation between two parts. This relation is negotiated and has a set of conditions, mutually accepted, so that the both parties are satisfied. The “electronic commerce” or the “e-commerce” refers to all commercial transactions in which one or more stages are processed electronically. These stages can be: advertising and promotion of products, selection, ordering, payment, delivery or use of products. Also, as the traditionally commerce these stages are defined by the type of them, like: B2B (business to business), B2C (business to consumer), C2C (consumer to consumer). The structure of the transactions is developed by the following 4 steps:

a. Pre – sales who provides information about the products through catalogs, specifications, prices, overviews of clients;
b. Agreement of terms from the trade contract or insurance policies who makes refers to the prices, discounts, delivery methods, terms of payment, warranties, risk and others conditions;
c. Settlement is represented by the fulfilling the agreements and includes the exchange of payment and completing the delivery logistic;
d. Post – sales provides additional information such as products upgrades, services and warranty terms.

2 Risk assessment
Any company, before developing a e-commerce platform, should stop a moment and take an overview on the service-side problems, transaction problems, client-side problems and legal and regulatory problems which may appear in the transactions.

2.1 Service - side problems
An organization infrastructure for supporting an e-commerce service must have two main elements. The first is an e-commerce front – end represented in generally by one or more web servers connected to the Internet and the second is a back – end system who supplies information in the front – end systems (products information’s and stock holding) and as well to extract information’s from them (such as orders for transferring to logistics systems and payments to be cleared through third parties).

2.2 Transaction issues
Transactions between buyers and sellers in e-commerce can include requests for information, quotation of prices, placement of orders and payment, and after sales services. The high degree of confidence needed in the authenticity, confidentiality and time delivery such as transactions can be difficult to maintain where they are exchanged over an untrusted public network such as the Internet.

One of the main threats in e-commerce transactions is the loss of confidentiality of the transmitted data, for example through interception of the communication. In particular, passwords used to obtain authentication or other confidential data such as the originator, recipient, amount of the payment etc. can be intercepted. Another threat of e-commerce transactions is the loss of integrity of the transmitted data, for example, due to bit errors which are attributable to technical defects, or are the result of intentional manipulations. In this case, payment amounts or recipients of payments can be manipulated so that a third part benefits financially. A third threat that we remind here is the loss of availability of transaction data; This problem could be due to force
major such as a network failure, network interruption or transmission error, or it could be the result of deliberate manipulation by third parts. Another one is the release of sensitive information due to unauthorized access to systems, so that sensitive information like passwords can be intercepted during transactions. The replay of old transaction data is a threat too; for example, an attempt could be made to repeat a payment by copying the data and reusing it. Unrecoverable costs incurred in fulfilling the order, might happen when a client denies a payment of a certain agreed value. In the masquerade threat, a perpetrator could pretend to be a particular vendor and divert the payment to his own benefit. But the customer himself could assume a false identity and make an invalid payment which the dealer would not actually receive. A frequently met threat is the fraud; for example, instead of attempting to manipulate an existing WWW server, a perpetrator can create his own website on the Internet and design it in such a way that visitors have the impression of being connected with an established, reputable institution. A perpetrator can also attempt to pass himself to vendors as a respectable customer even though he is not solvent.

2.3 Client – side issues
One of the most important component of the e – commerce application is the computer (or other device) used by the customers. In most cases, the client environment is outside the direct control of those who offers the e – commerce services. This distinguishes e – commerce from traditional business applications where organizations can often specify the software, hardware and configuration details of the client environments. The loss of sensitive information could be due to the unauthorized access to systems. Sensitive information like passwords could be stored on an insecure client PC and disclosed inappropriately. The loss of customers could be due to the impossibility of clients to use the service with their browsers. Many ecommerce systems make use of certain plug-ins, which might not be available to all browsers or could include malicious compatibilities. Loss of revenue refers to users that are unable to access the system. Some users are blocking cookies or active (Java, JavaScript and ActiveX) content which might contain malicious code and this might prevent the users to access the ecommerce system.

2.4 Legal and regulatory problems
The legal and regulatory framework for international e – commerce is an area of wide debate and covers areas outside the scope of this report, such as taxation, consumer protection and jurisdiction. However, many legal and regulatory issues are directly related to the security aspects of e – commerce and are: Internationalize (privacy selection) in which the EUDDP (The European Union Directive on Data Protection) requires to the members states to ensure that personal information held on informational system to be adequately protected. One of the measures introduced is a restriction on the export of personal data to countries that do not have comparable legislation in place. Another issue is the legal recognition of electronic documents as substitutes for paper equivalents varies from country to country. In some cases, certain types of document have to exist in paper form to have legal validity. In the same way, the electronic or digital signatures used to prove the authenticity of electronic transactions have varying legal acceptability in different jurisdictions. Some security solutions for e – commerce rest heavily on cryptographic products. These products are subject to restrictions on export, import or use in some countries because of their potential military or criminal application. The result is that the situation with cryptographic is changing and moves are being made in some countries to relax control.

3 Threats associated with e – commerce systems
Payments over public networks like the Internet are characterized by the fact that the payment is made purely electronically through the exchange of information. During such transactions, this information can be exchanged between several parts: customer - customer's bank, customer - vendor, customer - intermediary, vendor - vendor's bank, vendor - intermediary. If one assumes that the Internet, as a network open to all, uses switching nodes which essentially are unprotected, then the following threats must be considered for all communications links. The connected computers are also threatened, and here the perpetrators may not only be outsiders on the Internet, but insiders. In an attack from outsiders, a perpetrator could attempt to penetrate the supplier's server over the Internet by exploiting security weaknesses. He could then manipulate payment transaction data or delete such data. Instead of attacks from outsiders, in the attacks from the insiders, an aggrieved employee of the supplier could obtain access to the server and then misuse the stored data. Similarly, a person in the customer's family environment could misuse the customer's computer for the purpose of ordering goods at his expense.

3.1 Money thief's
E – commerce services are about transactions, and transactions are very largely driven by money. This attracts hackers, crackers and everyone with the
knowledge of exploiting loopholes in a system. Once a kink in the armor is discovered, they feed the system (and users) with numerous bits of dubious information to extract confidential data (phishing). This is particularly dangerous as the data extracted may be that of credit card numbers, security passwords, transaction details etc.

3.2 Identify thieves
Hackers often gain access to sensitive information like user accounts, user details, addresses, confidential personal information etc. It is a significant threat in view of the privileges one can avail with a false identity. For instance, one can effortlessly login to an online shopping cart under a stolen identity and make purchases worth thousands of dollars. He/she can then have the order delivered to an address other than the one listed on the records. One can easily see how those orders could be received by the impostor without arousing suspicion. While the fraudsters gains, the original account holder continues to pay the price until the offender is nabbed.

3.3 System failure
For example, the server could fail due to a technical defect. This would mean that neither customer nor vendor could utilize its services. Similarly the storage media on which the cryptographic keys or cash value bit strings are stored could fail so that the information is lost.

3.4 Computer viruses
Viruses, worms, Trojans are very deceptive methods of stealing information. Unless a sound virus-protection strategy is used by the e-commerce solutions firm, these malicious agents can compromise the credibility of all e-commerce web solution services. Often planted by individuals for reasons known best to them alone, viruses breed within the systems and multiply at astonishing speeds. Unchecked, they can potentially cripple the entire system. With e-commerce, a number of additional points have to be borne in minds which do not apply in the case of pure electronic money systems. These include: copyright, product liability, delivery guarantee and issues relating to obtaining redress.

4 Classes of threats
Many dangers are capable of affecting all the parties involved in an e-commerce system, whereas others affect only one part. When one considers the potential threats, these can be classified in different ways. Starting from the basic values which IT security measures are aimed at safeguarding, e.g. confidentiality, integrity and availability, one can consider how a loss in any of these basic features could be caused in relation to the different phases of an e-commerce transaction (providing/obtaining information, reaching agreement, delivering goods/services, after sales).

One of the major problem relating to the technical components is to work with stored data either is manipulation and the inconsistency of it, but also the damages to the hardware system. When we talk about hardware issues, we mean manipulation of software in components; weaknesses in the hardware or software, defective and theft of components are threats. In data communication, the dialogs must be authentic on every type of problems and communication and we must anticipate the masquerading of communications. The old messages must not be replayed. We have to focus on the communication message, and filter all the errors, redirection of messages and not allow unauthorized changed to messages. The Dangers in the area of payment transactions are faking of transactions, money laundering and insolvency and can bring major problems. Regarding the dangers in the cryptography area, the algorithms must be carefully implement especially the cryptographic keys must have the secure length and a form with no suggestive keys.

5 Solutions
In this section are described how security solutions can be used to address the issues described in the previous sections, many of them which may be holding companies to participate in the electronic market. These solutions carefully implemented will enable business to exploit the benefits of trading electronically while minimizing the security risks.

5.1 Service side – solutions
The front and back-end systems supporting an e-commerce application can be protected by developing applications and supporting systems that are robust, establishing a network environment that protects these systems and introducing essential management practices that ensure security. The electronic applications, web servers and internal systems should be able to deliberate security attacks and problems of overload and system failure. Web servers should have a platform that can be readily scaled in terms of disk space, memory and processing capacity, should as well be built from software components that are well understood (operating systems, web server applications, etc.). The internal systems must be prepared to block unexpected volumes of transactions that could cause critical business functions to become unacceptably slow or even completely unavailable. Another solution is that the software component must be updated with the latest
security weakness (e.g.: the most recent fixes), and the e-commerce applications should validate all user input to avoid accidental corruption, disclosing information. One of the most important solutions is to use where appropriate tamper–proof hardware devices is for storing cryptographic keys and performs cryptographic functions. Network environment of an e-commerce application supports the interconnection of the various service components and their connection to the Internet. The requirements are to avoid service availability problems caused by accidental overload and feature communication links, and the second requirement is to protect both web servers and internal systems from deliberate attacks by implementing appropriate network configuration measure. To avoid problems, companies should estimate traffic volume, establishing hot–standby communications links with alternative telecommunications organizations an ISPs (Internet Service Providers). Current Internet technology has an in–built mechanism SSL (Secure Sockets Layer) that can encrypt messages sent between browsers and servers. This mechanism is used to ensure the safety of the credit card numbers and other information that the customers are sending. Encryption can also be used to create virtual private networks. This refers to encrypted channels across the internet between two organizations, and is frequently used in the B2B e-commerce (VPN). Digital signatures represent cryptographic signatures who allow the source of an electronic message to be confirmed and to permit detections of any changes to it. They help to prove authenticity of an e–transaction, confirm the identity of an individual and provide proof of transmission and receipt of transactions to prevent repudiation. They are using a complex range of technologies, with public – key infrastructure (PKI), which are tested by Certification Authorities (CAs) and confirm them. Credit and debit card payments are usually encrypted with SSL because it is cheap to implement. Alternatives are the SET (Secure electronic transactions) developed by Master Card, Visa, Microsoft, Netscape and others to provide confidence in e–payment using encryption and enabling mutual authentication via digital signatures. Another two methods are S/MMIE (secure payments send via e–mail) and proprietary systems such as CyberCash Inc (electronic wallet which stores payment card details on PC and encrypt transactions between the parties). Electronic cash used for low values (e.g. Less than 10$) which use: digital signed CyberCoins transferred from an electronic wallet, Millicent (micro payment projects which uses a software electronic wallet for payments between 0, 01$ to 5$), Mondex and Visa Cash (Smart card – based solutions), digitally signed electronic vouchers (schemes designed to allow truly anonymous and untraceable electronic payments of real cash transactions), etc.

4 Conclusion
Before we start a business through e-commerce we have to give a big attention to our resources. Not just a platform will complete the work, but the people, the techniques, the time invested and the surveillance are necessarily to have a fluent and secure internet market.

References: