Secure Marketing Website

A. F. Sabeh
Foundation of Technical Education
Institute of Management\ Al-resafa

Abstract

The Internet provides business with new methods of reaching and interacting with customers as well as improving inter and intra-business communication.

In this research, a software marketing web site with a security tools is designed and implemented to protect the customer personal information and payment information when a customer tries to pay a software package.

A new protection method is suggested to protect the customer payment information passing through the network. This method is called a covert channel, because it use two ports to send and receive the payment information and downloads of software packages to the customer and these ports are dynamical and changes every time.

The modern techniques are used in building the web site and its security like ASP. NET, XML with their security rules, SQL database management, JavaScript and Visual Basic Script for encryption and controlling the communication operation, and Cookies for the chosen ports of covert channel.

The encryption technique (MD5 technique) is also used to protect the important information and payment pages transfer between both directions.

Introduction

Recently, there has been an increase in request for working in network because of the benefits of these networks and especially in transporting in the information, browsing, exchanging the massages, marketing, and … etc.(1)

As a result of the development in communication, the world has become a small village and communication process between people become very easy.

A goal of computer networking is to enable enterprise computing where users throughout an organization are able to communicate with each other and to access data, processing services, application, and other resources without regard to where they are located. (1,2)

The Internet is in actuality a network of networks, which means it's a collection of interconnected networks that span very large distance of kilometers. Internet contains different networks with different hardware and software and common form of Internet is a collection of LAN's connected as WAN, this is clearly not the case for the Internet, which is in reality both owned by no one and at the same time owned by every one. (3, 4)

Network Security

A network security is the foundation of security because it outlines what assets are worth protecting and what action or inaction's threaten the assets. Without a network security a proper security framework cannot be established.

A network security should be communicated to every one who uses the computed network, whether employee or contractor.(4)

The term "network security" is best defined and described via the three following characteristics: confidentiality, integrity and availability.

Confidentiality means that the data are accessible only by authorized parties. Integrity means that data can be modified only in authorized ways but all the possible ways of modifying data can monitor. Availability means that data are accessible to authorized parties and no one else threat to a computer network is circumstances that have the potential to cause loss or harm. (1,5)

Electronic Commerce

Definitions of electronic commerce have been around for while and have evolved over time, resulting in ever more sophisticated characterizations. (6)

One of the early definitions for electronic markets was given by Malone et al (1989), who referred to it as "networks that let customers compare and order offerings from competing suppliers." Later, Bakos (1991) introduced the terms "electronic marketplace" and "electronic market system" which he defined as "an interorganizational information system that allows the participating buyers and sellers to exchange information about prices and product offerings". (7)

These definitions were still somewhat vague but Rayport and Sviokla (1995) rendered a much more comprehensive definition of what they called "marketspace". They saw marketspace as "a virtual realm where products and services exist as digital information and can be delivered through information-based channels." This definition reflects to a greater degree the rapid development of the Internet, the new global medium that is no longer limited the environment of electronic commerce to organizations as Bakos's definition did. (8,9)

The MD5

The MD5 Message Digest Algorithm introduced by Ronald L. Rivest at Crypto '91 as a strengthened version of MD4 from MD4 on the following points:

– A fourth round has been added.
– The second round function has been changed from the majority function XY _ XZ _ Y Z to the multiplexer function XZ _ Y Z.
– The order in which input words are accessed in rounds 2 and 3 is changed.
– The shift amounts in each round have been changed. None are the same now.
– Each step now has a unique additive constant.
– Each step now adds in the result of the previous step.

The first four changes are clearly a consequence of the two existing attacks on the two round versions of MD4. The last two changes should additionally strengthen MD5. However both these changes can hardly be described as well-considered.

The unique additive constant in step k contains the first 32 bits of the absolute value of sin(k). This together with the following relation between four consecutive sine values

$(\sin(k) + \sin(k + 2))\sin(k + 2) = (\sin(k + 1) + \sin(k + 3))\sin(k + 1)$

establishes an approximate relation between any four consecutive additive constants.

This could be easily avoided by choosing the next 32 bits in the binary expansion of the sine values.

The last change however has more serious implications: adding in the result of the previous step allows creating collisions for the compression function of MD5.

This means that one of the design principles behind MD5, namely to design a collision resistant hash function based on a collision resistant compression function, is not satisfied.

The entire 640-bit input of the compression function is used to produce these collisions. Therefore they do not result in an attack on the MD5 hash function, having a single and fixed 128-bit initial value. (10)

The Proposed System Procedure

Commercial transactions depend on the participants' trust in their mutual integrity, trust in the quality of the exchange goods, and trust in the reliability of the systems for payment transfer or for purchase delivery. Because the exchange associated with electronic commerce takes place mostly at a distance, it is essential to establish a climate of trust that is conductive to business, even if the participants do not meet in person or if they use dematerialized monies. Thus, dematerialized commercial transaction introduces new requirements for presenting and displaying articles to the client and for integration information technology with remote banking: authentication of the parties, guarantee of the integrity of the exchanges, assembling of proofs in case of litigation, etc. (11)

The complete security of a remote transaction depends first on the availability of reliable transaction network. Therefore, the first step is to ensure that the communications network is continuously available, which means physical protection of the network plant, corrects routing of messages, and corrects functioning of the network maintenance of operation and administration.

The main component of this system is the Web site for software marketing and the companies' transactions control and management site. The main categories for software that user can be navigate on are divided into two types, the first type is a trial version and the second type is complete version (registers version).

The trial version software explains how this software work but this software is not completely installed because the software stops work either because number times used is finished or the date of registration is terminated.

Before the download occurs the user must be registered personal information about the customer.

When the user decided to buying software after he selects the software, at this point he must send the private information, including the credit card or electronic cash (digital money) information in additional to same fields in the registration operation.

The important field from these fields is a credit card, the registration information will be sending by using the covert channel. The covert channel begins work between the server (that contains the Web site) and the client (customer) to protect the private information of customer when sending through the network, also covert channel use to download of the selective software after complete the payment operation.

Another feature in the Web site is companies' uploading management that makes the companies able to do upload of their software (trails and complete) to represent in this side by using a covert channel (similar in work to the covert channel used between server and customer in its work). Before the upload begins the company must have a username and password to be authorized to do the upload operation.

After checking the authorization of this company, a small portion of server storage will be open (that contains folder of this company) for downloading from company.

Companies jobs (authorization and uploading) are associated with company is managed by server that is different from windows server that's to splat the company from the users. This server to control the FTP server to protect the companies' products from attacks (its used to split the security functions to web server security and the companies server security, because the isolating of security responsibility increase the performance and protection of the web site).

The system is built to deal with most types of the Internet e-commerce transactions. The main functions of this system are:

1. Marketing shop Web Site.
2. Web transactions security
    a. Authentications operation.
    b. Covert channel for registration and software downloading.
    c. Firewall Protection to the Marketing web site.
3. Companies Uploading Managements

The marketing web is designed to deal with the software marketing protocols with possible security to prevent the illegal copying of the software. It is also, designed to deal with two types of the software: trial version and register version.

Firewall is designed to protect the web server from hackers. The firewall tries to close the all unused ports and prevents the unauthorized operation to open these ports. So, when we need to open the covert channel, the system choice the ports for this operation and control the firewall to permit the covert channel to complete its work.

Authentication operation was used in authorize the companies to achieved there portions in the server storage. The authorization operation depends on the user name and password sends on the covert channel build between the company and the server.

The proposed security method (named above as covert channel) designed to be the channel linkage between the server and customer (or company) in purpose to transfer the private information (or download program). The transfer information thought the channel must be encrypted by any encryption technique (in this proposed system the MD5 technique was used to encrypt the information pass through the channel). This channel was build by using a Java Script to control the connection

operation. This Java script program generates the ports of the covert channel (one port to the transfer the private information and the second port is use to download the program to customer or upload the program from the company to server). After generation the ports and sending to the customer computer using the uploading operation (or using the cookies and Java script), the Java script will build the connection between the two side (server and customer) by sending the establish connection command to establish the channel.

The security of this channel will be depending on the following conditions:

1. The encryption technique (and encryption keys).
2. The changing ports.
3. The ability of Java script programs and cookies to control and protect the connections.

The encryption method must be chosen to be a better protection method and hard to broken with a good encryption key. In this system, the encryption key was dividing into three parts (explain below) to increase the protection of encryption.

The ports (as explain above) will generate by Java script. To increase the security of the ports will be selected randomly (between 1024 to 65535 the total ports of the computer), and each customer will use different ports from other customers. Also, if customer reconnected (for any causes) will take different ports from the previous connection. So, each establish connection will build by using ports different from other connections.

Finally, the Java script program and cookies have ability to get a better controlling of the connection. This ability was inherent from the JAVA language that used in many networking controlling and protection network systems.

In the most types of the marketing web sites, the site will be designed to accept a very larger number of the visitors, and customers. Also, the web will be able to display most information about the software source and the complete description of each software program. The flow chart of the proposed system is as shown in Fig (1).

The Marketing Web Site Design

A real Internet management services system could hardly exist, because of the variety of hardware and software platforms scattered around the world.

The web site simulates a management file system by having a central repository of folder and files published to a multitude of customer computers. The customer will communicate the web site to pay or to download (copy) the files between themselves.

In this research, a web marketing system is proposed to implement secure e-commerce transactions. The main purposes of the proposed Web site are:

1- Create dynamic Web site on the Internet, under the proposed standard specification design.
2- Add and extend some services to Web site, as Web-base software application, to be more useful to visitor from one sites in use today provide services to its visitors with little services for its developer such as provide some statistical information about Web traffic.
3- Make designed Web site as extranet Web site by cerate some pages as a separate security zone for internal-organizational use (privet zones) by isolating it from general public accessing.
4- Display the software programs in two types with their complete description: trail version and register version with complete registration operation.

These points of the design are to figure out exactly what should be done. Starting from the site specification, a design document should be built.

The proposed marketing web has the ability to deal with the database files that store the software programs complete information like: file name, file category, company name, address of company, file size, file location, trial version location, price, URL of company, software details.

The complete software programs (complete version) are stored into a special folder in the server called the "CSW" folder and encrypted by using MD5 encryption technique, while the trial version programs are

stored in folder called "TSW" folder without encryption. Also, the all software files are compressed using the ZIP compression program.

This proposed web site is implementing using the XML language complemented with HTML and Asp .NET technique. The dynamic ASP pages are used to create all these parts.

With the server-side model, the HTML source is sent to the web server with an intermingled set of instructions. There is a set of instructions, which will be used to generate HTML for the page at the time the user requests the page. The page is generated dynamically upon request.

The customer tries to pay the cost of the software product. The proposed system will load the Checkout page to check the validity of the customer information like: card number validity, card date validity, and the personal information structure validity. The main steps of the check out page operations are:

1. Generation of Jscript program and Cookies.
2. Send the Jscript and Cookies to customer computer.
3. Establishing the covert channel with customer computer.
4. Generating the Virtual Personal information page and encrypt it (using the MD5 method).
5. Uploading the virtual personal information page to customer computer through the covert channel.
6. Decrypting the receiving information from customer.
7. Checking the customer information.
8. Sending the encrypted software package through the second port of the covert channel.

The checkout page will generate the needed Jscript program that is needed for encryption and decryption the user information through when transfer through the network (Internet), and stores the first part of encryption key. The Jscript program will be uploaded to the customer computer.

Also, it generates the cookies that carry the ports numbers and the second part of the encryption key. The cookies will send to customer computer and save to a temporary location in the windows (or in the root directory of the customer hard disk). These cookies will delete when exit or complete the downloading operation. The ports numbers will be used

to determine the covert channel ports that used to load the personal information page, and to downloading the software package after complete the payment operation. These ports will change for each customer and each downloading operation.

XML security function that described in web site security. The personal information page contents the complete information about the customer like: customer name, customer address, email, location, city, state, card number, card name, card date, ...etc. This information will be sent through the covert channel (encryption case) with XML security protection.

After completing uploading the Jscript and cookies to customer computer, the proposed system waits for the acknowledgement signal over the selected port. When the proposed system sense the acknowledgment signal over the selected port, the proposed system will establish the connection through this port and the other port of the covert channel, and then sends the personal information page through the covert channel.

After completing uploading the personal information of customer from server to customer computer, the proposed system will wait until customer finishes the fills the information fields. Then the Jscript program encryption the customer information to start transfers them to server. The proposed system will decrypt the received information from customer through the covert channel port. Then, proposed system tries to check the fields of information with some rules like:

1. The length of the fields like: full name, address, city, state, and card information, ...etc.
2. The structure component of field as email address, telephone number.
3. The validity of number as card number, and card date.
4. The other rules for checking the validity of customer cache count

The flowchart of this function is as shown in Fig. (3).

Web Security

In this system, there are three types of the security techniques used to protect the information and software programs from the attacks. These techniques are:

1. Authentication operation.
2. Covert channel technique
3. Firewall system.

The authentication operation is used to authorize the users. There are two positions that use the registration form. The first case of the registration is register user try to download the trial version of software programs.

The second case is registration the sealers in the software program downloading or uploading.

The covert channel will be used to transfer the registration information from customer to marketing server, and from marketing server to bank for checking. Also, the covert channel will be used to download the register software program to the user.

Firewall system will be used to protect the web server from hacking by the attacker to illegal download software programs from the web server. It works with encryption controller used to encrypt/ decrypt the software program that is stored in the special folder (for each company there is a special folder for storing their programs).

Authentication of Software Company

Forms Authentication in ASP.NET can be a powerful feature. Windows Authentication gives user this flexibility, but it is not compatible with anything.

Role-based security in Forms Authentication is one thing Microsoft left out in this round for .NET. In this proposed system, we will covert the basics of Forms Authentication, how to adapt it to make use of role-based security, and how to implement role-based security on software company site with single signors.

This proposed authentication method in design depends on role-based security with Forms Authentication, a detail that Microsoft left out of .NET for this round. This method will use different techniques that are

almost completely incompatible with the standard Forms Authentication, save the setup.

To follow along in this method, the proposed system must create a database, a web application, several secured directories, and a few ASP.NET Web Forms (pages).

The proposed method will use the covert channel (secure channel will be explain below) to transfer the encrypted information using the MD5 hash encryption.

MD5 hashing is a one-way algorithm that makes a unique array of characters. Even changing one letter from upper case to lower-case in user password would generate a completely different hash. The proposed system stores the passwords in the database as hashes for protect them.

In a production environment, user also wants to consider having a question and response challenge that a user could use to reset the password. Since a hash is one-way, user won't be able to retrieve the password. If a site is able to give old password to user, the proposed system will prompt the client by the covert channel using the certificate along the way for encrypting user pass phrase and decrypting it for later use, though it should still be hashed.

Without using HTTP over covert channel, user password will still be sent in plaintext across the network. MD5 hashing the password on the server only keeps the stored password secured.

The username and roles are not stored plainly as part of the cookie (nor should it, since a user could modify his list of role-memberships), it needs to be generated for each request

After completing the registration operation of company, the proposed system will open the virtual drive of this company to permit this company to add the new version or update the software package, or add a new product. Finally the proposed system will add this update to the main database of software package.

Covert Channel Protection Method

Protecting the message content from being intercepted (confidentiality) or illegally modified (integrity) is a primary security

concern. This specification provides a means to protect a message by encrypting and/or digitally signing a body, a header, an attachment, or any combination of them (or parts of them) through the network.

In this proposed system, the transfer personal information of the customer will pass through covert channel in encryption format. The covert channel can be called secure channel due to the similarity with the Microsoft secure channel. But the differences are the ability of proposed covert channel to change encryption key automatically, encryption method, and the port of the connection. For each customer connected to the web site an encryption/decryption key differ from the other customers.

The encryption method will be applied by using a special Java Scripts program with a special cookie transfer the information about the customer system and the port number of received the response message.

Then proposed system sends cookies and Java script program to the customer computer to get information about the customer system and to send the port of the received messages. The proposed system will establish a connection through the selected port generated by Java scripts (grater than 1024 and lees than 65534) and stored in cookies. Then proposed system sends the encrypted registration page using selected port. The customer system will activate the received Java script program (the ability of this type of program to run automatically with windows Explorer) and receive the encrypted page to decrypt it and display to the customer.

The customer fills this registration form and clicks send command in the bottom of the page. The Java script program will encrypt the registration information and send it to the market server using the port number found in the received cookie.

If there is no cookie received, the Java script will use the same port that is used to receive registration page. The proposed system will receive the registration information and decrypt the received information and encrypt it by using a special key (a special key between proposed system and the Bank) to send information to the bank for checking the credit card number.

The response of the bank checking will encrypt and send to market server with one of the two values ("accept" or "not accept"). If the response is "accept", the proposed system transfers the software program to the customer using the same covert channel.

To increase the security of the transfer message, the message integrity will be provided by leveraging XML Signature in conjunction with security tokens to ensure that messages are transmitted without modifications. The integrity mechanisms are designed to support multiple signatures, potentially by multiple actors, and to be extensible to support additional signature formats.

Firewall Protections

In this proposed system, the firewall is used to protect the contents of the web server from the unauthorized user trying to intrude. The firewall is implemented in the web server and controls the web server ports operations. This operation will reduce the attack on the web server.

The proposed firewall system works by receive packet from the LAN card that connects to the Intranet (from the ports that the system scans it). Then it sends the packet to a buffer, the system will be examine each packet in the buffer by comparing the IP address of the source computer and destination computer of packet with unauthorized IPs table. Therefore the number of ports and the IP of source and destination computer determine the level of security. Whereas the IP of the source or destination computer is unauthorized the packet is rejected, access is denied and message is sent to the request owner (source computer) about this situation.

When the IP of the source and destination address are authorized, the firewall will record the login inside the web server. When the request is addressed to the Web server, this server responds to the request and sends the home page of the Web site to the request owner (source computer). The firewall program was used to protect the two servers (marketing web server and company management server). The firewall also supervised the covert channel operation. No port open without request firewall to open it. So, all the covert channels ports will open under the control of the firewall.

The flowchart Fig.(4) represent the mechanism of the proposed firewall system. The firewall system uses many algorithms to complete its work like start operation algorithm, add new unauthorized IPs or Ports, remove IPs or Ports from the access denied, ..etc. The startup algorithm is used to load firewall when Windows server system starts or when the firewall is run from program file of Windows system, as follows:

Input: Initial starting

Output: Firewall starting

Step 1: Initial conditions to starting firewall.

Step 2: Display the name of firewall.

Step 3: Load the last configuration of firewall.

Step 4: Load windows registry for the condition of firewall.

Step 5: Listen to specified ports.

Step 6: Begin the checking operation of the firewall.

Step 7: Display the status of communication status.

Step 8: End.

The first step is used to load the conditions and parameters of loading the firewall program. These conditions and parameters are used to link the firewall program to the operating system to get the flexibility and to control the communication process. The second step is used to display the name of program.

The third step is used to get the last configuration of the firewall; this makes the user get the best results depending on the last configured for his communication. After this the firewall will listen to specific ports and controls the communications requested and connections. The status of communication will be displayed on the interfaced screen for user to make to know online the status of the firewall if user needs.

The configuration of firewall must be loaded to optimize the operation of firewall program. The configuration of firewall contains the condition for starting its operation and the information about the computers connected to the server of the company.

The Company Managements Server

The company management server was used to control and management the companies' operation as uploading the new software, replace the software package with newer, add new categories of software, delete the software package, ..etc.

The operation of this server was described above. The main purpose of this server is constraint the secure communication between the web site and the companies. This server was use the covert channel to transfer the software between the web server storage and companies.

When starting this server operation, the server will take the ports 2004 and 2005 to connect through these ports with the companies. When company tries to connect with this server for some purposes, the company used the connection program to send the request for connection to this server over these ports.

The server will send the home page of this server and ask user to enter the company name and the password of this company. In this time, the Java scripts and cookies (as described above) controlling the connection to transfer these private information through the network by building the covert channel using the same technique of covert channel.

The private information will send through the covert channel will check in this server after decryption them. If the user authorized, the new covert channel will build to help company to work with special folder in company server (the server will decrypt the content of this folder). The company will do some operation like change the trail version software with newer, replace the complete version software with a newer version, remove their software from this server, add new category of software, ..etc.

After the company complete their works on this folder, the server released the connection with this company by released the covert channels.

Then apply these operation on the content of this folder after store the previous in the temp folder. After these operations the server re-encrypts the folder content by using the MD5 encryption technique to close this folder.

Finally, the server will correct the information of the marketing web server by change the database content by updating this database by the newer information in the specific fields.

The algorithm of this server is as shown below:

Input: Initial starting
Output: Company Management Server starting

Step 1: Initial conditions to starting server.
Step 2: Display the name of server.
Step 3: Load the last configuration of server.
Step 4: Load windows registry for the condition of server.
Step 5: Listen to specified ports(2004 and 2005).
Step 6: If the there request command on one of these ports then
Send the home page of this server.
Generate the Jscripts program and cookies need for covert channel building.
Send these Jscripts and cookies to the company computer.
Display the authorization Page.
Wait until the user click on the send command.
Encrypt the username(company name) and password
Build the covert channel.
Send the private information through the covert channel
Else goto step 8
Step 7: Decrypt and Check the private information
If the private information is correct then
Build the another covert channel.
Decrypt the folder of this company.
Open the folder of this company.
Copy the content of this folder into a temporary folder.

Wait until the company completes their work (their work will operate through the second covert channel on the temporary folder).

Replace the content of the main folder of the company with the temporary folder (vise versa).

Update the database of the Software marketing website.

Release the covert channels and the connection with company.

Conclusions

1. Payment security is not sufficient protection for users; legislation is necessary to combat fraud and breach of trust and also to protect the right to privacy.
2. Existing laws are not easily enforceable for online monetary transactions or for purchases of nonmaterial goods, especially software.
3.The exploitation of data collection from customers during the conduct of transactions, without their consent, poses a serious problem.
4.The proposed system increases the security of electronic transactions by using a security method as a covert channel with a powerful encryption method to reduce the attacks on the transfer/downloading software through the network.
5.The changing ports in covert channel increase the security of transfer information through the covert channel due to changing ports. This will reduce the interception from the intruders.
6. Dividing encryption key between the Jscript, cookies, and personal information page increases security in encryption information.
7.Using Jscript increases the encryption/ decryption speed due to the ability of this type of script to work with different types of operating systems and in very fast processing.
8.Losing Cookies during the transferring or due to any protection against cookies will not stop the proposed system checking operation, due to the ability of proposed system to recognize the losing (protection against) of cookies from the covert channel ports (if ports default this means the cookies are not working).

9.The stopping of cookies makes proposed system work in default mode (default ports, and encryption key are divided to two parts (in Jscript and personal information Page)).
10. The proposed system has a protect database due to the encryption technique used in encryption of the content of the database, and protects location for storing the database file.
11. Using the ASP. Net and XML in web site design increases the security of the web site (by applying the XML security rules and ability of the ASP.NET to work and link with Windows encryption techniques). Also, they increase the speed of web services.
12. Increase the request to downloading will reduce the quality of service of the web sever, but in this proposed web service using covert channel for each user will increase the ability to deals with large number of download request.

References

1. Abbas ,An.(2003) "Developing a Security for Simple Network Management Protocol (SNMPv3)", M.sc thesis,.
2.Cambell, A.J. 28. Retrieved February 5, (1999), Embracing electronic data interchange now will keep you company in step with the competition, Business America, 119 (6), from the World Wide Web: http://gw3.global.ebscohost.com/
3.Bradley C.wright, April 4, (2000) "Internet And E-Commerce Patents", Intellectual Property Law Section's Spring CLE Program on E-commerce and Internet Patents on.
4.Deloitte and Touche, (2002) E-commerce Secuirty, secuirty the network perimeter, ISACF Board of Trustees, USA,.
5.O. Algin,(2004) E-commerce security, publish key infrastructure, good practices for secure communications, ISACF Board of Trustees, USA,.
6.Dharm B. S. and Parag D., (2000) Computer Network and E-Commerece", Pentagon Press,.
7.Evans, M. (1998, December 21). Ecommerce, e-mmediately. Industry Week 247 (23). From the World Wide Web:

http://gw3.global.ebscohost.com/

8.Friet, W. (1998, March 23). Customer confidence is key to E-Commerce. Internetweek (707). from the World Wide Web: http://gw3.global.ebscohost.com/

9.Mostafa Hashem Sherif, 2000 " Protocols for secure Electroic Commerce", At& T Loboratories, New Jersey,.

10.Antoon Bosselaers ESAT Laboratory, be23 July (1993) K.U. Leuven Kard. Mercierlaan 94 B-3001 Heverlee, Belgium antoon.bosselaers@esat.kuleuven.ac

11. Gleckman. H., & Dwyer, P. (1999). Internet taxes. Business Week (3618), 43. from the World Wide Web: http://gw3.global.ebscohost.com/.

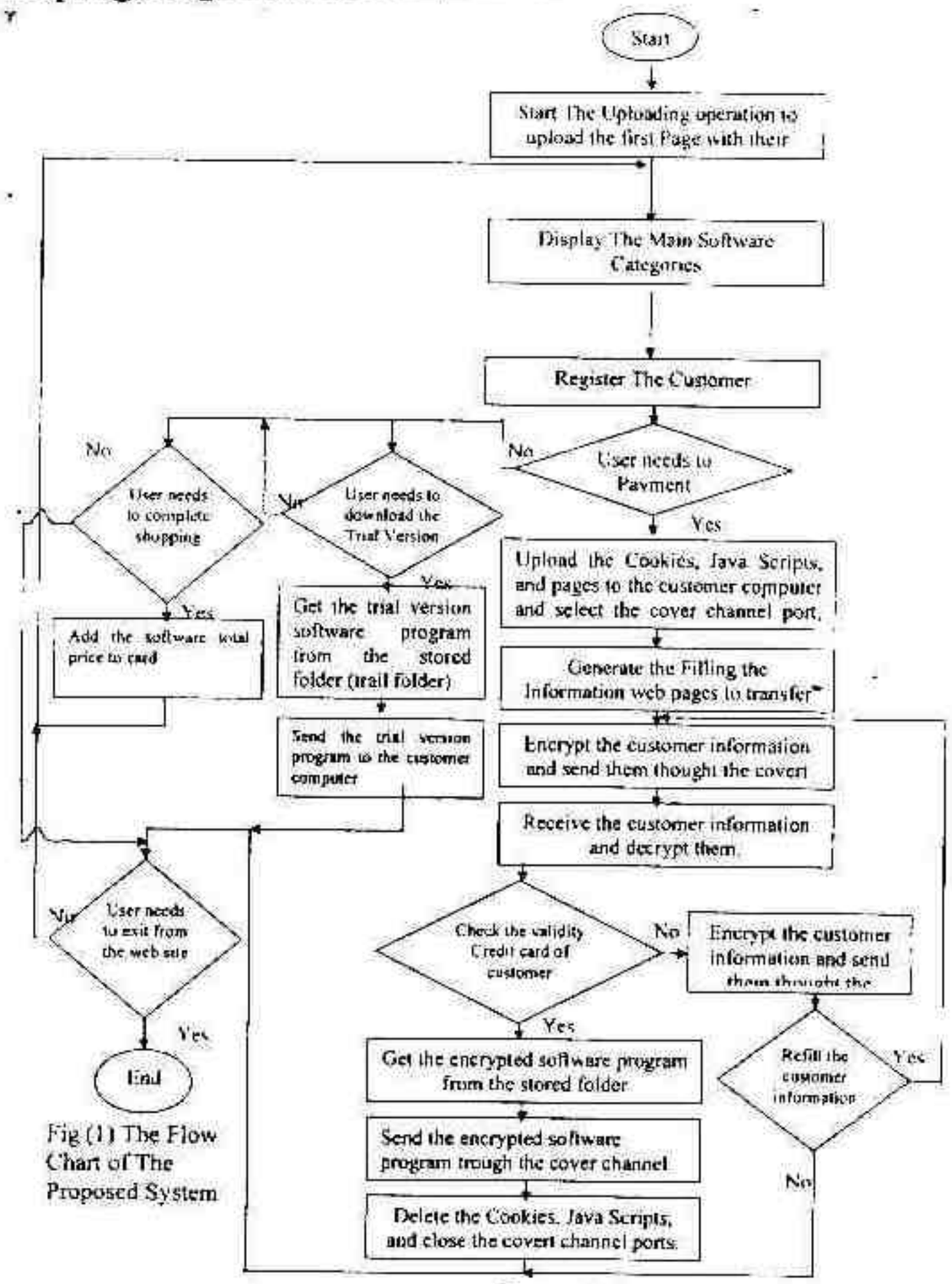

Fig (1) The Flow Chart of The Proposed System

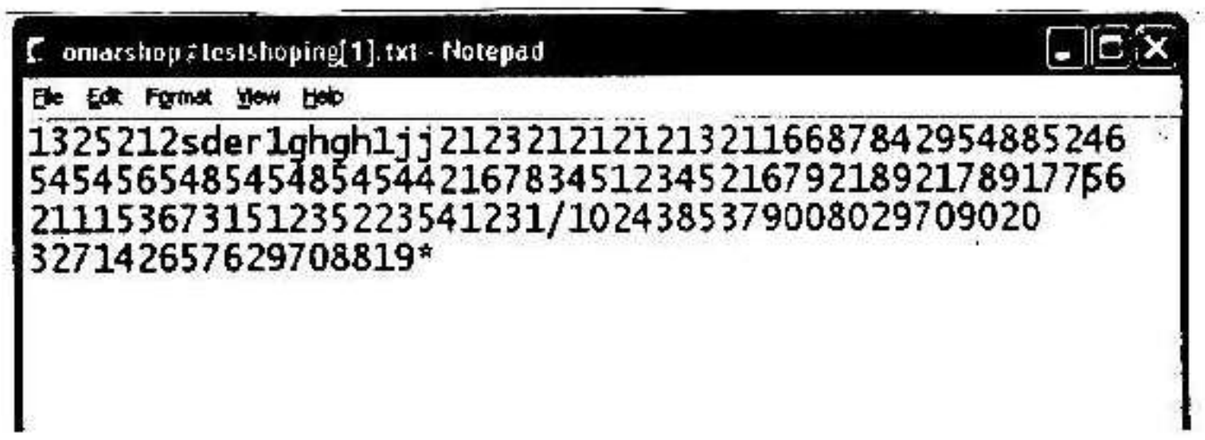

Fig.(2) The example of cookies content.

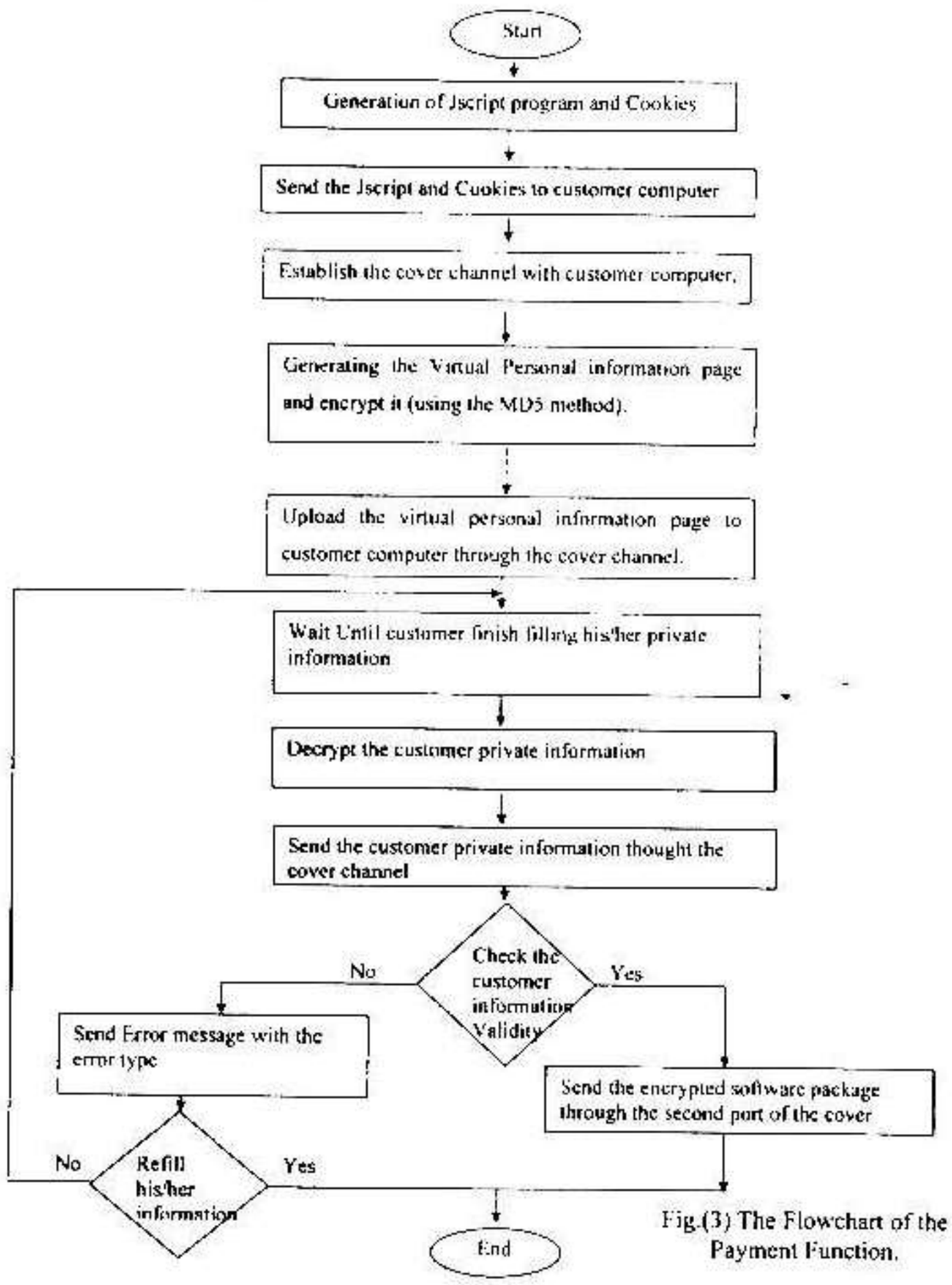

Fig.(3) The Flowchart of the Payment Function.

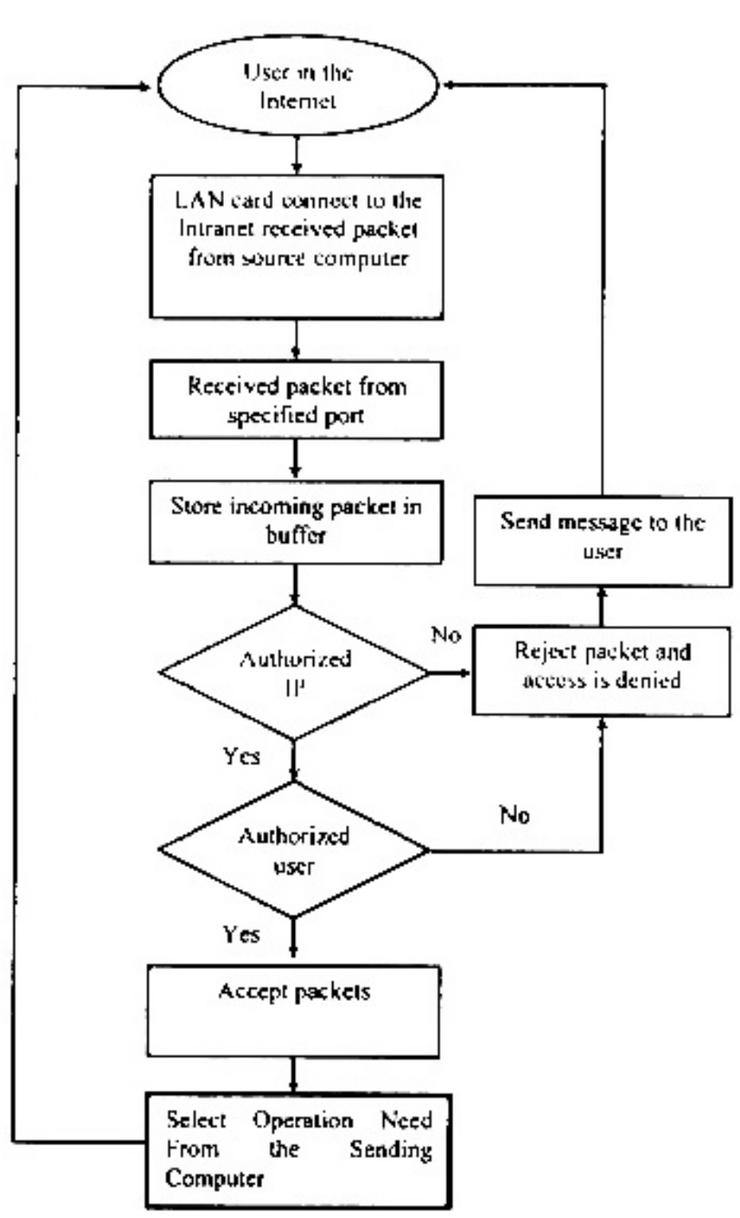

Fig.(4) The firewall system from the Internet

موقع التسويق الأدنى

آن فائق صبيح
هيئة المعاهد الفنية /معهدالأدارة الرصافة

الخلاصة

شبكة الأنترنت توفرامكانيات ذا طرائق حديثة لغرض التفاعلِ مع الزّبائنِ العاملين عليها وأمكانية الدخول وإلاتصال بصورة جيدة في أثناء العمل أيضا.

في هذا البحثِ، موقع تسويق البرامجيات مع الادوات الامنه المستخدمة صممت لكي تَحْمي الزّبون ومعلوماته الشخصيةَ ومعلوماتَ الدفع عندما يحاول الزبون أنْ يَدْفعَ لكي يشتري برنامجا.

ان طريقة الحمايةِ الجديدةِ المقترحة هي أنْ تَحْمي مرور معلوماتَ الزّبونِ عندما يقرر الشراء خلال الشّبكةِ. هذه الطّريقةِ تَدْعى القناة السرية، لأنها تَستعملُ قناتين لأنْ تُرسل وتَستلمَ معلومات الدّفعَ ويُحمّل عن طريقها مجموعة البرامجِ إلى الزّبونِ وهذه القنوات ديناميكية وغير ثابتة أي تتغير من وقت الى اخر.

إنّ التّقنياتَ الحديثةَ المستعملة في تصميم الموقع وحمايته مثل ASP.NET، XML ،مع القواعد الامنية المستخدمة، وSQL لأدارة قاعدة البيانات ، و JavaScript and Visual Basic Scrip للتّشفيرِ والسّيْطَرَة علي عمليات الإتصالِ ، و Cookies لأختيار القناة السّريةِ.

ان تقنية التّشفيرِ المستخدمة (MD5 technique) استعملت لحماية المعلومات المهمة وصفحات الدّفع المنتقلة بين كلا الجهات.