OPTIMIZING SECURITY IN E-COMMERCE THROUGH IMPLEMENTATION OF HYBRID TECHNOLOGIES

Gurjodh Singh Dhillon  
M.Sc. (Computer Science)  
Dept. Of Computer Science,  
Khalsa College, Amritsar-143002. INDIA

Jatinder Ohri  
Lecturer  
Dept. Of Computer Science,  
Khalsa College, Amritsar-143002. INDIA

Abstract: - Providing sensitive information over the net or even browsing the net could be the gateway to the misuse of data and other viruses. During the e-commerce process crucial business transactions are carried, even individuals perform online transactions like banking and shopping etc. over the internet and here the actual threat grips the minds of every common person that, Is the information passed on the net is secure? Of course this is the biggest question for which everybody tries to find the way out. Every year all the organization spends big amount to get away from this big threat. There is much more to think where as security issues are concerned but below are the main security solutions we are having but it is very clear that each has an application at different levels when e-commerce and network security is concerned. Hence we can wind up saying that there is up most need of using hybrid of these technologies with which we give 100% security to the e-commerce transactions so that 89% of the people should get rid of their negative thinking of Internet security during transactions.


1. Introduction

Our generation stands on the very cusp of the greatest technological revolution that mankind has ever faced the exponential growth of the Internet, lead to the search of new techniques for conduction effective business, and commercial activities on the Internet. Commerce is now undergoing a revolutionary phase where the medium of communication between the customer and the merchant is electronic. The cutting edge for business today is Electronic Commerce.

What exactly is the e-commerce? It refers to selling, advertising and marketing products, all done over Internet i.e., aspects of economics. Also majority of engineering design decisions are concerned closely with economics. Think off when commerce comes in can there be security and privacy issues are left behind? “NO” then if in the present day’s scenario commerce and Internet are converging to increase the effectiveness of overall business, how can we leave the security and privacy issues.

Commerce on the Internet is a reality with online entertainment, retail, and financial sites, among others, flourishing. The ability to conduct business on the Internet has now become a necessity. Unfortunately, conducting business on the Internet brings it with new threats and vulnerabilities. The implementation that you choose today will likely to change within the coming years as your business trend changes. We can help you select the electronic commerce method that best provides the protection and functionality needed by both you and your customers.

A few important applications for e-commerce which we are all dealing in our day to day life like Education and training, entertainment, medical, telephone, electricity, transportation and specially Banking and the Financial transactions on which whole commerce revolves. Broadly we divide the e-commerce in three categories. a) Business to Business (B-2-B). b) Business to Commerce (B-2-C). c) Business to Government (B-2-G).

Among all the categories the common is everybody just want to be a “Click” away from their respective parties with a big target in their mind that expected e-business transactions in India will go up to 400,000 million by the end of this year (up to 2004) as per survey of NASSCOM. Also report by Forrester Research in Feb.97 quoted “Corporate spending on e-commerce systems and applications will go from few hundred million dollars in 1997 and has been raised to 3 Billion in 2000 and a growth of 60 times by the end of 2004”.

Proceedings of the 5th WSEAS Int. Conf. on CIRCUITS, SYSTEMS, ELECTRONICS, CONTROL & SIGNAL PROCESSING, Dallas, USA, November 1-3, 2006   165
In e-commerce we always make transactions, which may be either sending/receiving documents or online operations through the Internet. In other words and more specifically saying B-2-B e-commerce demands an online environment that authenticates the identity of business groups and ensures that transactions remain confidential. So required to fences on the net to achieve main security aspects i.e., Data Integrity, Data availability, Data Confidentiality and Privacy.

“The core idea to be achieved for e-commerce is the flexibility yet secure way of customer services and payments to be made to all involved parties without compromising on the privacy of the participating agents”. Hence any company using the concepts of e-commerce can be able to explore big domain to trade large number of customers from all over globe.

**Principle components of E-commerce**

The principle components of this beautiful technology are

1. Electronic Fund Transfer
2. Electronic Data Interchange
3. Corporate Digital Library Mechanism
4. Electronic Messaging

Without going into the details of the components, we will straight way try to explore the various security aspects and technologies. Seeing such a sharp, lucrative and multiplier growth gives courage to the hackers, some driven by technical challenge and other for some financial gain, giving rise to the cyber crimes. The baffling variety of cyber crimes are: Hacking, Fraud through program manipulation, Tempering with cash dispensers, Use of internet and militancy, Pornography, Gambling and Betting, Spoofing and masquerading, Preaching, Interception, Time theft, Unauthorized access, Alteration of data through viruses, Logic Bombs, Computer sabotage and vandalism of software and hardware, theft of trade secrets and Use of online bulletin board for material relating to criminal offences and offences related to e-commerce.

Now days many companies have already implemented or are investigating e-commerce systems to increase opportunities for work to be carried out at faster pace by making data sharing between departments and individuals across company boundaries. But these benefits have to pay the price. The moment our network is connected to Internet it becomes vulnerable to attack by hackers. The CERT Coordination Centre is the major center for reporting Internet security problems. As per the statistics of CERT/CC we can see how fast the Internet problems increase at different levels.

**Number of incidents reported**

<table>
<thead>
<tr>
<th>Year</th>
<th>Incidents</th>
<th>Year</th>
<th>Incidents</th>
</tr>
</thead>
<tbody>
<tr>
<td>1988</td>
<td>6</td>
<td>1996</td>
<td>2573</td>
</tr>
<tr>
<td>1989</td>
<td>132</td>
<td>1997</td>
<td>2134</td>
</tr>
<tr>
<td>1990</td>
<td>252</td>
<td>1998</td>
<td>3734</td>
</tr>
<tr>
<td>1991</td>
<td>406</td>
<td>1999</td>
<td>9859</td>
</tr>
<tr>
<td>1992</td>
<td>773</td>
<td>2000</td>
<td>21756</td>
</tr>
<tr>
<td>1993</td>
<td>1334</td>
<td>2001</td>
<td>52658</td>
</tr>
<tr>
<td>1994</td>
<td>2340</td>
<td>2002</td>
<td>82094</td>
</tr>
<tr>
<td>1995</td>
<td>2412</td>
<td>2003</td>
<td>137529</td>
</tr>
</tbody>
</table>

Total Incidents Reported (1988-2003) **319,992**

Please note that an incident may involve one site or hundreds (or even thousands) of sites. Also, some incidents may involve ongoing activity for long periods of time.

**Vulnerabilities Reported**

<table>
<thead>
<tr>
<th>Year</th>
<th>Vulnerabilities</th>
<th>Year</th>
<th>Vulnerabilities</th>
</tr>
</thead>
<tbody>
<tr>
<td>1995</td>
<td>171</td>
<td>2000</td>
<td>1090</td>
</tr>
<tr>
<td>1996</td>
<td>345</td>
<td>2001</td>
<td>2437</td>
</tr>
<tr>
<td>1997</td>
<td>311</td>
<td>2002</td>
<td>4129</td>
</tr>
<tr>
<td>1998</td>
<td>262</td>
<td>2003</td>
<td>3784</td>
</tr>
<tr>
<td>1999</td>
<td>417</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Total vulnerabilities reported (1995-2003) **12946**

**Mail messages handled**

<table>
<thead>
<tr>
<th>Year</th>
<th>Mail</th>
<th>Year</th>
<th>Mail</th>
</tr>
</thead>
<tbody>
<tr>
<td>1988</td>
<td>539</td>
<td>1996</td>
<td>31268</td>
</tr>
<tr>
<td>1989</td>
<td>2869</td>
<td>1997</td>
<td>39626</td>
</tr>
<tr>
<td>1990</td>
<td>4448</td>
<td>1998</td>
<td>41871</td>
</tr>
<tr>
<td>1991</td>
<td>9629</td>
<td>1999</td>
<td>34612</td>
</tr>
<tr>
<td>1992</td>
<td>14463</td>
<td>2000</td>
<td>56365</td>
</tr>
<tr>
<td>1993</td>
<td>21267</td>
<td>2001</td>
<td>118907</td>
</tr>
<tr>
<td>1994</td>
<td>29580</td>
<td>2002</td>
<td>204841</td>
</tr>
<tr>
<td>1995</td>
<td>32084</td>
<td>2003</td>
<td>542754</td>
</tr>
</tbody>
</table>

Total Mail Messages handled (1988-2003) **1,185,123**
2. E-Security

Providing sensitive information over then net or even browsing the net could be the gateway to the misuse of data and other viruses. During the e-commerce process crucial business transactions are carried, even individuals perform online transactions like banking and shopping etc. over the internet and here the actual threat grips the minds of every common person that is the information passed on the net is secure? Of course this is the biggest question for which everybody try to find the way out. Every year all the organization spends big amount to get away from this big threat. First of all we have to identify what we are trying to secure, no doubt “information”. Information can be secured in two forms.

1. When it is stored on the system.
2. When it is being transmitted over the Internet.

When we start talking about this particular aspect there are some terms, which must be clear in everybody’s mind.

**Threats:** Disrupt the integrity or functionality.

**Vulnerability:** Inherent flaw caused by improper design.

**Attack:** Method of exploiting vulnerability.

2.1 Stages/Challenges of e-security

Security should be provided must be two fold:

1. One Passive stage: It is based on user authentication and control. The various threats in this category are
   i) Unauthorized access
   ii) Unauthenticated access
   iii) Spoofing (fabrication or impersonation)
   iv) Attack (making resources unavailable)
   v) Malicious Software

2. Two-transmission stage. Major challenges in this category are to provide integrity and confidentiality.
   i) Sniffing (interception)
   ii) Modification
   iii) Repudiation (Denial of action)
   iv) Relay the information

To beef up the security of our on-line transactions Encryption and compression are used for making information unreadable. We can provide security at two different levels.

1. At Desktop level.
2. At Enterprise level.

1. Desktop is considered to be the weakest part on the Internet. We should restrict the user’s movement using the access control systems. These systems can be designed targeting the following points:
   i) Authorized persons should get access to the desktops.
   ii) Eliminate all static passwords to ensure elimination of unauthorized access through logging or sharing.
   iii) Monitoring the aspect of moving company employs on desktop along with their profile.

2. Enterprises must include anti-virus software, firewalls, VPNs, intrusion detection and vulnerability assessment along with their best practices. All like client and server, gateway can use these tools. Antivirus and firewalls working hand to hand to protect the information flowing out and coming in. Also the firewalls are complemented with VPNs, which offers encryption and authentication for remote clients of the network. Key issues dodging at the enterprise level are secure authentication, masquerading, integrating encryption/PKI capabilities without investigating in expensive manpower of technology.

2.2 Solution with Latest E-Security Technologies

Before going to see the technologies for the securing the transactions on net one must be sure about the answers of the few questions like 1. Do we understand the risk presented to the Internet. 2. Is the security underpinning today’s system sufficient for the use we make of the Internet? 3. Is it sufficient future support? 4. Do we understand the security of our system to make data 100% secure? 5. Virus protection is adequate. 6. Subject of an attack? The common answer we got is “We have firewalls”. But this way not be true due to lack of our understanding of security aspect. One must know firewalls are only part of security solutions and they need not to be properly configured and handled. Also it may come under hacking attacks due to bugs in
the software inside the firewalls. Survey shows 80% of firewalls are incorrectly configured. Hence we should leave behind the myth of firewalls, should go for other technologies commonly used but from the following chart it is very clear that no one gives us perfect security and forcing us to use combination of the technologies. One can provide security at different levels/stages of our Internet commerce transactions. Like during communication, Authentication, E-mail and web security. The technologies, which are in use, are as under.

### 2.2.1 Cryptography

It is being used in many security solutions and become a standard to provide security during transmission. We are using two main types of techniques. The first one is symmetric key or private key or secret key or single key cryptography and the second one are asymmetric or public key or combination of two keys encryption.

### 2.2.2 Firewalls

It is combination of hardware and software that works towards ensuring and enforcing a security policy for the network. But as we discussed that it does not provide 100% security, which means reality of its fades into the background. For using Firewalls we need to put appropriate security policy. Without the appropriate security policy that take into the account the myriad of variables and has dynamic features to accommodate the constantly changing variants and exploits, firewalls are almost useless. Lastly we can say it can only detect and protect an incoming downstream data.

### 2.2.3 VPN (VIRTUAL PRIVATE NETWORK)

It provides the means to set up a secure network connection between sites using the Internet. A VPN is basically transmit information in a secure network over the untrusted network using encryption, authentication and tunneling. VPNs are reliable for the use of public Internet to transmit private data between sites. There is other security method which is coming up in place of VPN i.e. SSH (Secure Shell) which provides an open protocol for security network communication that is less complex and expensive than hardware based on VPN solution.

### 2.2.4 KERBEROS

It is a centralized authentication service that allows both users and services to authenticate themselves to each other and provide a secure authentication service in a distributed environment. Hence it adds flexibility and gives us robust authentication framework. But there are limitations like for user’s weak password, it won’t provide any safety against password guessing attacks, and also it is having a single point of failure and security breach.

### 2.2.5 INTRUSION DETECTION SYSTEM

This technology is either host-based or network based. Intrusion detection products are software and hardware products that monitor a device or network for malicious activity. IDS compare network and resource activity to list of signatures known to represent malicious activity. NIDS (Network Intrusion detection system) are dedicated software systems that reside on a network wire and analyze networks packets. The data encapsulated in these packets is compared to a database of known attack signature, if match does not found then packet traffic continues otherwise alert is generated. HIDS (Host based Intrusion system) have emerged due to the practice of monitoring audit log files. With compassion of traditional system of searching the entire log file from malicious activity. HIDS offers a local agent that scans all the activities as the event occurs. It has ability to monitor application log files for evidence of additional attacks. It also has the ability to monitor application log files for evidence of additional attacks. It also has the ability to monitor local files for any changes or modifications.

### 2.2.6 BIOMETRIC SECURITY

Positive and better security is to make or to authenticate individuals. This is based on the methods like fingerprint, retina or iris scan, voiceprint and face geometry. These can be done in two methods registration of characteristics and then matching the stored pattern to actual characteristics.

### 2.2.7 WEB SECURITY

The fastest growing factor in IT is Internet based applications and up most requirements is securing the web-based applications. SSL
SSL: It is a big leap in the direction of providing safe security to the online transactions involving critical information like electronic fund transfer, cyber cash etc. As per survey of WORLDPAY E-COMMERCE, 89% of e-commerce users base their decision of purchase of transaction security and 59% on price. But with the increasing trend of e-commerce this ration is changing slowly. During online transaction, it is an event of client/server architecture and is still vulnerable. SSL provides strong solution for security. It is based on the principles of cryptography, authentication, confidentiality, integrity and non-repudiation. The confidentiality is maintained by encryption technology between the two SSL-enable pairs. Mainly it contains two sub protocols, one is SSL that defines format for transmitting data preserving integrity and the second one is SSL handshake protocol defines the steps that lead to decision regarding the choice of session layer. Handshake begins with sending the information like version, cipher setting and other data to the server, which issues digital certificates.

With the increasing traffic, SSL accelerator cards, appliances and servers designed to handle heavy load. SSL cards fitted in the web servers for authentication activities and handle increasing SSL sessions. SSL appliances are fitted to give high performance. These engines executing complex authentication and key generation activities. Load balancing device is also integrated with appliances. SSL traffic is sent through both and routes all network traffic to the servers. With the sharp growth leads to another SSL solution is “Packetised SSL” developed by Andes Networks.

Reports from research organization indicate that the demand for load balances is growing and SSL hardware revenues will touch $60 million with total revenues growing to $595 million by 2005. Along with this the threat is of poor performance on servers leading to a limited number of sessions.

SSL and HTTPS are the mechanisms that are typically meant for point-to-point interaction. The advance part of the security of web services is to use new paradigm to SOA (Service oriented architecture) based software, which is more dynamic for developing and deploying these web services. For this we can use SOAP (Simple object access protocol), is easily implemented on other popular protocols. The future foundation of web service security lies is shielding the XML data that flows as a part of SOAP payload. For securing standard XML documents a combination of security standards is to be used (for securing web services) is XML encryption, XML digital signature, XKMS (XML key management services), SAML (Security assertions markup language)

2.2.8 E-MAIL SECURITY

Most common and most popular application of the Internet is e-mail and it is highly insecure. As during sending, receiving and during modifications the information can be exposed to the hackers at transit time or storage time. There is no lack of standards for secure e-mail such as MIME object security service (MOSS), message security protocol (MSP) and PEM. But the most deployed and popular solution is PGP and S/MIME. The actual operation of PGP as opposed to the management of keys consists of five services: Authentication, confidentiality, compression, e-mail compatibility and segmentation. PGP is the main choice of personnel e-mail where as commercial and industry standards are concerned S/MIME is emerging strongly.

3. Feature Wise comparison of Security Solutions, common measures to be taken for making our Security Strong:

One should perform the best efforts to stop the most of the attacks along with the use of the technologies are:
1. Employ a Layer 7, full inspection firewall.
2. Automatically update your anti-virus at client, server and the gateways.
3. Make all applications and systems updated.
4. Make it sure that you have patched and up to date your server and its applications.
5. Delete all unused programs
6. Turn off all the options of network services, which you are not using regularly.
7. Regularly scan network for common backdoor services using detection.
There is much more to think where as security issues are concerned but above are the main security solutions we are having but it is very clear that each has an application at different levels when e-commerce and network security is concerned. Hence we can conclude there is up most need of using hybrid of these technologies or in other words we can say we all need to explore and work on the development of some new technologies with which we give 100% security to the e-commerce transactions so that 89% of the people should get rid of their negative thinking of Internet security during transactions.

REFERENCES


