Assistance with University Projects? Research Reports? Writing Skills?

We've got you covered!

www.assignmentstudio.net

WhatsApp: +61-424-295050

Toll Free: 1-800-794-425

Email: contact@assignmentstudio.net

Follow us on Social Media

Facebook:

https://www.facebook.com/AssignmentStudio

Twitter:

https://twitter.com/AssignmentStudi

LinkedIn:

https://au.linkedin.com/company/assignment-studio

Pinterest:

http://pinterest.com/assignmentstudi

Table of Contents

Electronic Commerce Security

1 Introduction

1.1 E-Commerce

E-Commerce is a term used to describe a business, commercial transaction or in simple words the selling and buying of products over the internet. It uses many technologies such as transactions over the Internet, marketing on the Internet, mobile E-Commerce, inventory management systems, E-Commerce content management systems etc.

A wide range of businesses are covered by E-Commerce, or it should be said that almost all types of products are being sold on the Internet. The products include music, movies, books, e-books, softwares, clothes, electronics, automobiles and the list just keeps on going. Whatever you can think of is available to be sold on the Internet. E-Commerce has expanded very quickly over the past few years and is expected to keep growing in the future. Even though there's still a distinct difference between conventional and Electronic commerce, this line of difference is expected to blur in a not too distant future.

1.2 Advantages of E-Commerce

The success of E-Commerce is down to many advantages that it offers to the customers and the retailer. Many of these advantages are listed below:

1. The effect of geographical location is minimized. If you are dealing with conventional commerce and you have a store that is present physically on a certain geographical location, then it can only impact that certain area, and can't provide service in a far-off location. While using E-Commerce the effect of geographical location is minimized due to the products availability on the Internet.

2. As the owner of an online store doesn't have to pay for any physical location, and also the number of the people required to manage the store is also reduced significantly, so the products offered by him are available at lower costs, which gives the customer as well as the retailer some advantage.
3. You don't have to go and find the product in a market by roaming around. You can just find any product just by searching it in your web browser, which will save a lot of time and effort.
4. It also reduces the travel time and cost.
5. Information about a product is abundant.

1.3 Disadvantages of E-Commerce

There are many disadvantages to E-Commerce too. The content you are buying is only available for you to see and feel when it is delivered to you. Although you can save time, effort and money by finding and buying the product online, but the delivery of the products can take a long time and this is certainly not an advantage. There are many products which you can't buy on the Internet, not because they are not available, but because they could cause the retailer and the customer a lot of disadvantage. There are many more disadvantages to E-Commerce but the biggest problem being faced is that of security.

1.4 Security

Anything available on the Internet is never entirely safe. The information available over the Internet is more vulnerable to theft or misuse than it is in a physical form. The websites dealing with money transactions are more at risk of being targeted than other websites which deal with other things. The information contained on these websites is highly confidential and requires a lot more security.

The type of crime committed on the Internet is known as electronic crime or, technology crime or cyber-crime. This type of crime use technologies such as phishing, data-theft and payment fraud (Hall, 2008). Softwares which use key-logging or packet sniffing to acquire personal information are very easy available and are not very difficult to use. And when available in the hands of cyber-criminal organizations or individuals, are used to get confidential information about the users to cause damage, or to get financial gain. The most vulnerable to these kinds of attacks are e-commerce websites and their customers. The people involved in these crimes could be of the internal staff or externally could be any criminal organization or individual.

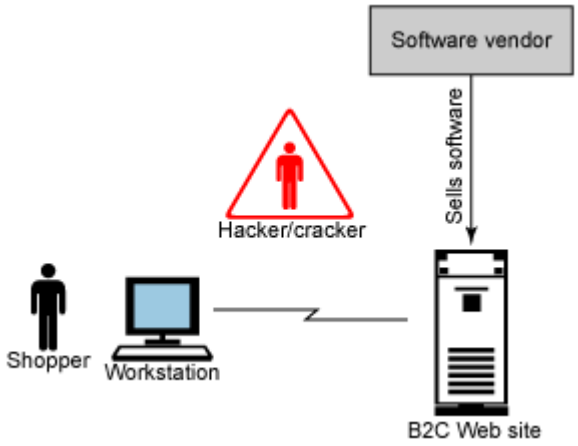
Banking services or applications that are used for e-commerce are targeted by the criminals to get credit card details or the details about the bank account of certain individuals.

2 Working of E-Commerce

There are many popular E-Commerce websites, which have millions of users who are buying their products and are registered with their websites. Two of the most popular websites are Amazaon.com and E-bay. Every E-Commerce website uses different technologies to implement the transactions. We take a look at Amazon.com and how it implements E-Commerce.

Buying a product at amazon is very simple. You start at the amazon.com home page and there's a search box available there. You can simply type the name of the product there and then search for it if it is available or not. If available the page will give you an option to add the product to your Shopping Cart. Shopping cart is a technology used in e-commerce in which you select all the items you want to purchase and then pay at the end, when you have selected all the items. After adding the product to your shopping cart, the shopping cart technology processes the information and displays a list of products you have placed in the shopping cart. From there you have the options of changing the quantity of the products you have added to the shopping cart, removing an item from the shopping cart or adding more items to the shopping cart.

After selecting all the products, you have to place your order and proceed to checkout. After you are ready to place your order, the website will ask you for your information. If you are using the website for the first time, it will ask you to fill your name, shipping address, shipping preference, credit-card information etc. and then assigns you a username and password for all future transactions. If you have used the website before, you can use your username and password to buy the products. (Byron, 1999)



2.1 Security Issues

With all the data that is being entered on this website, it is important that it is kept secure. The credit card information along with the bank account information in the wrong hands could cause a lot of harm to the customer. Also the username and password of the customer can be used to get unfair advantage. The main problem being faced by the Electronic merchants is to provide security to the customers and helping them to distinguish between authentic online stores and fraudulent stores. Many of the websites claim to be online stores doing e-commerce, but take information of the users and then take advantage of it.

3 Security Overview

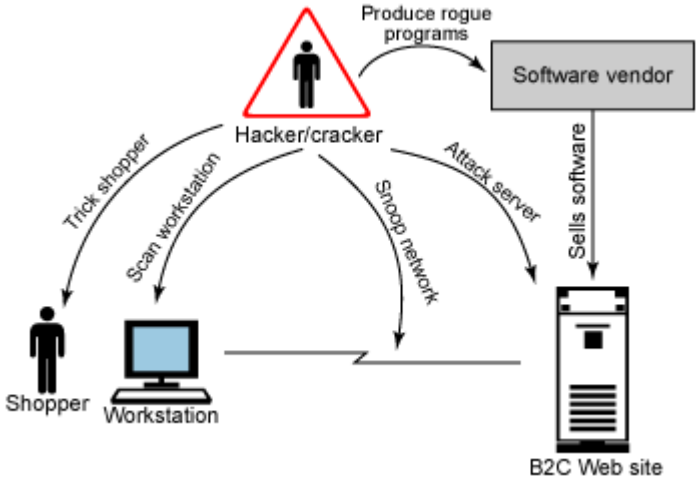
The security of the system has to be implemented at both ends. Making sure that the website is secure, reliable, and providing services which are not prone to being attacked are not enough. You can take an example of securing your house with the latest technologies, and not only one but a

number of them, but still if you still leave your doors unlocked then you are leaving yourself vulnerable to being attacked. Same is the case here; the weakest link in the whole system determines the security of the system. (Khusial, 2005)

4 Vulnerable Points

These are the points an attacker can target.

- Shopper
- Shopper' computer
- Network connection between shopper and Web site's server
- Web site's server
- Software vendor



(Khusial, 2005)

5 Types of Attacks

Following are the types of attacks that the hackers use:

1. Tricking the shopper
2. Getting into the shopper's computer
3. Sniffing the network
4. Password Cracking
5. Denial of Service Attacks
6. Exploiting known bugs in system

5.1 Tricking the shopper

The attackers often use different tricks to get the personal information about the user and then use this information to get the password and username that they use to shop from an online website. Many websites and online stores reset the passwords for their users after asking for personal information. The attackers usually trick the users by calling them and claiming to be

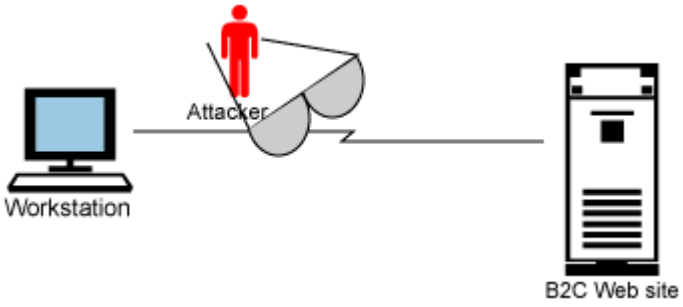
representatives of a site visited, take their information. Then they use this information to get their username or passwords.

5.2 Getting into the shoppers computer

Computer systems are often not secured by the users due to the complexity involved, with such systems, the attackers use softwares to locate ports on the computer and find vulnerable entries. After getting an entry point into the system the attackers can get the required information about the user and take advantage of it.

5.3 Sniffing the network

This technique is used by various hackers and crackers to get information about their target. Softwares are easily available which can be used to sniff all the data sent and forth in between a network. One such software is Cain and Abel and it is available for free. This software can be used to sniff the data being sent on a network, and then even decrypts the information that has been sent in encrypted form. Such kind of attacks is very common.



5.4 Password Cracking

The attackers use different techniques to crack an account of a user. They can either guess the passwords of the users, if they know them closely. For example if you know that your friend uses his family members name as the password to his computer, then this information can be used to guess that that person uses such kind of password for his online shopping account. The password can also be guessed by using automated tools, which use a dictionary to try millions of passwords and see if one opens the account.

5.5 Denial of Service Attacks

Websites work in a client/server manner. Where the website is being run on a server and provides service to the client. Websites can serve a limited amount of users at a given time. So the attackers can use this limitation to their advantage. They can attack the website by accessing their website from a large amount of clients, so that the limit of the website is reached and it can't provide service to the real customers that they have.

5.6 Exploiting the Server Bugs

Websites are run on a server, which is a computer powered on most of the time. Like every other computer a server runs an operating system. Different operating systems have different

vulnerabilities and cannot provide 100% security. The hackers can use this information to exploit these vulnerable points and attack the website.

6 Ways of Defense

With all the vulnerabilities present, the E-commerce business doesn't seem to be secure. But it is not the case. These vulnerabilities can be secured and the user can be provided with a reliable experience. The companies which are authentic have an enormous amount of resources available, and make use of them to provide security to their customers.

Following are the different ways to prevent attacks from hackers:

1. The most responsible party in the E-Commerce business is the merchant. They are responsible for providing a secure website and service to their customers, which makes sure that a minimum amount of threat is posed to their customers.
2. The information of the users should be stored securely and sensitive information should be encrypted.
3. Users can use their education to make sure that they are not vulnerable to being attacked. They should not use weak passwords, which can be guessed or cracked easily. The provider should also store this type of information in a secure manner and should encrypt it before storing it.
4. Where customers order by email, information should be encrypted with PGP or similar software. Or payment should be made by specially encrypted checks and ordering software.
5. Secure Socket Layer is a protocol which is used to encrypt information being sent and forth between the server and the client. When an SSL-protected page is requested, the browser identifies the server as a trusted entity and initiates a handshake to pass encryption key information back and forth
6. Where credit cards are taken online and processed later, it's the merchant's responsibility to check security of the hosting company's webserver. Use a reputable company and demand detailed replies to your queries.
7. Password Policies should be used by the online stores to make sure that their users are never allowed to use passwords which are easy or weak.

7 Bibliography

Byron, L., 1999. *Elcetronic Commerce and Security,* s.l.: Prentice Hall.

Digest, E.-C., 2013. *Internet Security Issues.* [Online]
Available at: http://www.ecommerce-digest.com/staying-safe.html
[Accessed 2013].

Hall, W., 2008. *E-Commerce Security.* [Online]
Available at: https://www.watsonhall.com/e-commerce-security/
[Accessed 8 April 2013].

Iliadis, J., n.d. *E-Commerce Security: a Premer,* s.l.: s.n.

Khusial, D., 2005. *e-Commerce security: Attacks and preventive strategies.* [Online]
Available at: http://www.ibm.com/developerworks/library/co-0504_mckegney/
[Accessed 8 April 2013].

Kumar, P., 2010. *E-Commerce Data Security 2010: Learning From 2009's Debacles.* [Online]
Available at: http://www.ecommercetimes.com/story/69129.html
[Accessed 8 April 2013].

RUSHINEK, A. & RUSHINEK, S., 2002. *E-COMMERCE SECURITY MEASURES.* [Online]
Available at: http://ubiquity.acm.org/article.cfm?id=763945
[Accessed 8 April 2013].

SSC, P., 2013. *PCI SSC Data Security Standards Overview.* [Online]
Available at: https://www.pcisecuritystandards.org/security_standards/index.php
[Accessed 2013].