

# E-commerce & Network Security Attack

Tirth Jain<sup>1</sup>, Jayant Grover<sup>2</sup>, Namit Gupta sir<sup>3</sup>

<sup>1</sup>Student, College of Computing Sciences And Information Technology, Teerthanker Mahaveer University, Moradabad

<sup>2</sup>Student, College of Computing Sciences And Information Technology, Teerthanker Mahaveer University, Moradabad

<sup>3</sup> Associate Professor, College of Computing Sciences And Information Technology, Teerthanker Mahaveer University, Moradabad

[tirth886jain@gmail.com](mailto:tirth886jain@gmail.com)

[jayantgrover7417@gmail.com](mailto:jayantgrover7417@gmail.com)

Abstract: - This short paper introduces about.

**E-Commerce and Network Security Attack.** E-commerce Stand for Electronic commerce. The E-Commerce market is thriving and poised for robust growth in Asia. There are players who made a good beginning. Their success depends on their understanding of the market and offering various types of features.

**Network security Attack** is main issue of this generation of computing because many types of attacks are increasing day by day. Establishing a network is not a big issue for network administrators but protecting the entire network is a big issue. There are various methods and tools are available today for destroying the existing network. In this paper we mainly emphasize on the network security also we present some major issues that can affect our network.

**Keywords—** Introduction of E-commerce, Type of E-commerce, Application of E-commerce, Advantage of E-commerce, Network Security, Threats, Cryptography, Ping.

## I. INTRODUCTION

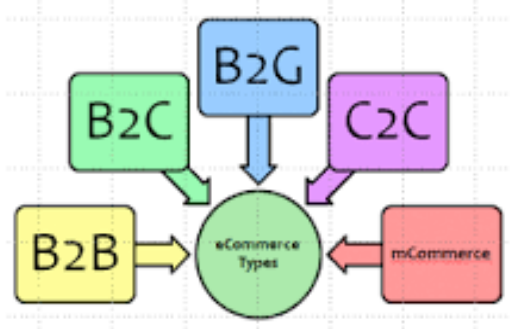


The E-commerce Industry in India has come a long way since its early days. The market has matured and new players have entered the market space. In the present dynamic scenario, ecommerce market in the B2C space is growing in demand as

well as in the array of services. The transition to online purchasing from traditional purchasing is taking a long time in the Indian market. E commerce includes not only buying and selling goods over Internet, but also various business processes within individual organizations that support the goal. As with ecommerce, e-business (electronic business) also has a number of different definitions and is used in a number of different contexts.

The security of network is a big issue for security administrators because network is growing day by day. Security on the Internet and on Local Area Networks is now at the forefront of computer network related issues. Network security consists of the provisions and policies adopted by a network administrator to prevent and monitor unauthorized access, misuse, modification, or denial of a computer network and network-accessible resources. Network security involves the authorization of access to data in a network, which is controlled by the network administrator. Each and every client who is working on the internet wants security of information but sometimes he or she do not know that someone else may be an intruder is collecting the information. Information is an asset that must be protected. Network security is the process by which digital information assets are protected, the goals of security are to protect confidentiality, maintain integrity, and assure availability.

## II. TYPES OF E-COMMERCE



- (i) **B2B** E-Commerce: Companies doing business with each other such as manufacturers selling to distributors and wholesalers selling to retailers. Pricing is based on quantity of order and is often negotiable.
- (ii) **B2C** E-Commerce: Businesses selling to the general public typically through catalogs utilizing shopping cart software. By dollar volume, B2B takes the prize, however B2C is really what the average Joe has in mind with regards to e-commerce as a whole. For example [indiatimes.com](http://indiatimes.com).
- (iii) **C2C** E-Commerce: There are many sites offering free classifieds, auctions, and forums where individuals can buy and sell thanks to online payment systems like PayPal where people can send and receive money online with ease. EBay's auction service is a great example of where customer-to customer transactions take place every day.
- (iv) Others:  
 G2G (Government-to-Government),  
 G2E (Government-to-Employee),  
 G2B (Government-to-Business),  
 B2G (Business-to-Government).  
 M-commerce (Mobile Commerce)

## III. APPLICATION OF E-COMMERCE

The Application of E-commerce are used in various business areas such as retail and Wholesale and manufacturing. The most common E-commerce application are as follow:

### A. Retail and Wholesale:

E-commerce has a number of application in retail and wholesale. E-retailing or on-line retailing is the selling of good from business-to-Consumer through electronic stores that are designed using the electronic catalog and shopping cart model. E.g., Cybermall is a single website that offer different product and services at one Internet location. It attracts the customer and the seller into one virtual space through a web browser.

### B. Marketing:

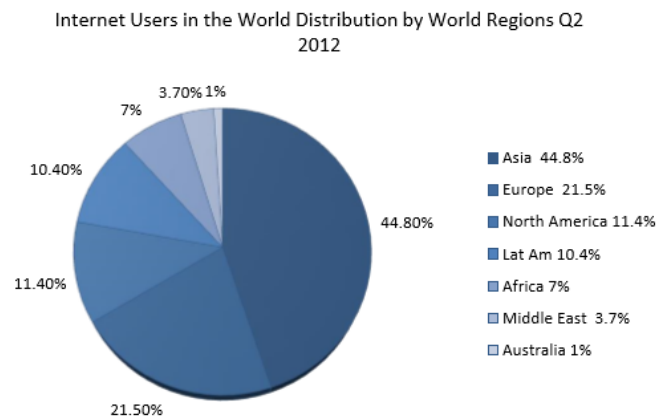
Data Collection about Customer behaviour, preferences, needs and buying pattern is possible through web and E-commerce.

### C. Finance:

Customer can Checks the Balances of their saving and loan account, transfer money to their other Account and pay their bill through on-line banking or E-Banking.

### D. Manufacturing:

E-Commerce is also used in the supply chain operation of companies. Some companies from an electronic exchange by providing together buy and sell good, trade market information and run back office information such as inventory control.



IV. ADVANTAGES OF E-COMMERCE

- Attractive to a significant segment of the demographics for most customer profiles. It can effectively reach the target customer.
- Faster and less expensive to conduct direct marketing campaigns
- Measurable, which means that successes are identifiable and repeatable
- Open 24-hours a day
- Cost-effective, in the long run.

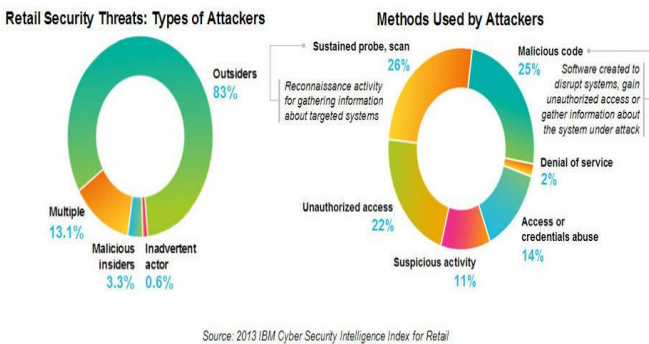
Network Security Attack: -



I. Basic Type of Attack: -

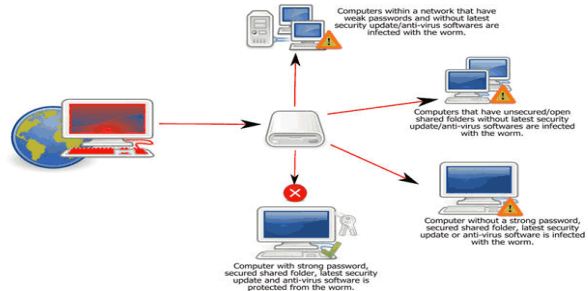
Here we are presenting some basic class of attacks which can be a cause for slow network performance, uncontrolled traffic, viruses etc.

A. Security Threats



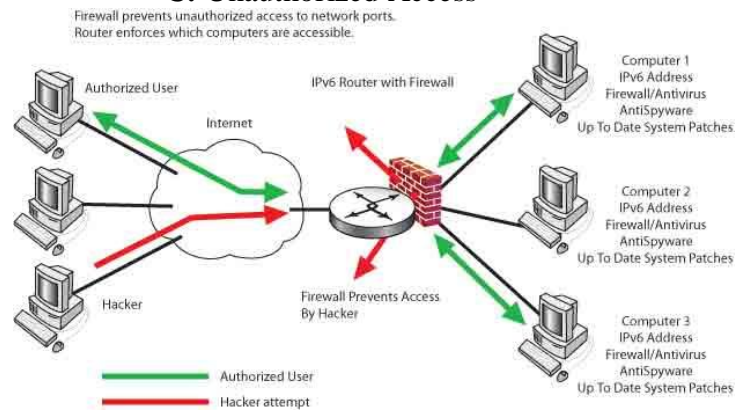
There are a number of security threats that can be the cause of a network security attack. Main security threats are denial of service, distributed denial of service, viruses, Trojan horses, spywares, malwares, unauthorized access to the network resources and data, accidental deletion of the files and the uncontrolled internet access.

B. Virus Attack  
 Worm: Win32 Conficker



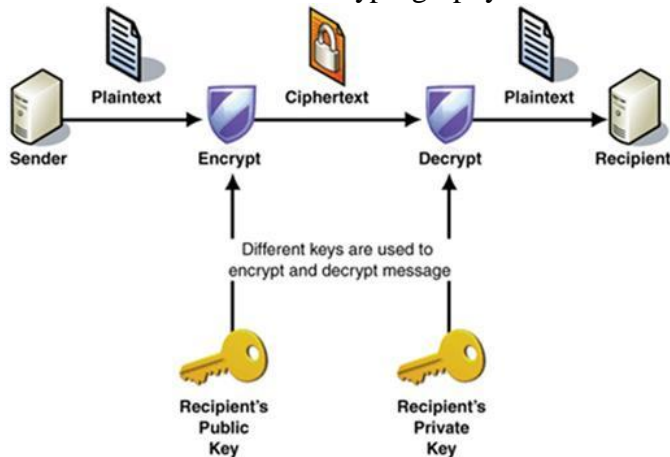
A computer virus is a small program or an executable code that when executed and replicated, perform different unwanted and harmful functions for a computer and a network. Viruses can destroy your hard disks and processors, consume memory at a very large scale and destroy the overall performance of a computer or network. A Trojan is a malicious code that performs harmful actions but it cannot be replicated. Trojan can destroy systems' critical data. A computer worm is a program that replicates to all network and destroy useful data. The viruses, malware, adware and Trojan horses can be prevented if you have an updated antivirus program with the latest pattern files.

C. Unauthorized Access



Access to the network resources and data should be allowed only to the authorized persons. Every shared folder and resources in your network should have been accessed only by the authorized persons and should also be scanned and monitored regularly.

#### D. Theft and cryptography



Another threat to a network is to loss of the important information and this loss can be prevented, if you good encryption methods such as 128 bit security or 256 bit security encryption methods. In this way, your data when transferred through FTP programs, can be encrypted and can't be read or use.

#### E. Unauthorized application

Another virus and security attack prevention method is to install only the authorized software applications to our network server and your all client computers. Nobody should be allowed to install any kind of program which can cause security threats such as songs or video programs, codec, gaming software or other web based applications.

#### F. Application-Level Attacks

The attacker exploits the weakness in the application layer – for example, security weakness in the web server, or in faulty controls in the filtering of an input on the server side. Examples include malicious software attack (viruses, Trojans, etc.), web server attacks, and SQL injection.

#### V. BASIC SECURITY TIPS

This basic Network Security useful security tips and methods to secure your network such as installing a update antivirus program, email scanning programs, network monitoring tools, internet access policy and other security prevention methods. Network security is the most vital component in information security because it is responsible for securing all information passed through networked computers .Network security is a very important aspect of a computer network. Minor security vulnerability can result in a heavy loss of the critical data of your server and other client computers. Keeping the computer as well as network secure, is the big responsibility of the network administrator and the security specialists. There are lot of security measures and prevention methods which I will discuss in this section. Typically a computer network can be attacked by a number of ways such as virus attacks, unauthorized access, cryptography attacks and a number of other security threats. Regularly scan all the network devices, emails, open ports, server and client computers. It's the responsibility of the network administrators to check and deploy the missing security patches in all the network computers. They should also remove the unnecessary network shares, user's accounts, wireless access points and restrict the access to the network users.

#### VI. CONCLUSION

This paper deals the conceptual knowledge of search engine marketing or e-commerce, literature review, current and future aspects of e-commerce in Indian context. This paper discussed about the top motivator factors of shopping online.

There are a number of ways, which guarantee for the safety and security of your network. Perform regular network security testing. Don't provide more or unwanted access to any network user. Must have an updated antivirus program. Operating system should be regularly updated. If you have windows based operating system you can update it

from the Microsoft website. Keep inventory of your network resources such as devices and software applications. Turn off your computer when you are away and don't leave your computer unattended. Put a strong network and system administrator password. Use a switched network, so that you can identify the problem very quickly

#### REFERENCES

- 1) Nisha Chanana, Sangeeta Goel: Introduction of E-commerce.
- 2) Wag mare G.T.: Types of E-commerce.
- 3) <http://www.myreadingroom.co.in/notes-and-studymaterial/66-e-commerce/516-applications-of-e-commerce.html> : Application of E-commerce
- 4) M. Y. Kiang and R. T. Chi: Advantages of E-commerce
- 5) Siddhartha Hansel: Introduction of Network Security
- 6) Simmonds, A; Sandilands, P; van Ekert, L, Chen S., Iyer R., and Whisnant K.: Basic Type of Security Attack, Basic Security Tips.