E-COMMERCE AND SECURITY

WHAT IS E-COMMERCE ?

- e-Commerce refers to the exchange of goods and services over the Internet. All major retail brands have an online presence, and many brands have no associated bricks and mortar presence. However, e-Commerce also applies to business to business transactions, for example, between manufacturers and suppliers or distributors.
- e-Commerce systems are also relevant for the services industry. For example, online banking and brokerage services allow customers to retrieve bank statements online, transfer funds, pay credit card bills, apply for and receive approval for a new mortgage, buy and sell securities, and get financial guidance and information.

TYPES OF ECOMMERCE

There are primarily five types of e-commerce models:

Business to Consumer (B2C)

B2C stands for Business to Consumer as the name suggests, it is the model taking businesses and consumers interaction. Online business sells to individuals. The basic concept of this model is to sell the product online to the consumers.
B2c is the indirect trade between the company and consumers. It provides direct selling through online. For example: if you want to sell goods and services to customer so that anybody can purchase any products directly from supplier's website. Directly interact with the customers is the main difference with other business model. As B2B it manages directly relationship with consumers, B2C supply chains normally deal with business that are related to the customer.

Business to Business (B2B)

B2B stands for Business to Business. It consists of largest form of Ecommerce. This model defines that Buyer and seller are two different entities. It is similar to manufacturer issuing goods to the retailer or wholesaler. Dell deals computers and other associated accessories online but it is does not make up all those products. So, in govern to deal those products, first step is to purchases them from unlike businesses i.e. the producers of those products.

"It is one of the cost effective way to sell out product through out the world"

Benefits:

Encourage your businesses online
Products import and export
Determine buyers and suppliers
Position trade guides

Consumer to Consumer (C2C)

C2C stands for Consumer to Consumer. It helps the online dealing of goods or services among people. Though there is no major parties needed but the parties will not fulfil the transactions without the program which is supplied by the online market dealer such as eBay.

Peer to Peer (P2P)

It is a discipline that deal itself which assists people to instantly shares related computer files and computer sources without having to interact with central web server. If you are going to implement this model, both sides demand to install the expected software so that they could able to convey on the mutual platform.

This kind of e-commerce has very low revenue propagation as from the starting it has been tended to the release of use due to which it sometimes caught involved in cyber laws.

M-Commerce

It deals with conducting the transactions with the help of mobile. The mobile device consumers can interact each other and can lead the business. Mobile Commerce involves the change of ownership or rights to utilize goods and related services.

ADVANTAGES OF E-COMMERCE

- It enables a business concern or individual to reach the global market.
- It caters to the demands of both the national and the international market, as your business activities are no longer restricted by geographical boundaries.
- Even time restrictions are nonexistent while conducting businesses, as e-commerce empowers one to execute business transactions 24 hours a day and even on holidays and weekends.

- Electronic commerce gives the customers the opportunity to look for cheaper and quality products.
- consumers can easily research on a specific product and sometimes even find out the original manufacturer to purchase a product at a much cheaper price than that charged by the wholesaler.
- Shopping online is usually more convenient and time saving than conventional shopping.
- e-commerce significantly cuts down the cost associated with marketing, customer care, processing, information storage and inventory management.
- Electronic commerce reduces the burden of infrastructure to conduct businesses and thereby raises the amount of funds available for profitable investment.

DISADVANTAGES OF E-COMMERCE

- the Internet has still not touched the lives of a great number of people, either due to the lack of knowledge or trust. A large number of people do not use the Internet for any kind of financial transaction. Some people simply refuse to trust the authenticity of completely impersonal business transactions, as in the case of e-commerce.
- Many people have reservations regarding the requirement to disclose personal and private information for security concerns. Many times, the legitimacy and authenticity of different e-commerce sites have also been questioned.

- It is not suitable for perishable commodities like food items. People prefer to shop in the conventional way than to use e-commerce for purchasing food products. So e-commerce is not suitable for such business sectors. The time period required for delivering physical products can also be quite significant in case of e-commerce.

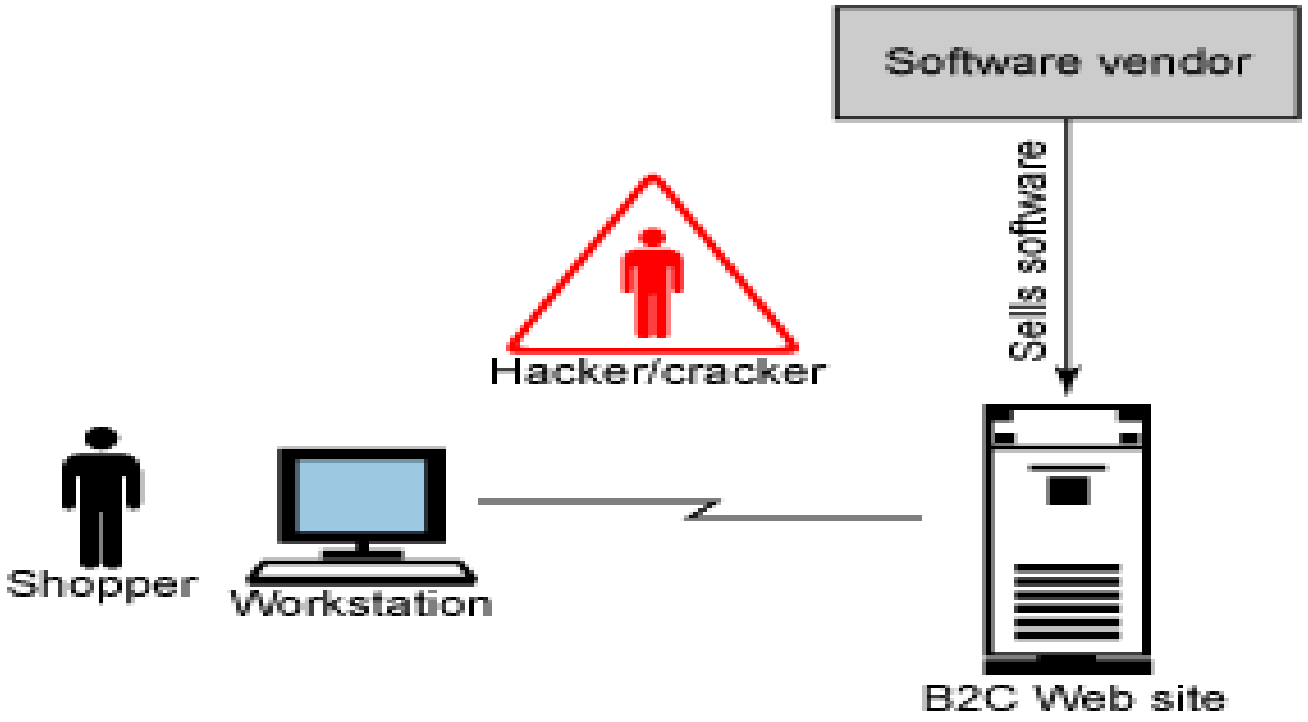
PLAYERS IN E-COMMERCE

- One player is the shopper who uses his browser to locate the site.
- The site is usually operated by a merchant, also a player, whose business is to sell merchandise to make a profit.
- . The software vendor is the last of the three legitimate players.
- . The attacker is the player whose goal is to exploit the other three players for illegitimate gains.

THE PLAYER IN E COMMERCE

- One player is the **SHOPPER** who uses his browser to locate the site.
- The site is usually operated by a **merchant**, also a player, whose business is to sell merchandise to make a profit.
- As the merchant business is selling goods and services, not building software, he usually purchases most of the software to run his site from third party **SOFTWARE VENDOR.**
- **ATTACKER** is the player whose goal is to exploit the other three players for illegitimate gains.

PLAYERS IN E-COMMERCE



SECURITY FEATURES

While security features do not guarantee a secure system, they are necessary to build a secure system. Security features have four categories:

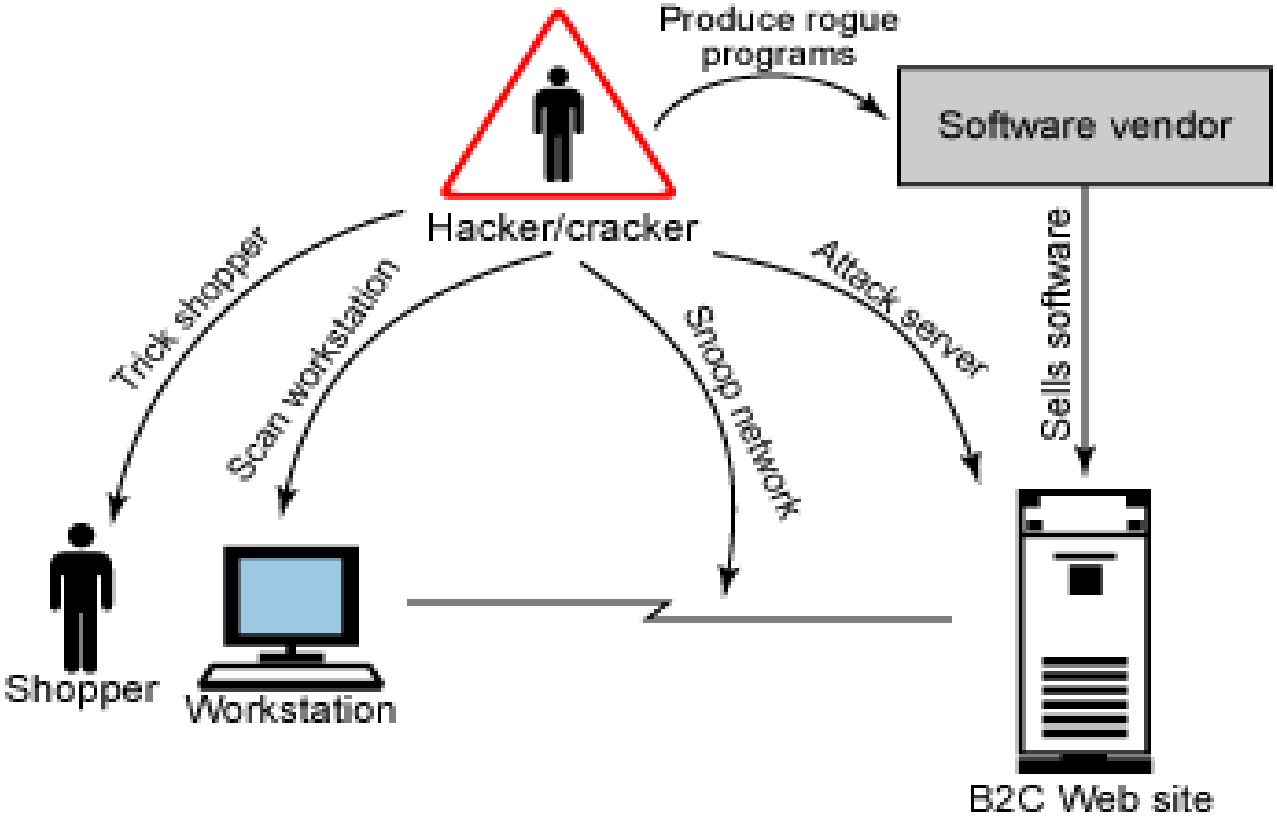
- Authentication: Verifies who you say you are. It enforces that you are the only one allowed to logon to your Internet banking account.
- Authorization: Allows only you to manipulate your resources in specific ways. This prevents you from increasing the balance of your account or deleting a bill.
- Encryption: Deals with information hiding. It ensures you cannot spy on others during Internet banking transactions.
- Auditing: Keeps a record of operations. Merchants use auditing to prove that you bought a specific merchandise.

POINT THE ATTACKER CAN TARGET

As mentioned, the vulnerability of a system exists at the entry and exit points within the system. Figure shows an e-Commerce system with several points that the attacker can target:

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

POINT THE ATTACKER CAN TARGET



SECURITY THREATS TO ECOMMERCE

Most businesses that have made the move towards an online presence have experienced some kind of security threat to their business. Since the Internet is a public system in which every transaction can be tracked, logged, monitored and stored in many locations, it is important for businesses to understand possible security threats to their business.

There are many threats to e-commerce that may come from sources within an organization or through some external channel. The following are the top corporate security threats categorized by internal and external threats.

- Unauthorized internal users who accesses confidential information by using a stolen passwords for the purpose of committing fraud or theft.
- Former employees of an organization that maintain access to information resources directly by creating alternative passwords, “back doors” into the computer system, or indirectly through former co-workers.
- Weak access points in information infrastructure and security that can expose company information and trade secrets.
- Management that undermines security is maybe the greatest risk to e-commerce as there.
- Contractors, partners, consultants, and temps who take advantage of even limited access to important systems.
- Peoples mentality on Internet security is changing this is evident through the increase in sales of antivirus software and subscriptions to email virus protection.
- Businesses may take Visa’s lead of requiring its service providers and merchants to have firewalls, encryption, as well as testing and access policies as a condition of doing business with them. They feel that the security of their B2B partner is as important as their creditworthiness.

SECURITY THREATS TO E COMMERCE

A secure system accomplishes its task with no unintended side effects. Using the analogy of a house to represent the system, you decide to carve out a piece of your front door to give yours pets easy access to the outdoors. Security has three main concepts:

1. confidentiality:
2. Integrity
3. Availability

CONFIDENTIALITY

Confidentiality is the protection of information in the system so that unauthorized persons cannot access it. Many believe this type of protection is of most importance to military and government organizations that need to keep plans and capabilities secret from potential enemies. However, it can also be significant to businesses that need to protect proprietary trade secrets from competitors or prevent unauthorized persons from accessing the company's sensitive information (e.g., legal, personnel, or medical information).
Confidentiality must be well defined, and procedures for maintaining confidentiality must be carefully implemented, especially for standalone computers. A crucial aspect of confidentiality is user identification and authentication

INTEGRITY

Integrity is the protection of system data from intentional or accidental unauthorized changes. The challenge of the security program is to ensure that data is maintained in the state that users expect. Although the security program cannot improve the accuracy of data that is put into the system by users, it can help ensure that any changes are intended and correctly applied.

Examples of government systems in which integrity is crucial include air traffic control systems, military fire control systems (which control the firing of automated weapons), and Social Security and welfare systems. Examples of commercial systems that require a high level of integrity include medical prescription systems, credit reporting systems, production control systems, and payroll systems.

AVAILABILITY

Availability is the assurance that a computer system is accessible by authorized users whenever needed. Two facets of availability are typically discussed:

1. Denial of service.

2. Loss of data processing capabilities as a result of natural disasters (e.g., fires, floods, storms, or earthquakes) or human actions (e.g., bombs or strikes).

Denial of service usually refers to actions that tie up computing services in a way that renders the system unusable by authorized users. For example, the Internet worm overloaded about 10% of the computer systems on the network, causing them to be nonresponsive to the needs of users.

The loss of data processing capabilities as a result of natural disasters or human actions is perhaps more common. Such losses are countered by contingency planning, which helps minimize the time that a data processing capability remains unavailable.

SECURITY FEATURES

- Authentication: It verifies that you are the only one allowed to logon to your internet banking account.
- Authorization: It allows only you to manipulate your resources in specific ways.
- Encryption: It deals with information hiding. It ensures you cannot spy on others during internet banking transaction.
- Auditing: keeps a record of operations. Merchants use auditing to prove that you bought a specific merchandise.

VIRTUAL ORGANIZATION

You might ask yourself the question

"Why do we need to go to a specific physical place to work?".

- The answer often is that either "this is where the people that you work with are" or "that this is where you find the information you need as well as the means to process it"- in summary where your office is.
- But what if you no longer had to go to this place to contact the people or get the information? Instead all this could be done electronically and you and everyone else would do their work from any location.

ATTACKS

This section describes potential security attack methods from an attacker or hacker.

Tricking the shopper

Some of the easiest and most profitable attacks are based on tricking the shopper, also known as social engineering techniques. These attacks involve surveillance of the shopper's behavior, gathering information to use against the shopper.

A common scenario is that the attacker calls the shopper, pretending to be a representative from a site visited, and extracts information. The attacker then calls a customer service representative at the site, posing as the shopper and providing personal information. The attacker then asks for the password to be reset to a specific value.

SNOOPING THE SHOPPER'S COMPUTER

Millions of computers are added to the Internet every month. Most users' knowledge of security vulnerabilities of their systems is vague at best. Additionally, software and hardware vendors, in their quest to ensure that their products are easy to install, will ship products with security features disabled. In most cases, enabling security features requires a non-technical user to read manuals written for the technologist. The confused user does not attempt to enable the security features. This creates a treasure trove for attackers.

A popular technique for gaining entry into the shopper's system is to use a tool, such as SATAN, to perform port scans on a computer that detect entry points into the machine. Based on the opened ports found, the attacker can use various techniques to gain entry into the user's system. Upon entry, they scan your file system for personal information, such as passwords.

While software and hardware security solutions available protect the public's systems, they are not silver bullets. A user that purchases firewall software to protect his computer may find there are conflicts with other software on his system. To resolve the conflict, the user disables enough capabilities to render the firewall software useless.

SNIFFING THE NETWORKS

GUESSING PASSWORDS

WHAT MAKES A VIRTUAL ORGANIZATION DIFFERENT?

- It removes many barriers - especially that of time and location.
- It emphasizes concentrating on new services and products, especially those with intensive information and knowledge characteristics, rather than concentrating on cost savings made possible by removing the barriers.
- **It goes beyond outsourcing and strategic alliances** and is more flexible in:
- that it has continuously changing partners,
- the arrangements are loose and goal oriented,
- emphasizes the use of knowledge to create new products and services,
- its processes can change quickly by agreement of the partners.

What are the steps to a virtual organization?

Often the steps here go through:
•outsourcing mainly to reduce costs where there is some experience in working at a distance, but three is one dominant party and high certainty of what everyone must do.
•forming strategic alliances to share the work and gain experience in developing and sharing common goals. Here there is no dominant party although the parties are fixed. and
•then becoming virtual organizations to achieve flexibility. Now the partners themselves can quickly change, with greater emphasis on the use of knowledge to create new and innovative products.
It is of course possible for only a part of an organization to become virtual. In that case organizations can gradually evolve from real to virtual. Typical virtual structures can include:

What are the steps to a virtual organization?

Virtual Team	Here team roles are defined as needed and people are chosen to fill the roles depending on their expertise.
Virtual Laboratory (Collaboratories)	In this case laboratory participants can be experts from anywhere, who are called to contribute to a project whenever particular expertise is needed.
Virtual Office	Here office roles may be assigned to people who are only called upon to carry out office duties when needed.
Virtual Shops	Here the shop products can quickly change with different vendors becoming part of the virtual shopping center.
Virtual Organization	Here the entire organizartion is virtual.

In all cases virtual implies:
Continually changing membership of participants,
Self-management within teams and units,
Knowledge (not structure) oriented work.

Why virtual?

What are the reasons for organizations becoming virtual. These include:

- Globalization, with growing trends to include global customers,
- Ability to quickly pool expert resources,
- Creation of communities of excellence,
- Rapidly changing needs,
- Increasingly specialized products and services,
- Increasing required to use specialized knowledge

Working electronically.

In a virtual organization all places of work would be through communication using computer workspaces. You can the go from electronic workplace to workplace to see the activities that are taking place in the organization.
A number of people can structure electronic workspace networks to establish the relationships needed to function as an organization.

HOW TO STRUCTURE ELECTRONIC WORKSPACES?

Workplace structures must mirror the way that a virtual organization works.

They must easily grow and evolve with the virtual organization. To do this they must support the organization's mission by developing and using information consistently with the mission.

Workspaces should mahke it easy to:

- create new roles and assign peoiple to them,change goals,
- add new documents,
- set up new communication links between people.

HOW TO STRUCTURE ELECTRONIC WORKSPACES?

Typical structures include:

•A production system where there is a workplace for each production task. As one task completes it activates the workpace for the next task. bIt should be possible to easily create a new task and provide a workspace for it.

•Design systems where people in a design can "meet" at an electronic workspace to discuss coordination issues. They then go to their individual workspaces to carry out their part of the design.

BENEFITS

•VOs make it possible to satisfy constantly changing customer and market requirements in a competitive manner . The access to market increases.
•It becomes possible to provide services precisely tailored to a specific customer need.
•An ability to participate in VOs increases the total service range a company can offer to its customers
•Participation in VOs increases the total number of end-customers a company can reach indirectly via its partners.
•A particular organization can both “multiply itself” virtually by participating in several VOs and initiate a VO that will be constituted from different parties. This creates the possibility for coexistence of the opposites in one organization.
•By participation in a VO the concept-to-cash time is reduced.

SECURITY RISKS

The main challenges related to the trust establishment are:

•Each party has its own policies on access control and conditions of use.

•VO parties need to establish trust between them on a peer-to-peer basis.

•Parties may be located in different countries under different jurisdictions and, as a consequence, adhere to different legal and business requirements.

•Since VOs rely on IT, exposure to fraud or misuse of technology is a major concern.

•Security systems of VO partners must be mutually trusted. This brings up the challenge to come up with an effective and flexible security system.

•Contract management needs to be effective in order to be able to quickly reconfigure in VOs. Services for management of electronic contracts must be trusted.

•Confidentiality, privacy, integrity availability and accountability at a VO level have to be assured. At the same time parties have to provide access to their services and resources, as specified in agreements.

Trust is established by the means of digital identities, certification, access control mechanisms, authentication, secure connection, reputation and inspection of the parties.