Technologies

Different Types of Networking For E-Commerce:

Internet:

The Internet is a global network of computers that allows people to send email, view web sites, download files such as mp3 and images, chat, post messages on newsgroups and forums and much more.

The Internet was created by the Advanced Research Projects Agency (ARPA) of the U.S. government in 1960's and was first known as the ARPANet. At this stage the Internet's first computers were at academic and government institutions and were mainly used for accessing files and to send emails. From 1983 onwards the Internet as we know it today started to form with the introduction of the communication protocol TCP/IP to ARPANet. Since 1983 the Internet has accommodated a lot of changes and continues to keep developing.

The last two decades has seen the Internet accommodate such things as network LANs and ATM and frame switched services. The Internet continues to evolve with it becoming available on mobile phones and pagers and possibly on televisions in the future.

Advantages of internet:

There many advantages to using the internet such as:

E-mail

Email is now an essential communication tool in business. It is also excellent for keeping in touch with family and friends. The advantage to email is that it is free (no charge per use) when compared to telephone, fax and postal services.

Information

There is a huge amount of information available on the internet for just about every subject known to man, ranging from government law and services, trade fairs and conferences, market information, new ideas and technical support.

Services

Many services are now provided on the internet such as online banking, job seeking and applications, and hotel reservations. Often these services are not available off-line or cost more.

Buy or sell products.

The internet is a very effective way to buy and sell products all over the world.

Communities communities of all types have sprung up on the internet. Its a great way to meet up with people of similar interest and discuss common issues.

A Leading-Edge Image

Presenting your company or organization as leading-edge shows your customers and prospective customers that you are financially strong, technologically savvy, and ready for the 21st century. And that you care enough about your customers to take advantage of new technologies for their benefit. And finally that you have the resources to support your clients in the most beneficial manner possible.

More and more advertisers on television, radio, magazines, and newspapers are including a Web address. Now is the time to avoid playing catch-up later.

Improved Customer Service

The companies are available to their customers 24 hours a day, 7 days a week. The Internet never sleeps. Whenever customer needs information about any company, products or services, they can access the company's Web Page.

Market Expansion

The Internet is a global system. Latest estimates are that there are about 40 million people with access to the Internet, and this number is growing every day. By simply posting a Web Page you are also addressing International markets.

Low Cost Marketing

Imagine developing a full color brochure without having to incur the costs of proofs, printers, wasted paper, long lead times between revisions, and more. Then imagine a full color product or services brochure that is interactive and which incorporates text, graphics, audio, and/or video. One that can be immediately updated without incurring the usual costs of product material updates.

Low Cost Selling

Without the cost of direct selling potential customers can get detailed information about your products or services at any time. And they can easily order your products over the Internet, or request additional information be sent to them via a request form on your Web page.

Lower Communication Costs

Your time, and your employees time, is valuable. Most businesses and organizations spend time answering the same questions over and over again. With a Web page you can make the answers available to everyone immediately. You can also update your Wed page with new information quickly and easily.

Intranet:

- An intranet is a computer network that uses Internet Protocol technology to share information, operational systems, or computing services within an organization. This term is used in contrast to extranet, a network between organizations, and instead refers to a network within an organization.
- The objective is to organize each individual's desktop with minimal cost, time and effort to be more productive, cost efficient, timely, and competitive.
- An intranet may host multiple private websites and constitute an important component and focal point of internal communication and collaboration.
- Any of the well known Internet protocols may be found in an intranet, such as HTTP (web services), SMTP (e-mail), and FTP (file transfer protocol). Internet technologies are often deployed to provide modern interfaces to legacy information systems hosting corporate data.

Uses of Intranet:

- Increasingly, intranets are being used to deliver tools, e.g. collaboration (to facilitate working in groups and teleconferencing) or sophisticated corporate directories, sales and customer relationship management tools, project management etc., to advance productivity.
- Intranets are also being used as corporate culture-change platforms. For example, large numbers of employees discussing key issues in an intranet forum application could lead to new ideas in management, productivity, quality, and other corporate issues.
- In large intranets, website traffic is often similar to public website traffic and can be better understood by using web metrics software to track overall activity. User surveys also improve intranet website effectiveness. Larger businesses allow users within their intranet to access public internet through firewall servers. They have the ability to screen messages coming and going keeping security intact.
- When part of an intranet is made accessible to customers and others outside the business, that part becomes part of an extranet. Businesses can send private messages through the public network, using special encryption/decryption and other security safeguards to connect one part of their intranet to another.
- Intranet user-experience, editorial, and technology teams work together to produce in-house sites. Most commonly, intranets are managed by the communications, HR or CIO departments of large organizations, or some combination of these.

- Because of the scope and variety of content and the number of system interfaces, intranets of many organizations are much more complex than their respective public websites. Intranets and their use are growing rapidly.

Advantages:

- **Workforce productivity**: Intranets can help users to locate and view information faster and use applications relevant to their roles and responsibilities. With the help of a web browser interface, users can access data held in any database the organization wants to make available, anytime and — subject to security provisions — from anywhere within the company workstations, increasing employees' ability to perform their jobs faster, more accurately, and with confidence that they have the right information.
- **Time**: Intranets allow organizations to distribute information to employees on an *as-needed* basis; Employees may link to relevant information at their convenience, rather than being distracted indiscriminately by email.
- **Communication**: Intranets can serve as powerful tools for communication within an organization, vertically strategic initiatives that have a global reach throughout the organization. By providing this information on the intranet, staff have the opportunity to keep up-to-date with the strategic focus of the organization. Some examples of communication would be chat, email, and/or blogs. A great real world example of where an intranet helped a company communicate is when Nestle had a number of food processing plants in Scandinavia. Their central support system had to deal with a number of queries every day.
- **Web publishing**: allows cumbersome corporate knowledge to be maintained and easily accessed throughout the company using hypermedia and Web technologies. Examples include: employee manuals, benefits documents, company policies, business standards, news feeds, and even training, can be accessed using common Internet standards (Acrobat files, Flash files, CGI applications). Because each business unit can update the online copy of a document, the most recent version is usually available to employees using the intranet.
- **Business operations and management**: Intranets are also being used as a platform for developing and deploying applications to support business operations and decisions across the internetworked enterprise.
- **Cost-effective**: Users can view information and data via web-browser rather than maintaining physical documents such as procedure manuals, internal phone list and requisition forms. This can potentially save the business money on printing, duplicating

documents, and the environment as well as document maintenance overhead.

- **Enhance collaboration**: Information is easily accessible by all authorised users, which enables teamwork.
- **Cross-platform capability**: Standards-compliant web browsers are available for Windows, Mac, and UNIX.
- **Built for one audience**: Many companies dictate computer specifications which, in turn, may allow Intranet developers to write applications that only have to work on one browser (no cross-browser compatibility issues).
- **Promote common corporate culture**: Every user has the ability to view the same information within the Intranet.
- **Immediate updates**: When dealing with the public in any capacity, laws, specifications, and parameters can change. Intranets make it possible to provide your audience with "live" changes so they are kept up-to-date, which can limit a company's liability.
- **Supports a distributed computing architecture:** The intranet can also be linked to a company's management information system, for example a time keeping system.

Security Threats to E-commerce:

E-Commerce security requirements can be studied by examining the overall process, beginning with the consumer and ending with the commerce server. Considering each logical link in the commerce chain, the assets that must be protected to ensure secure e-commerce include client computers, the messages travelling on the communication channel, and the web and commerce servers – including any hardware attached to the servers. While telecommunications are certainly one of the major assets to be protected, the telecommunications links are not the only concern in computer and e-commerce security. For instance, if the telecommunications links were made secure but no security measures were implemented for either client computers or commerce and web-servers, then no communications security would exist at all.

Client threats

Until the introduction of executable web content, Web pages were mainly static. Coded in HTML, static pages could do little more than display content and provide links to related pages with additional information. However, the widespread use of active content has changed this perception.

Active content: Active content refers to programs that are embedded transparently in web pages and that cause action to occur. Active content can display moving graphics, download and play audio, or implement web-based spreadsheet programs. Active content is used in e-commerce to place items one wishes to purchase into a shopping cart and to compute the total invoice amount, including sales tax, handling, and shipping costs. The best known active content forms are Java applets, ActiveX controls, JavaScript, and VBScript.

Malicious codes: Computer viruses, worms and trojan horses are examples of malicious code. A trojan horse is a program which performs a useful function, but performs an unexpected action as well. Virus is a code segment which replicates by attaching copies to existing executables. A worm is a program which replicates itself and causes execution of the new copy. These can create havoc on the client side.

Server-side masquerading*:* Masquerading lures a victim into believing that the entity with which it is communicating is a different entity. For example, if a user tries to log into a computer across the internet but instead reaches another computer that claims to be the desired one, the user has been spoofed. This may be a passive attack (in which the user does not attempt to authenticate the recipient, but merely accesses it), but it is usually an active attack.

Communication channel threats

The internet serves as the electronic chain linking a consumer (client) to an e-commerce resource. Messages on the internet travel a random path from a source node to a destination node. The message passes through a number of intermediate computers on the network before reaching the final destination. It is impossible to guarantee that every computer on the internet through which messages pass is safe, secure, and non-hostile.

Confidentiality threats: Confidentiality is the prevention of unauthorized information disclosure. Breaching confidentiality on the internet is not difficult. Suppose one logs onto a website – say www.anybiz.com – that contains a form with text boxes for name, address, and e-mail address. When one fills out those text boxes and clicks the submit button, the information is sent to the web-server for processing. One popular method of transmitting data to a web-server is to collect the text box responses and place them at the end of the target server's URL. The captured data and the HTTP request to send the data to the server is then sent. Now, suppose the user changes his mind, decides not to wait for a response from the anybiz.com server, and jumps to another website instead – say www.somecompany.com. The server somecompany.com may choose to collect web demographics and log the URL from which the user just came (www.anybiz.com). By doing this, somecompany.com has breached confidentiality by recording the secret information the user has just entered.

Integrity threats: An integrity threat exists when an unauthorized party can alter a message stream of information. Unprotected banking transactions are subject to integrity violations. Cyber vandalism is an example of an integrity violation. Cyber vandalism is the electronic defacing of an existing website page. Masquerading or spoofing – pretending to be someone you are not or representing a website as an original when it really is a fake – is one means of creating havoc on websites. Using a security hole in a domain name server (DNS), perpetrators can substitute the address of their website in place of the real one to spoof website visitors. Integrity threats can alter vital financial, medical, or military information. It can have very serious consequences for businesses and people.

Availability threats: The purpose of availability threats, also known as delay or denial threats, is to disrupt normal computer processing or to deny processing entirely. For example, if the processing speed of a single ATM machine transaction slows from one or two seconds to 30 seconds, users will abandon ATM machines entirely. Similarly, slowing any internet service will drive customers to competitors' web or commerce sites.

Server threats

The server is the third link in the client-internet-server trio embodying the e-commerce path between the user and a commerce server. Servers have vulnerabilities that can be exploited by anyone determined to cause destruction or to illegally acquire information.

Web-server threats: Web-server software is designed to deliver web pages by responding to HTTP requests. While web-server software is not inherently high-risk, it has been designed with web service and convenience as the main design goal. The more complex the software is, the higher the probability that it contains coding errors (bugs) and security holes – security weaknesses that provide openings through which evildoers can enter.

Commerce server threats: The commerce server, along with the web-server, responds to requests from web browsers through the HTTP protocol and CGI scripts. Several pieces of software comprise the commerce server software suite, including an FTP server, a mail server, a remote login server, and operating systems on host machines. Each of this software can have security holes and bugs.

Database threats: E-commerce systems store user data and retrieve product information from databases connected to the web-server. Besides product information, databases connected to the web contain valuable and private information that could irreparably damage a company if it were

disclosed or altered. Some databases store username/password pairs in a non-secure way. If someone obtains user authentication information, then he or she can masquerade as a legitimate database user and reveal private and costly information.

Common gateway interface threats: A common gateway interface (CGI) implements the transfer of information from a web-server to another program, such as a database program. CGI and the programs to which they transfer data provide active content to web pages. Because CGIs are programs, they present a security threat if misused. Just like web-servers, CGI scripts can be set up to run with their privileges set to high – unconstrained. Defective or malicious CGIs with free access to system resources are capable of disabling the system, calling privileged (and dangerous) base system programs that delete files, or viewing confidential customer information, including usernames and passwords.

Password hacking: The simplest attack against a password-based system is to guess passwords. Guessing of passwords requires that access to the complement, the complementation functions, and the authentication functions be obtained. If none of these have changed by the time the password is guessed, then the attacker can use the password to access the system.

Security Requirements For E-Commerce:

Authentication:

This is the ability to say that an electronic communication (whether via email or web) does genuinely come from who it purports to.Without face-to-face contact, passing oneself off as someone else is not difficult on the internet.

In online commerce the best defence against being misled by an imposter is provided by unforgeable digital certificates from a trusted authority (such as VeriSign). Although anyone can generate digital certificates for themselves, a trusted authority demands real-world proof of identity and checks its validity before issuing a digital certificate. Only certificates from trusted authorities will be automatically recognized and trusted by the major web browser and email client software.

Authentication can be provided in some situations by physical tokens (such as a drivers license), by a piece of information known only to the person involved (eg. a PIN), or by a physical property of a person (fingerprints or retina scans). Strong authentication requires at least two or more of these. A digital certificate provides strong authentication as it is a unique token and requires a password for its usage.

Privacy:

In online commerce, privacy is the ability to ensure that information is accessed and changed only by authorized parties. Typically this is achieved via encryption. Sensitive data (such as credit card details, health records, sales figures etc.) are encrypted before being transmitted across the open internet – via email or the web. Data which has been protected with strong 128-bit encryption may be intercepted by hackers, but cannot be decrypted by them within a short time. Again, digital certificates are used here to encrypt email or establish a secure HTTPS connection with a web-server. For extra security, data can also be stored long-term in an encrypted format.

Authorization:

Authorization allows a person or computer system to determine if someone has the authority to request or approve an action or information. In the physical world, authentication is usually achieved by forms requiring signatures, or locks where only authorized individuals hold the keys.

Authorization is tied with *authentication*. If a system can securely verify that a request for information (such as a web page) or a service (such as a purchase requisition) has come from a known individual, the system can then check against its internal rules to see if that person has sufficient authority for the request to proceed.

In the online world, authorization can be achieved by a manager sending a digitally signed email. Such an email, once checked and verified by the recipient, is a legally binding request for a service. Similarly, if a web-server has a restricted access area, the server can request a digital certificate from the user's browser to identify the user and then determine if they should be given access to the information according to the server's permission rules.

Integrity:

Integrity of information means ensuring that a communication received has not been altered or tampered with. Traditionally, this problem has been dealt with by having tight control over access to paper documents and requiring authorized officers to initial all changes made – a system with obvious drawbacks and limitations. If someone is receiving sensitive information

online, he not only wants to ensure that it is coming from who he expects it to (authentication), but also that it hasn't been intercepted by a hacker while in transit and its contents altered. The speed and distances involved in online communications requires a very different approach to this problem from traditional methods.

One solution is afforded by using digital certificates to digitally "sign" messages. A travelling employee can send production orders with integrity to the central office by using their digital certificate to sign their email. The signature includes a hash of the original message – a brief numerical representation of the message content. When the recipient opens the message, his email software will automatically create a new hash of the message and compare it against the one included in the digital signature. If even a single character has been altered in the message, the two hashes will differ and the software will alert the recipient that the email has been tampered with during transit.

Non-repudiation:

Non-repudiation is the ability to guarantee that once someone has requested a service or approved an action. Non-repudiation allows one to legally prove that a person has sent a specific email or made a purchase approval from a website. Traditionally non-repudiation has been achieved by having parties sign contracts and then have the contracts notarized by trusted third parties. Sending documents involved the use of registered mail, and postmarks and signatures to date-stamp and record the process of transmission and acceptance. In the realm of e-commerce, non repudiation is achieved by using digital signatures. Digital signatures which have been issued by a trusted authority (such as VeriSign) cannot be forged and their validity can be checked with any major email or web browser software. A digital signature is only installed in the personal computer of its owner, who is usually required to provide a password to make use of the digital signature to encrypt or digitally sign their communications. If a company receives a purchase order via email which has been digitally signed, it has the same legal assurances as on receipt of a physical signed contract.

REFERENCE

Cyber Law: Intellectual Property and E-Commerce Security Hardcover – January 1, 2011

by Kumar & Sharma (Author)

Cyberlaw and E-Commerce 1st Edition by David Lee Baumer (Author), J. C. Poindexter (Author)

CYBER LAW AND E COMMERCE IN 60 MINUTES Jun 3, 2014 by sukhdarshan sehgal

Managing Cyber Attacks in International Law, Business, and Relations: In Search of Cyber Peace Jul 10, 2014 by Scott J. Shackelford