INTRODUCTION TO ELECTRONIC COMMERCE

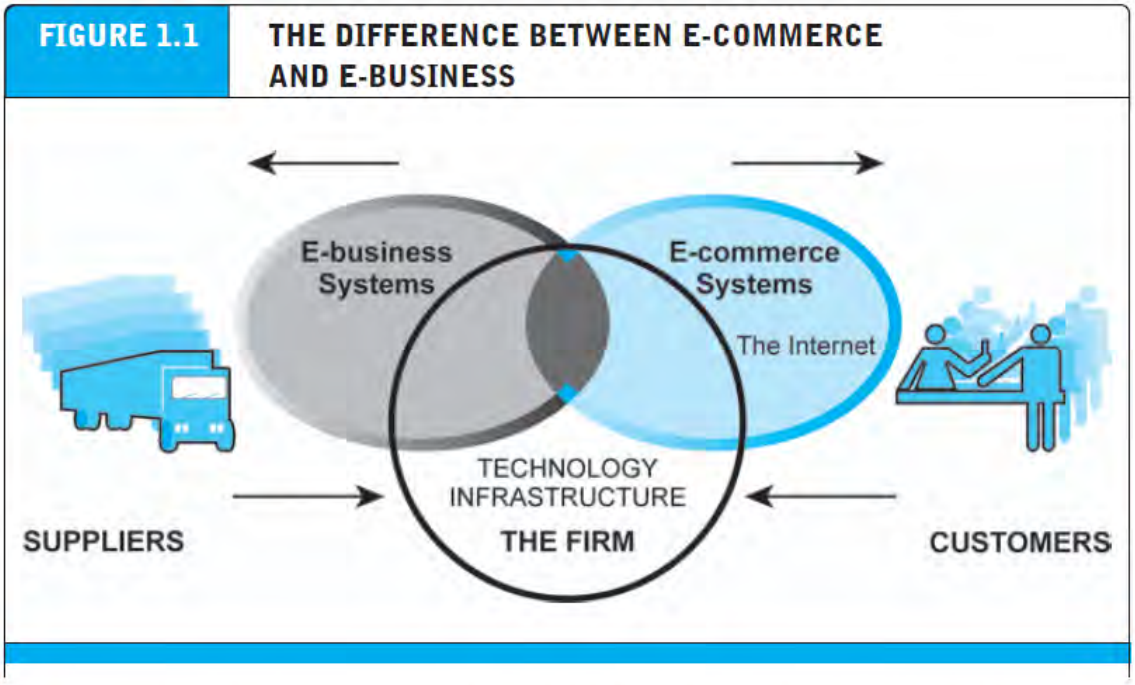
Electronic commerce (e-commerce) remains a relatively new, emerging and constantly changing area of business management and information technology. E-commerce is digitally enabled commercial transactions between and among organizations and individuals. *Digitally enabled transactions* include all transactions mediated by digital technology e.g. Internet. For the most part, this means transactions that occur over the Internet and the Web. *Commercial transactions* involve the exchange of value (e.g., money) across organizational or individual boundaries in return for products and services. Exchange of value is important for understanding the limits of e-commerce. Without an exchange of value, no commerce occurs.

Some of the definitions of e-commerce often heard and found in publications and the media are:

- Electronic Commerce (EC) is where business transactions take place via telecommunications networks, especially the Internet.
- Electronic commerce describes the buying and selling of products, services, and information via computer networks including the Internet.
- Electronic commerce is about doing business electronically.
- E-commerce is defined as the conduct of a financial transaction by electronic means.

THE DIFFERENCE BETWEEN E-COMMERCE AND E-BUSINESS

E-business refers primarily to the digital enablement of transactions and processes *within* a firm, involving information systems under the control of the firm as shown in figure below.



E-commerce primarily involves transactions that cross firm boundaries. E-business primarily involves the application of digital technologies to business processes within the firm.

For the most part, in our view, e-business does not include commercial transactions involving an exchange of value across organizational boundaries. For example, a company's online inventory control mechanisms are a component of e-business, but such internal processes do not directly generate revenue for the firm from outside businesses or consumers, as e-commerce, by definition, does. It is true, however, that a firm's e-business infrastructure provides support for online e-commerce exchanges; the same infrastructure and skill sets are involved in both e-business and e-commerce. E-commerce and e-business systems blur together at the business firm boundary, at the point where internal business systems link up with suppliers or customers, for instance. E-business applications turn into e-commerce precisely when an exchange of value occurs (see Mesenbourg, U.S. Department of Commerce, August 2001 for a similar view).

BENEFITS OF E-COMMERCE

The benefits of e-commerce can be seen to affect three major stakeholders: organisations, consumers and society.

1) Benefits of e-commerce to organisations

International marketplace. What used to be a single physical marketplace located in a geographical area has now become a borderless marketplace including national and international markets. By becoming e-commerce enabled, businesses now have access to people all around the world.

Operational cost savings. The cost of creating, processing, distributing, storing and retrieving paper-based information has decreased.

Mass customisation. E-commerce has revolutionised the way consumers buy good and services. In the past when Ford first started making motor cars, customers could have any colour so long as it was black. Now customers can configure a car according to their specifications within minutes on-line via the www.ford.com website.

Enables reduced inventories and overheads by facilitating 'pull'-type supply chain management – this is based on collecting the customer order and then delivering through JIT (just-in-time) manufacturing. This is particularly beneficial for companies in the high technology sector, where stocks of components held could quickly become obsolete within months. For example, companies like Motorola (mobile phones), and Dell (computers) gather customer orders for a product, transmit them electronically to the manufacturing plant where they are manufactured according to the customer's specifications (like colour and features) and then sent to the customer within a few days.

Lower telecommunications cost. The Internet is much cheaper than value added networks (VANs) which were based on leasing telephone lines for the sole use of the organisation and its authorised partners. It is also cheaper to send a fax or e-mail via the Internet than direct dialling.

Digitisation of products and processes. Particularly in the case of software and music/video products, which can be downloaded or e-mailed directly to customers via the Internet in digital or electronic format.

No more 24-hour-time constraints. Businesses can be contacted by or contact customers or suppliers at any time.

2) **Benefits of e-commerce to consumers**

24/7 access. Enables customers to shop or conduct other transactions 24 hours a day, all year round from almost any location. For example, checking balances, making payments, obtaining travel and other information.

More choices. Customers not only have a whole range of products that they can choose from and customise, but also an international selection of suppliers.

Price comparisons. Customers can 'shop' around the world and conduct comparisons either directly by visiting different sites. (for example www.moneyextra.co.uk for financial products and services).

Improved delivery processes. This can range from the immediate delivery of digitised or electronic goods such as software or audio-visual files by downloading via the Internet, to the on-line tracking of the progress of packages being delivered by mail or courier.

An environment of competition where substantial discounts can be found or value added, as different retailers for customers.

3) **Benefits of e-commerce to society**

Enables more flexible working practices, which enhances the quality of life for a whole host of people in society, enabling them to work from home. It also potentially reduces environmental pollution as fewer people have to travel to work regularly.

Connects people. Enables people in developing countries and rural areas to enjoy and access products, services, information and other people which otherwise would not be so easily available to them.

Facilitates delivery of public services. For example, health services available over the Internet (on-line consultation with doctors or nurses), filing taxes over the Internet through the Inland Revenue website.

LIMITATIONS OF E-COMMERCE

There was much hype surrounding the Internet and e-commerce over the last few years of the twentieth century. Much of it promoted the Internet and e-commerce as the panacea for all ills, which raises the question, are there any limitations of e-commerce and the Internet?

Isaac Newton's 3rd Law of Motion, 'For every action there is an equal and opposite reaction' suggests that for all the benefits there are limitations to e-commerce. These again will be dealt with according to the three major stakeholders – organisations, consumers and society.

Limitations of e-commerce to organisations

Lack of sufficient system security, reliability, standards and communication protocols.
There are numerous reports of websites and databases being hacked into, and security holes in software. For example, Microsoft has over the years issued many security notices and 'patches' for their software. Several banking and other business websites, including Barclays Bank, Powergen and even the Consumers' Association in the UK, have experienced breaches in security where 'a technical oversight' or 'a fault in its systems' led to confidential client information becoming available to all.

Rapidly evolving and changing technology, so there is always a feeling of trying to 'catch up' and not be left behind.

Under pressure to innovate and develop business models to exploit the new opportunities which sometimes leads to strategies detrimental to the organisation. The ease with which business models can be copied and emulated over the Internet increase that pressure and curtail longer-term competitive advantage.

Facing increased competition from both national and international competitors often leads to price wars and subsequent unsustainable losses for the organisation.

Problems with compatibility of older and 'newer' technology. There are problems where older business systems cannot communicate with webbased and Internet infrastructures, leading to some organisations running almost two independent systems where data cannot be shared. This often leads to having to invest in new systems or an infrastructure, which bridges the different systems. In both cases this is both financially costly as well as disruptive to the efficient running of organisations.

Limitations of e-commerce to consumers

Computing equipment is needed for individuals to participate in the new 'digital' economy, which means an initial capital cost to customers.

A basic technical knowledge is required of both computing equipment and navigation of the Internet and the World Wide Web.

Cost of access to the Internet, whether dial-up or broadband tariffs.

Cost of computing equipment. Not just the initial cost of buying equipment but making sure that the technology is updated regularly to be compatible with the changing requirement of the Internet, websites and applications.

Lack of security and privacy of personal data. There is no real control of data that is collected over the Web or Internet. Data protection laws are not universal and so websites hosted in different countries may or may not have laws which protect privacy of personal data.

Physical contact and relationships are replaced by electronic processes. Customers are unable to touch and feel goods being sold on-line or gauge voices and reactions of human beings.

A lack of trust because they are interacting with faceless computers.

Limitations of e-commerce to society

Breakdown in human interaction. As people become more used to interacting electronically there could be an erosion(divide) of personal and social skills which might eventually be detrimental to the world we live in where people are more comfortable interacting with a screen than face to face.

Social division. There is a potential danger that there will be an increase in the social divide between technical haves and have-nots – so people who do not have technical skills become unable to secure better-paid jobs and could form an underclass with potentially dangerous implications for social stability.

Reliance on telecommunications infrastructure, power and IT skills, which in developing countries nullifies the benefits when power, advanced telecommunications infrastructures and IT skills are unavailable or scarce or underdeveloped.

Wasted resources. As new technology dates quickly how do you dispose of all the old computers, keyboards, monitors, speakers and other hardware or software?

Facilitates Just-In-Time manufacturing. This could potentially cripple an economy in times of crisis as stocks are kept to a minimum and delivery patterns are based on pre-set levels of stock which last for days rather than weeks .

Difficulty in policing the Internet, which means that numerous crimes can be perpetrated and often go undetected. There is also an unpleasant rise in the availability and access of obscene material and ease with which paedophiles and others can entrap children by masquerading in chat rooms.

SEVEN UNIQUE FEATURES OF E-COMMERCE TECHNOLOGY

1. **Ubiquity:** In traditional commerce, a marketplace is restricted i.e. we can be in limited physical area to buy or sell. Whereas E-Commerce is ubiquitous meaning that it is available just about everywhere, at all times. It make possible to shop from your desktop, at home, at work or even from your car, using mobile commerce. The result is called a **market space** - a marketplace extended beyond traditional boundaries and removed from a temporal and geographic location. From a consumer perspective, ubiquity reduces transaction costs – the costs of participating in a market. To transact, it is no longer necessary that you spend time and money traveling to a market.

2 **Global Reach:** Unlike traditional commerce, e-commerce technology permits commercial transaction to cross cultural and national boundaries far more conveniently and cost effectively. As a result, the potential market size for e-commerce merchants is roughly equal to the size of the world's online population.

3 **Universal Standards:** One strikingly unusual feature of e-commerce technologies is that the technical standards of the Internet, and therefore the technical standards for conducting e-commerce, are universal standards – they are shared by all nation around the world. In contrast, most traditional commerce technologies differ from one nation to the next. For instance, television and radio standards differ around the world, as doe's cell telephone technology. The universal technical standards of e-commerce greatly lower market entry cost –t he cost merchants must pay just to bring their goods to market.

4 **Richness:** With the use of e-commerce technology merchant can present their message in effective way. Information richness refers to the complexity and content of the message.

5 **Interactivity:** E-Commerce technologies are interactive, meaning they allow two-way communication between merchant and consumer. Television, for instant, cannot ask the viewer any questions, enter into a conversation with a viewer, or request customer information be entered into a form. In contrast, all of these activities are possible on an e-commerce Web site. Interactivity allows an online merchant to engage a consumer in a ways similar to a face-to-face experience, but on a much more massive, global scale.

6 **Information density:** The Internet and the Web vastly increase information density – the total amount and quality of the information available to all market participants, consumers and merchants alike. E-commerce technologies reduce information collection, storage, processing and communication costs. At the same time, these technologies increase greatly the accuracy and timeliness of information – making information more useful and important than ever. As a result, information becomes more plentiful, cheaper and of higher quality.

7 **Personalization/Customization:** E-commerce technologies permit **personalization**: Merchants can target their marketing message to specific individuals by adjusting the message. The technology also permits **customization** – changing the delivered product or service based on a user's preference or prior behavior.

E-COMMERCE FRAMEWORK

E-Commerce applications will be built on the existing technology infrastructure - a myriad of computers, communication networks, and communication software forming the nascent Information Superhighway. The **technology infrastructure** of the Internet is both an enabler and a driver of change. An infrastructure is defined as "*the foundation of a system*." In this case, the technological foundation of the Internet, simply put, enables the running of the e-commerce enterprises. The hardware backbone of computers, routers, servers, fiber optics, cables, modems, and other network technologies provides half of the technology equation. The other half includes the soft-ware and communications standards that run on top of the hardware, including the core protocols for the Web. Understanding technology infrastructure —and there-fore understanding what is and is not achievable—is essential to formulating a company's vision and strategy.

The framework for e-Commerce consists of three parts as shown in below figure.

1 The first part consists of a *variety of electronic commerce applications* including both inter- and intra-organizational and electronic market examples such as Supply Chain Management, Video-on-Demand, Procurement and purchasing, On-line marketing and advertising, Home shopping etc.

2 The second part of the building blocks of the infrastructure consists of:

- **Common business services**, for facilitating the buying and selling process.

- **Messaging and information distribution**, as a means of sending and retrieving information (ex-EDI, e-mail, P2P file transfer)
- **Multi-media content and network publishing**, for creating a product and a means to communicate about it.
- **Information Superhighway infrastructure** consisting of telecommunication, cable operator, ISPs , Wireless technologies and Internet.

3 The third part consists of the *public policy* and *technical standards* necessary to support the applications and the infrastructure.

- **Public policies** govern issues like universal access, privacy, and information pricing. The public policy infrastructure affects not only the specific business but also direct and indirect competitors. It should take into consideration of:
  - Cost of accessing information
  - Regulation to protect consumers from fraud and protect their right to privacy.
  - Policies of global information traffic to detect information pirating and obscene sites**.**
- **Technical Standards** governs issues like technology for communication and as well as for Internet

Fig: Generic Framework of Electronic Commerce

ELEMENTS OF E-COMMERCE APPLICATIONS

Remarks: see the notes provided at the class.

UNIT 2: BUSINESS MODELS FOR E-BUSINESS

Introduction to Business Model

A business model is the method of doing business by which a company can sustain itself, that is, generate revenue. The business model spells out how a company makes money by specifying where it is positioned in the value chain.

Some models are quite simple. A company produces goods or services and sells it to customers. If all goes well, the revenues from sales exceed the cost of operation and the company realizes profit. Other models can be more complex. Radio and television broadcasting is a good example. The broadcaster is part of a complex network of distributors, content creators, advertisers, and listeners or viewers. Who makes money and how much, It is not always clear at the outset. The bottom line depends on many competing factors.

For our understanding, e-commerce can be defined as any form of business transaction in which the parties interact electronically.' A transaction in an electronic market represents a number of interactions between parties. For instance, it could involve several trading steps, such as marketing, ordering, payment, and support for delivery. An electronic market allows the participating sellers and buyers to exchange goods and services with the aid of information technology. Electronic markets have three main functions such as: (i) matching buyers and sellers, (ii) facilitating commercial transactions, and (iii) providing legal infrastructure. Information technology permeates all the three functions and also helps to increase market efficiency and reduce transaction costs.

The interaction between participants is supported by electronic trade processes that are basically search, valuation, payment and settlement, logistics, and authentication, as shown in Figure 2.1. The Internet and the World Wide Web allow companies to efficiently implement these key trading processes. For instance, many search services and brokers are available to help buyers find information, products, and merchants in electronic markets.

E-commerce can be formally defined as technology-mediated exchanges between parties (individuals, organizations, or both) as well as the electronically-based intra- or interorganizational activities that facilitate such exchanges. It is global. It favours intangible things— ideas, information, and relationships. And it is intensely interlinked. These three attributes produce a new type of marketplace and society.

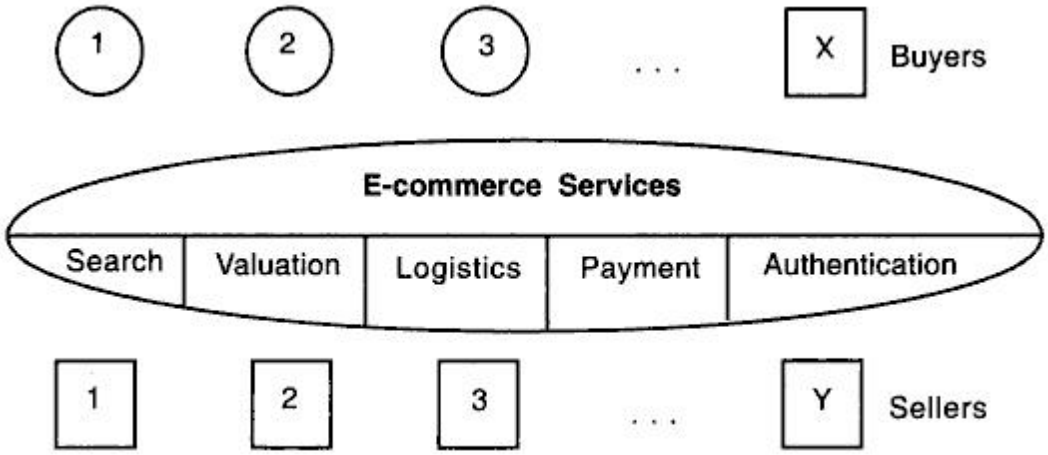


Fig. 2.1 Representation of an electronic market.

A company's business model is the way in which it conducts business in order to generate revenue. In the new economy, companies are creating new business models and reinventing old models. Reading the literature, we find business models categorized in different ways. Presently, there is no single, comprehensive and cogent taxonomy of Web business models that one can point to. Although there are many different ways to categorize e-business models, they can be broadly classified as follows:

- E-Business models based on the relationship of Transaction Parties
- E-Business models based on the relationship of Transaction Types

E-Business models based on the relationship of Transaction Parties

Electronic markets are emerging in various fields. Different industries have markets with different characteristics. For example, an information B2C market differs in many respects from the automotive B2B market.

The information B2C market represents companies that sell digital information goods, such as news, articles, music, books, or digital videos. In the information B2C market, the electronic infrastructure not only helps match customers and sellers, but also acts as the distribution channel, delivering products to customers.

In the automotive B2B market, the products traded, such as parts and components of cars, have a high degree of specificity. The market infrastructure used is to be mainly based on Electronic Data Interchange (EDI) over expensive VAN services. EDI involves the exchange of standardized, structured information between organintions, permitting direct communication between computer systems. B2B is also a closed market in the sense that the number of participants involved in trading is limited and known a priori.

Understanding the nature of the market's requirements is critical for creating the underlying e-business infrastructure. The relation between B2B and B2C models is clearly shown in Figure 2.3.

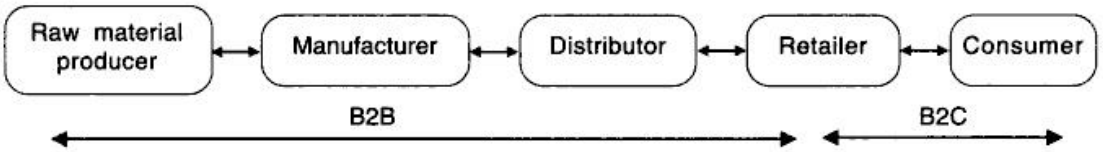


Fig. 2.3 Relation between B2B and B2C models.

B2B covers business transactions along the various interactions existing in the value chain from producers of raw materials to retailers and consumers including manufacturers and distributors. On the contrary. B2C reflects only the interactions between a customer and a retailer. Basically, B2C transactions include the following steps: (i) account acquisition. (ii) product discovery through search and browse, (iii) price negotiation, (iv) payment, and (v) product delivery. In some cases, customer services may also exist.

E-commerce can be classified according to the transaction partners such as

1) business toconsumer (B2C),
2) business-to-business (B2B),
3) business-to-government (B2G),
4) consumer to-consumer (C2C), and
5) consumer-to-business (C2B).

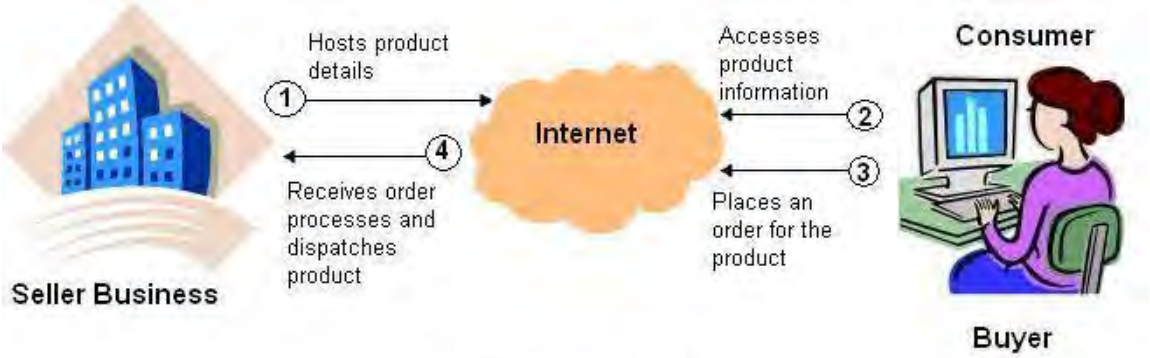
Within these broad categories, there are a number of variations in the way the models are implemented. Table 2.1 summarizes souse of the current e-business models.

TABLE 2.1
SUMMARY OF E-BUSINESS TRANSACTION MODELS

Model	*Description*	*Examples*
B2C	Sells products or services directly to consumers.	*amazon.com, autobytel.com, eDiets.com, Pets.com*
B2B	Sells products or services to other businesses or brings multiple buyers and sellers together in a central marketplace.	*MetalSite.com, VerticalNet.com, SHOP2gether.com*
B2G	Businesses selling to local, state, and federal agencies.	*iGov.com*
C2C	Consumers sell directly to other consumers.	*ebay.com, InfoRocket.com*
C2B	Consumers fix price on their own, which businesses accept or decline.	*Priceline.com*

1) Business-to-Consumer (B2C)

The B2C model involves transactions between business organizations and consumers. It applies to any business organization that sells its products or services to consumers over the Internet. These sites display product information in an online catalog and store it in a database. The B2C model also includes services online banking, travel services, and health information and many more as shown in figure below.



B2C Business Model

Consumers are increasingly going online to shop for and purchase products, arrange financing, arrange shipment or take delivery of digital products such as software, and get service after the sale. B2C e-business includes retail sales, often called e-retail (or e-tail), and other online purchases such as airline tickets, entertainment venue tickets, hotel rooms, and shares of stock.

Some B2C e-businesses provide high-value content to consumers for a subscription fee. Examples of e-business following this subscription model include the Wall Street Journal (financial news and articles), Consumer Reports (product reviews and evaluations), and ediels.com (nutritional counseling).

B2C e-business models include virtual malls, which are websites that host many online merchants. Virtual malls typically charge setup, listing, or transaction fees to online merchants, and may include transaction handling services and marketing options. Examples of virtual malls include excite.com, choicemall, women.com, networkweb.com, amazon.com, Zshops.com, and yahoo.com.

E-tailers that offer traditional or Web-specific products or services only over the Internet are sometimes called virtual merchants, and provide another variation on the B2C model. Examples of virtual merchants include amazon.com (books. electronics, toys, and music), eToys.com (children's books and toys), and ashford.com (personal accessories).

Some businesses supplement a successful traditional mail-order business with an online shopping site, or move completely to Web-based ordering. These businesses are sometimes called catalogue merchants. Examples include avan.com (cosmetics and fragrances), chefs (cookware and kitchen accessories), Omaha Steaks (premium steaks, meats, and other gourmet food), and Harry and David (gourmet food gifts).

Many people were very excited about the use of B2C on the Internet, because this new communication medium allowed businesses and consumers to get connected in entirely new ways. The opportunities and the challenges posed by the B2C e-commerce are enormous. A large amount of investment has gone into this and many sites have either come up or are coming up daily to tap this growing market.

Some of the reasons why one should opt for B2C are:

1. **Inexpensive costs**, big opportunities. Once on the Internet, opportunities are immense as companies can market their products to the whole world without much additional cost.
2. **Globalization**. Even being in a small company, the Web can make you appear to be a big player which simply means that the playing field has been levelled by e- business. The Internet is accessed by: millions of people around the world, and definitely, they are all potential customers.
3. **Reduced operational costs**. Selling through the Web means cutting down on paper costs, customer support costs, advertising costs, and order processing costs.
4. **Customer convenience**. Searchable content, shopping carts. promotions, and interactive and user-friendly interfaces facilitate customer convenience. Thus, generating more business. Customers can also see order status, delivery status, and get their receipts online.
5. **Knowledge management**. Through database systems and information management, you can find out who visited your site, and how to create, better value for customers.

Processes in B2C (How Does B2C Work?)

B2C e-commerce is more than just an online store. It really is about managing the entire process, but just using technology as a tool for order processing and customer support. Figure 2.5 depicts the processes in B2C.

The B2C process is now explained in greater details:

1. **Visiting the virtual mall**. The customer visits the mall by browsing the online catalogue —a very organized manner of displaying products and their related information such as price, description, and availability. Finding the right product becomes easy by using a keyword search engine. Virtual malls may include a basic to an advanced search engine, product rating system, content management, customer support systems, bulletin boards, newsletters and other components which make shopping convenient for shoppers.
2. **Customer registers**. The customer has to register to become part of the site's shopper registry. This allows the customer to avail of the shop's

complete services. The customer becomes a part of the company's growing database and can use the same for knowledge management and data mining.

3. **Customer buys products**. Through a shopping cart system, order details, shipping charges, taxes, additional charges and price totals are presented in an organized manner. The customer can even change the quantity of a certain product. Virtual malls have a very comprehensive shopping system, complete with check-out forms.
4. **Merchant processes the order**. The merchant then processes the order that is received from the previous stage and fills up the necessary forms.
5. **Credit card is processed**. The credit card of the customer is authenticated through a payment gateway or a bank. Other payment methods can be used as well, such as debit cards, prepaid cards, or bank-to-bank transfers.
6. **Operations management**. When the order is passed on to the logistics people, the traditional business operations will still be used. Things like inventory management. Total quality management, warehousing, optimization and project management should still be incorporated even though it is an e-business. Getting the product to the customer is still the most important aspect of e-commerce.

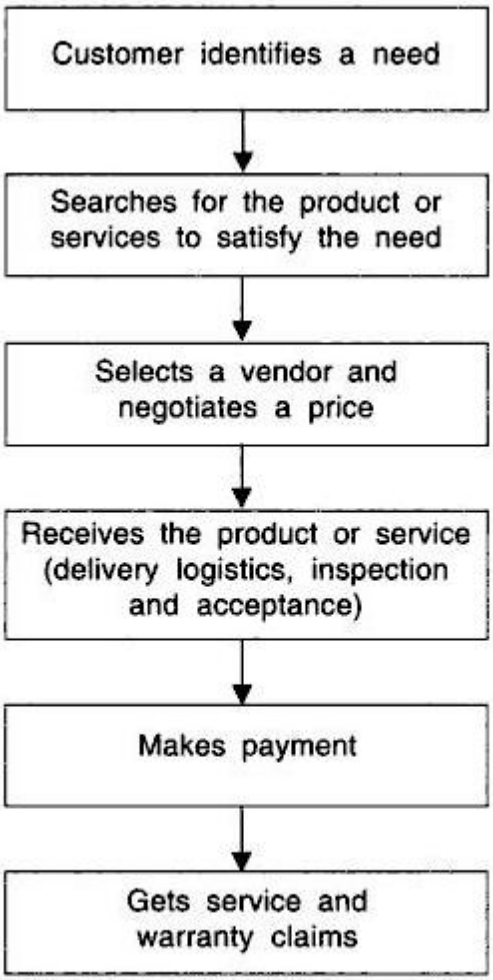


Fig. 2.5 Processes in B2C.

7. **Shipment and delivery**. The product is then shipped to the customer. The customer can track the order/delivery as virtual malls have a delivery tracking module on the website which allows a customer to check the status of a particular order.
8. **Customer receives**. The product is received by the customer, and is verified. The system should then tell the firm that the order has been fulfilled.
9. **After-sales service**. After the sale has been made, the firm has to make sure that it maintains a good relationship with its customers. This is done through customer relationship management or CRM.

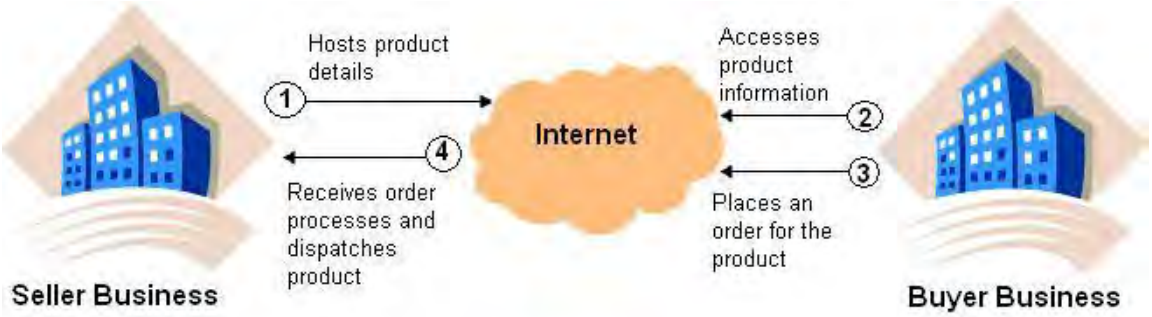
The example of the www.amazon.com site also involves the B2C model in which the consumer searches for a book on their site and places an order, if required. This

implies that a complete business solution might be an integration solution of more than one business model. For example, www.amazon.com includes the B2B model in which the publishers transact with Amazon and the B2C model in which an individual consumer transact with the business organization. The B2C model of e-commerce is more prone to the security threats because individual consumers provide their credit card and personal information n the site of a business organization. In addition, the consumer might doubt that his information is secured and used effectively by the business organization. This is the main reason why the B2C model is not very widely accepted. Therefore, it becomes very essential for the business organizations to provide robust security mechanisms that can guarantee a consumer for securing his/her information.

2) Business to Business (B2B)

The B2B model involves electronic transactions for ordering, purchasing, as well as other administrative tasks between business houses. It includes trading goods, such as business subscriptions, professional services, manufacturing, and wholesale dealings. Sometimes in the B2B model, business may exist between virtual companies, neither of which may have any physical existence. In such cases, business is conducted only through the Internet.

Let us look at the example of www.amazon.com. As you know, www.amazon.com is an online bookstore that sells books from various publishers including Wrox, O'Reilly, Premier Press, and so on. In this case, the publishers have the option of either developing their own site or displaying their books on the Amazon site (www.amazon.com), or both. The publishers mainly choose to display their books on www.amazon.com at it gives them a larger audience. Now, to do this, the publishers need to transact with Amazon, involving business houses on both the ends, is the B2B model as shown in figure below.



B2B Business Model

Thus, B2B is that model of e-commerce whereby a company conducts its trading and other commercial activity through the Internet and the customer is another business itself. This essentially means commercial activity between companies through the Internet as a medium.

This is supposed to be a huge opportunity area on the Web. Companies have by and large computerized all the operations worldwide and now they need to go into the next stage by linking their customers and vendors. This is done by supply chain software, which is an integral part of your ERP application. Companies need to set up a backbone of B2B applications, which will support the customer requirements on the Web. Many B2B sites are company and industry specific, catering to a community of users, or are a combination of forward and backward integration. Companies have achieved huge savings in distribution-related costs due to their B2B applications.

Major Advantages of B2B

1. **Direct interaction with customers**. This is the greatest advantage of e-business.
2. **Focused sales promotion**. This information gives authentic data about the likes, dislikes and preferences of clients and thus helps the company bring out focused sales promotion drives which arc aimed at the right audience.
3. **Building customer loyalty**. It has been observed that online customers can be more loyal than other customers if they are made to feel special and their distinct identity is recognized and their concerns about privacy are respected. It has also been found that once the customers develop a binding relationship with a site and its product, they do not like to shift loyalties to another site or product.
4. **Scalability**. This means that the Web is open and offers round-the-clock access. This provides an access never known before, to the customer. This access is across locations and time zones. Thus a company is able to handle many more customers on a much wider geographical spread if it uses an e-business model. The company can set up a generic parent site for all locations and make regional domains to suit such requirements. Microsoft is using this model very successfully.
5. **Savings in distribution costs**. A company can make huge savings in distribution, logistical and after-sales support costs by using e-business models. Typical examples are of computer companies, airlines, and telecom companies.

Processes for Business-to-Business Transactions and Models

B2B interactions involve much more complexity than B2C. For instance, typical B2B transactions include, among others, the following steps:

- review catalogues,
- identify specifications.
- define requirements,
- post request for proposals (REP).

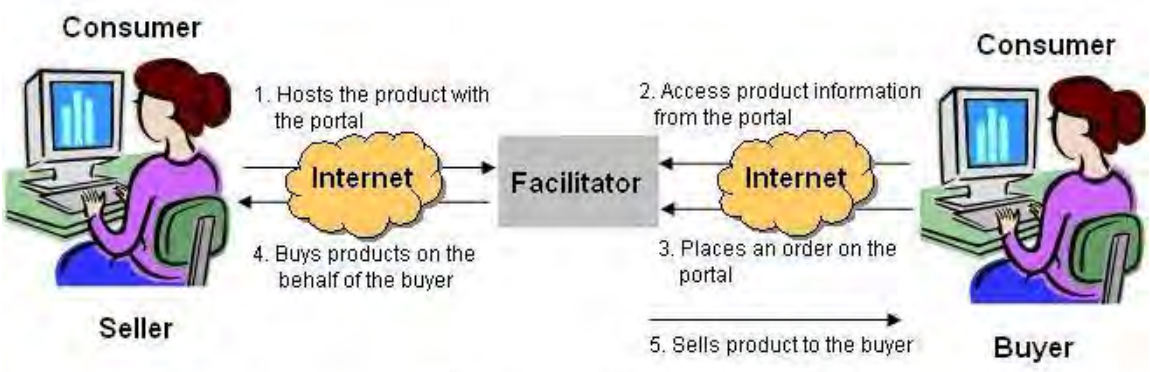
- review vendor reputation.
- select vendor.
- fill out purchase orders (PO).
- send PO to vendor,
- prepare invoice,
- make payment,
- arrange shipment, and
- organize product inspection and reception.

Due to the large number of transactions involved, business-to-business operations can be too risky if e-business sites cannot guarantee adequate quality of service in terms of performance, availability, and security.

3) Consumer to Consumer (C2C)

The C2C model involves transaction between consumers. Here, a consumer sells directly to another consumer. eBay and www.bazee.com are common examples of online auction Web sites that provide a consumer to advertise and sell their products online to another consumer.

However, it is essential that both the seller and the buyer must register with the auction site. While the seller needs to pay a fixed fee to the online auction house to sell their products, the buyer can bid without paying any fee. The site brings the buyer and seller together to conduct deals as shown in figure below.



C2C Business Model

Let us now look at the previous figure with respect to eBay. When a customer plans to sell his products to other customers on the Web site of eBay, he first needs to interact with an eBay site, which in this case acts as a facilitator of the overall transaction. Then, the seller can host his product on www.ebay.com, which in turn charges him for this. Any buyer can now browse the site of eBay to search for the product he interested in. If the buyer comes across such a product, he places an order for the same on the Web site of eBay. eBay now purchase the product from

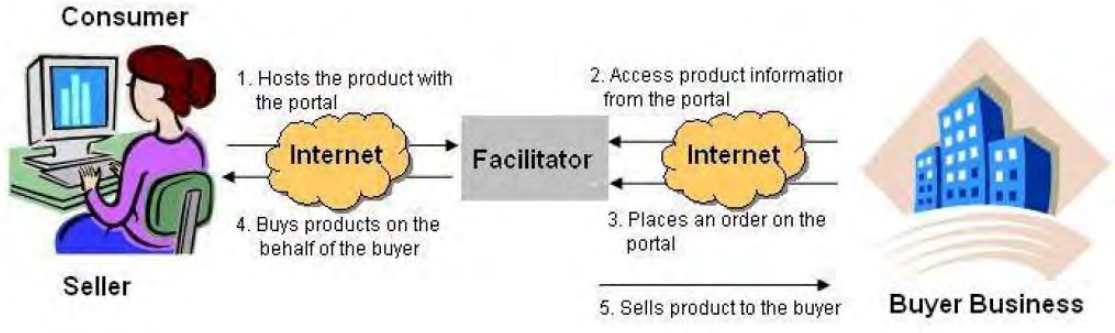
the seller and then, sells it to the buyer. In this way, though the transaction is between two customers, an organization acts as an interface between the two organizations.

There are also a number of new consumer-to-consumer expert information exchanges that are expected to generate $6 billion in revenue by 2005. Some of these exchanges, such as AskMe.com and abuzz, are free, and some allow their experts to negotiate fees with clients.

InfoRocket.com, one of the first question-and-answer marketplaces, is driven by a person-to-person auction format. The InfoRocket.com bidding system allows a person who submits a question to review the profiles of the "experts" who offer to answer the question. When the person asking the question accepts an "expert" offer, infoRocket.com bills the person's credit card, delivers the answer, and takes a 20 percent commission.

4) Consumer to Business (C2B)

The C2B model involves a transaction that is conducted between a consumer and a business organization. It is similar to the B2C model, however, the difference is that in this case the consumer is the seller and the business organization is the buyer. In this kind of a transaction, the consumers decide the price of a particular product rather than the supplier. This category includes individuals who sell products and services to organizations. For example, www.monster.com is a Web site on which a consumer can post his bio-data for the services he can offer. Any business organization that is interested in deploying the services of the consumer can contact him and then employ him, if suitable as shown in figure.



C2B Business Model

Let us look at another example of the C2B model. William Ward needs to buy an airline ticket for his journey from New York to New Jersey. William needs to travel immediately. Therefore, he searches a Web site for a ticket. The Web site offers bidding facility to people who want to buy tickets immediately. On the Web site, William quotes the highest price and gets the ticket.

5) Government Based Model

In addition to the models discussed so far, five new models are being worked on that involves transactions between the government and other entities, such as

consumer, business organizations, and other governments. All these transactions that involve government as one entity are called e-governance. The various models in the e-governance scenario are:

- **Government-to-Government (G2G) model**: This model involves transactions between 2 governments. For example, if the American government wants to by oil from the Arabian government, the transaction involved are categorized in the G2G model.
- **Government-to-Consumer (G2C) model**: In this model, the government transacts with an individual consumer. For example, a government can enforce laws pertaining to tax payments on individual consumers over the Internet by using the G2C model.
- **Consumer-to-Government (C2G) model**: In this model, an individual consumer interacts with the government. For example, a consumer can pay his income tax or house tax online. The transactions involved in this case are C2G transactions.
- **Government-to-Business (G2B) model**: This model involves transactions between a government and business organizations. For example, the government plans to build a fly over. For this, the government requests for tenders from various contractors. Government can do this over the Internet by using the G2B model.
- **Business-to-Government (B2G) model**: In this model, the business houses transact with the government over the Internet. For example, similar to an individual consumer, business houses can also pay their taxes on the Internet.

E-Business models based on the relationship of Transaction Types

Based on transaction type, different types of transactions can be identified as listed below:

1. Brokerage
2. Aggregator
3. Info-mediary
4. Community
5. Value chain
6. Advertising

These transaction types take place in a variety of ways. Moreover, any given firm may combine one or two of these as part of its web business strategy.

1) Brokerage Model

Brokers are market-makers: they bring buyers and sellers together and facilitate transactions. Brokers play a frequent role in business-to-business (B2B), business-to-consumer (B2C), or consumer-to-consumer (C2C) markets. Usually a broker charges a fee or commission for each transaction it enables. The formula for fees can vary depending on context. Brokerage models include:

- **Marketplace Exchange** -- offers a full range of services covering the transaction process, from market assessment to negotiation and fulfillment. Some examples are [Orbitz, ChemConnect]
- **Buy/Sell Fulfillment** -- takes customer orders to buy or sell a product or service, including terms like price and delivery. Some examples are [CarsDirect, Respond.com]
- **Auction Broker** -- conducts auctions for sellers (individuals or merchants). Broker charges the seller a listing fee and commission scaled with the value of the transaction. Auctions vary widely in terms of the offering and bidding rules. Some examples are [eBay]
- **Transaction Broker** -- provides a third-party payment mechanism for buyers and sellers to settle a transaction. Some examples are [PayPal, Escrow.com]
- **Search Agent** -- a software agent or "robot" used to search-out the price and availability for a good or service specified by the buyer, or to locate hard to find information.
- **Virtual Marketplace** -- or virtual mall, a hosting service for online merchants that charges setup, monthly listing, and/or transaction fees. It may also provide automated transaction and relationship marketing services. Some examples are [zShops and Merchant Services at Amazon.com]

2) Aggregator Model

Electronic commerce business model where a firm (that does not produce or warehouses any item) collects (aggregates) information on goods and/or services from several competing sources at its website. The firm's strength lies in its ability to create an 'environment' which draws visitors to its website, and in designing a system which allows easy matching of prices and specifications. Aggregator model includes:

- **Virtual Merchant** -- this is a business that operate only from the web and offers either traditional or web specific goods and services. The method of selling may be listing price or auction. Some example includes [Amazon, eToys]
- **Catalog Merchant** – Catalog business is a migration of mail order to web-based order business.

- **Bit Vendor** – This is the merchant that deals strictly in digital products and services in its purest form.
- **Subscription model** – the users have to pay for the access of the site. High value added content should be essential for subscription model. Some examples are [Wall street journal, Consumer Reports]

3) Info-mediary Model

Data about consumers and their consumption habits are valuable, especially when that information is carefully analyzed and used to target marketing campaigns. Independently collected data about producers and their products are useful to consumers when considering a purchase. Some firms function as infomediaries (information intermediaries) assisting buyers and/or sellers understand a given market. Info-mediary model includes:

- **Advertising Networks** -- feed banner ads to a network of member sites, thereby enabling advertisers to deploy large marketing campaigns. Ad networks collect data about web users that can be used to analyze marketing effectiveness. [DoubleClick]
- **Audience Measurement Services** -- online audience market research agencies. [Nielsen//Netratings]
- **Incentive Marketing** -- customer loyalty program that provides incentives to customers such as redeemable points or coupons for making purchases from associated retailers. Data collected about users is sold for targeted advertising. [Coolsavings]
- **Metamediary** -- facilitates transactions between buyer and sellers by providing comprehensive nformation and ancillary services, without being involved in the actual exchange of goods or services between the parties. [Edmunds]

4) Community Model

The viability of the community model is based on user loyalty. Users have a high investment in both time and emotion. Revenue can be based on the sale of ancillary products and services or voluntary contributions; or revenue may be tied to contextual advertising and subscriptions for premium services. The Internet is inherently suited to community business models and today this is one of the more fertile areas of development, as seen in rise of social networking.

- **Open Source** -- software developed collaboratively by a global community of programmers who share code openly. Some examples are [Red Hat, Linux]
- **Open Content** -- openly accessible content developed collaboratively by a global community of contributors who work voluntarily. [Wikipedia]

- **Public Broadcasting** -- user-supported model used by not-for-profit radio and television broadcasting extended to the web. A community of users support the site through voluntary donations. [The Classical Station (WCPE.org)]
- **Social Networking Services** -- sites that provide individuals with the ability to connect to other individuals along a defined common interest (professional, hobby, romance). Social networking services can provide opportunities for contextual advertising and subscriptions for premium services. [Facebook, Orkut]

5) Value Chain Model

Value chain selling is supported through two business models: demand chain and a supply chain; E-Commerce supports the transactions through both the demand chain business model and supply chain business model.

Products, goods, services, or information are delivered through the parties of the value chain from producers to end users. A value chain also has relationship and administrative aspects, that is, you can manage the relationship of the partners or enterprises in your value chain, as well as offer some administrative services to those parties.

As a result, value chain business models must manage the two sides of their businesses: their customers and direct sales, and their channel partners and suppliers. Each requires its own management channels and practices.

To sell directly to customers (direct sales), value chain models usually include a storefront, where customers can purchase their goods or services directly. To manage relationships with partners or suppliers, the demand chain and a supply chain models within the value chain include a hub.

6) Advertising Model

The web advertising model is an extension of the traditional media broadcast model. The broadcaster, in this case, a web site, provides content (usually, but not necessarily, for free) and services (like email, IM, blogs) mixed with advertising messages in the form of banner ads. The banner ads may be the major or sole source of revenue for the broadcaster. The advertising model works best when the volume of viewer traffic is large or highly specialized. Advertising model includes:

- **Portal** -- usually a search engine that may include varied content or services. A high volume of user traffic makes advertising profitable and permits further diversification of site services. Some common examples are [Google, Yahoo!]
- **Classifieds** -- list items for sale or wanted for purchase. Listing fees are common, but there also may be a membership fee. [Monster.com, Craigslist]

- **User Registration** -- content-based sites that are free to access but require users to register and provide demographic data. Registration allows inter-session tracking of user surfing habits and thereby generates data of potential value in targeted advertising campaigns. [NYTimes]
- **Contextual Advertising / Behavioral Marketing** -- For example, a browser extension that automates authentication and form fill-ins, also delivers advertising links or pop-ups as the user surfs the web. Contextual advertisers can sell targeted advertising based on an individual user's surfing activity.

Electronic Data Interchange (EDI)

UNIT 3

Introduction to EDI…

- **What is EDI?**
  - **Electronic Data Interchange is the computer-to-computer exchange of business data and documents between companies using standard formats recognized both nationally and internationally.**
  - **The information used in EDI is organized according to a specified format set by both companies participating in the data exchange.**

http://www.x12.org/x12org/about/faqs.cfm#a1

Electronic Data Interchange

- EDI Is the electronic transfer of information between two trading partner's systems using a set of transactions that have been adopted as a national or international standard for the particular business function.
- Each term in the definition is significant:
  1. **Computer-to-computer**– EDI replaces postal mail, fax and email.
  2. **Business documents** –purchase orders, invoices and advance ship notices, bill of lading, customs documents, inventory documents, shipping status documents and payment documents
  3. **Standard format**– ANSI, EDIFACT

History of EDI

- The general idea behind EDI was originated by a group of railroad companies in the mid-1960's, in the United States.
- Much of the early work on EDI was driven by the industry sectors for:
  - transportation
  - pharmaceuticals
  - groceries
  - automobiles
  - banking

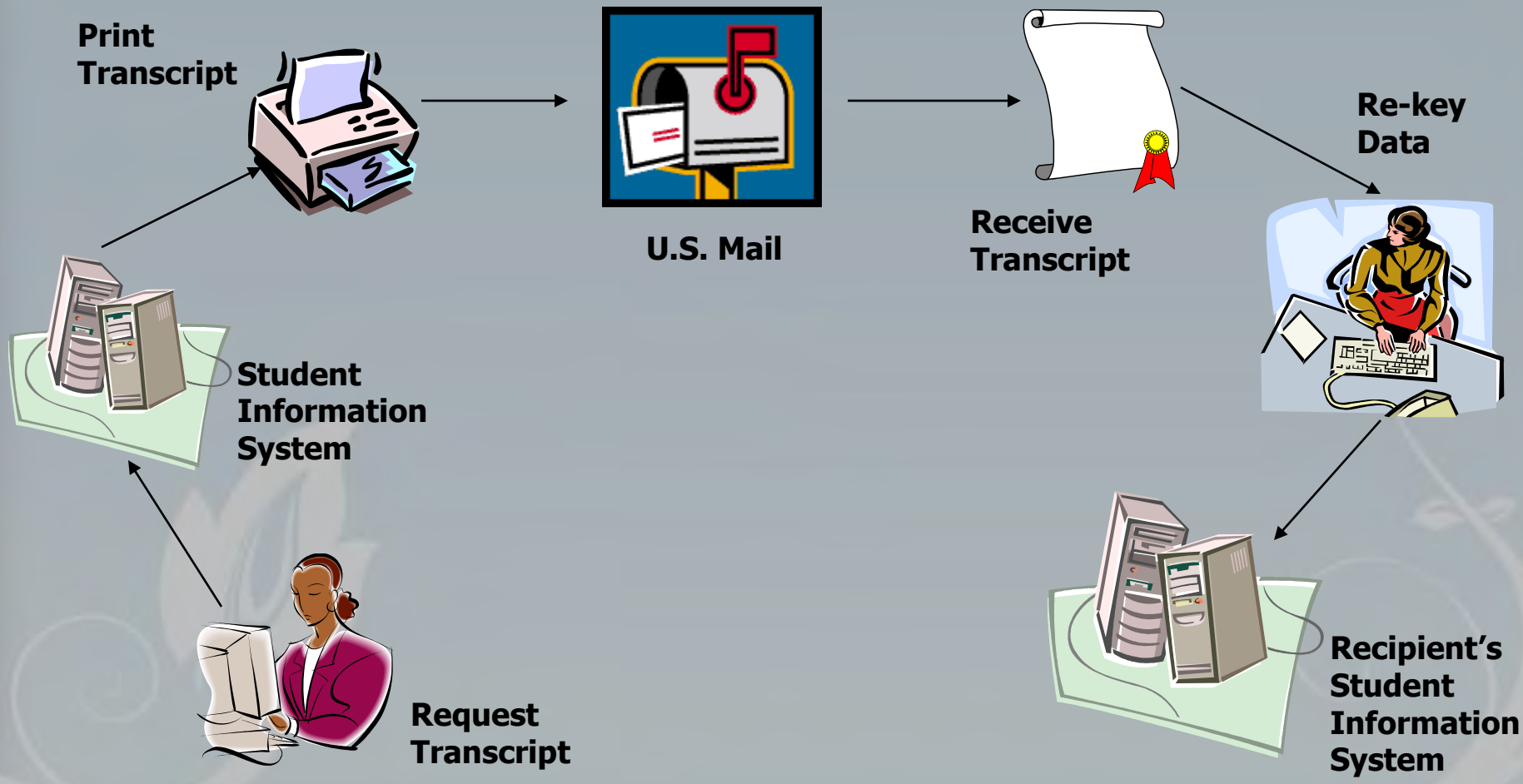
www.edi-guide.com/edi-history.htm

History of EDI

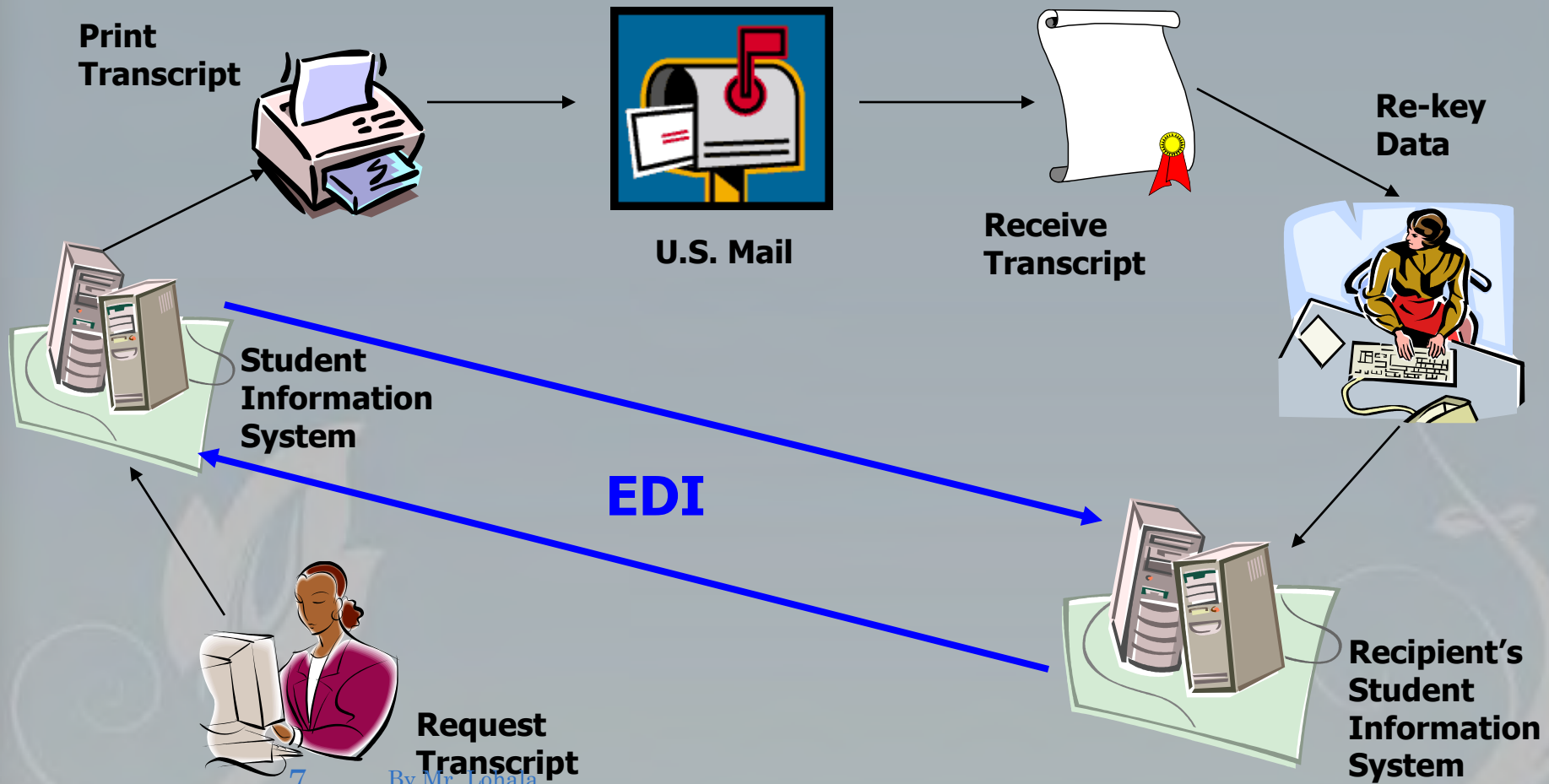
- It was not until the 1970's, when work began for national EDI standards.
- Both client and vendors input their requirements to create a set of standard data formats that
  - were hardware independent;
  - were unambiguous and could be used by all trading partners;
  - reduced labor-intensive tasks such as data-entry;
  - allowed the sender of data to control the exchange including receipt confirmation of by the other party

www.gotedi.com/term_history.htm

The Transcript Trail



The Transcript Trail with EDI



EDI Layered Architecture

EDI SEMANTIC LAYER	APPLICATION LEVEL SERVICES	
EDI STANDARD LAYER	EDIFACT BUSINESS FORM STANDARDS	
	ANSI X12 BUSINESS FORM STANDARDS	
EDI TRANSPORT LAYER	EMAIL	X.435 MIME
	POINT TO POINT	FTP TELNET
	WWW	HTTP
PHYSICAL LAYER	DIAL UP LINES, INTERNET, IWAY	

EDI semantic layer

- The EDI **semantic layer** describes the business application that is driving EDI.
- For a procurement application, this translates into requests for quotes, price quotes, purchase orders, acknowledgments, and invoices.
- This layer is specific to a company and the software it uses.
- the user interface is customized to local environments.

EDI standards

- The information seen at the EDI semantic layer must be translated from a company-specific form to universal form
- To achieve this, companies must adopt universal EDI standards that lay out the acceptable fields of business forms.
- structure of EDI forms:
  - the **X12 standard**, developed by the American National Standards Institute (ANSI),
  - **EDIFACT**, developed by United Nations Economic Commission for Europe (UN /ECE).

EDI translation

- When the trading partner sends a document, the EDI translation software converts the proprietary format into a standard mutually agreed on by the processing systems.
- When a company receives the document, their EDI translation software automatically changes the standard format into the proprietary format of their document processing software so that the company can manipulate the information in whatever way it chooses to.

Advantages of EDI

- Lower operating costs
  - Saves time and money
- Less Errors = More Accuracy
  - No data entry, so less human error
- Increased Productivity
  - More efficient personnel and faster throughput
- Faster trading cycle
  - Streamlined processes for improved trading relationships

What it takes to use EDI

- EDI server
- Internet access
- Translation & mapping software
- Staffing
- Registration
- Encryption software

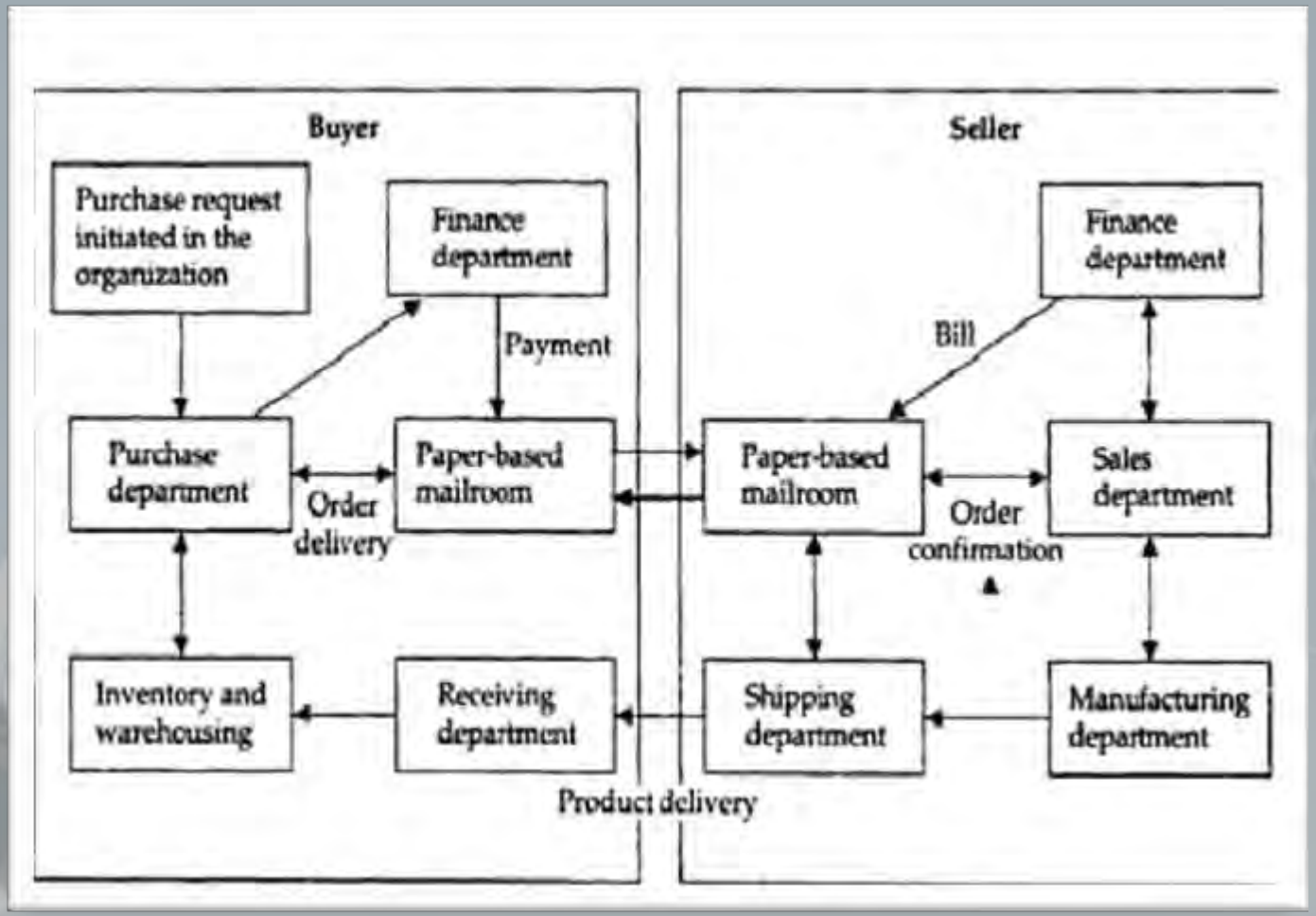
Electronic Data Interchange versus E-mails

- EDI document transport is far more complex than simply sending e-mail messages or sharing files through a network.
- These EDI documents are more structured than e-mail.
- EDI from messaging is its emphasis on the automation of business transactions conducted between organizations.
- In addition, EDI messages have certain legal status.
- For instance, if a buyer sends a supplier EDI purchase orders that specify the requirements, time of delivery, and quantity and the supplier does not uphold its end of the contract, it can be taken to court with the EDI trading agreements serving as evidence.

How EDI works?

- EDI seeks to take a form from a business application, translates that data into a standard electronic format, and transmit it. At the receiving end, the standard format is "untranslated" into a format that can be read by the recipient's application.
- output from one application becomes input to another through the computer-to-computer exchange of information. The result is an elimination of the delays and the errors inherent in paper-based transactions.

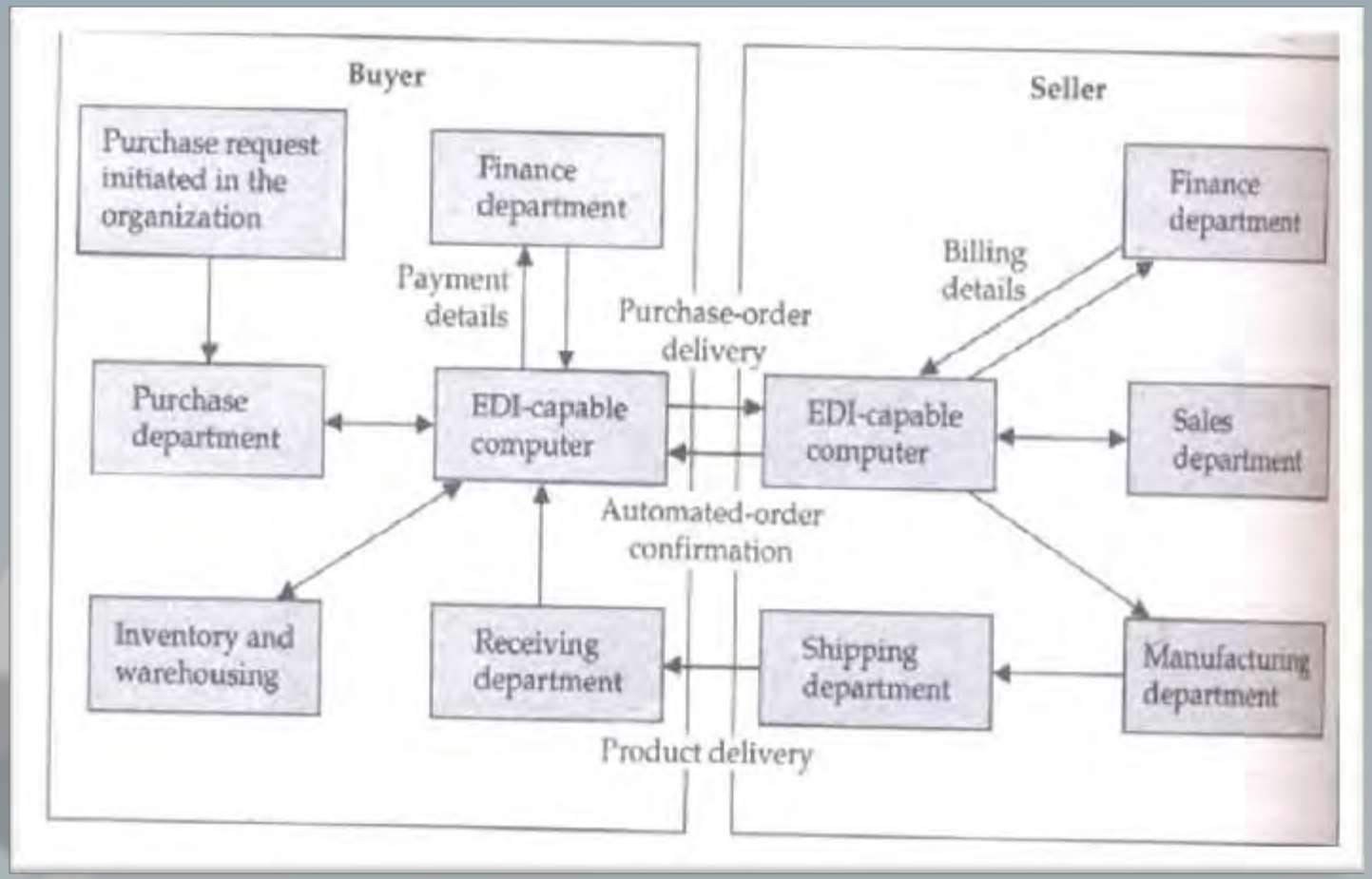
EDI in Action
Information flow without EDI



Information flow without EDI

- The fig shows the information flow when paper documents are shuffled between organizations via the mailroom
- When the buyer sends a purchase order, then relevant data extracted & recorded on a hardcopy.
- This hard copy is forwarded to several steps, at last manually entered into system by the data entry operators
- This process is somewhat overhead in labor costs & time delays

EDI in Action

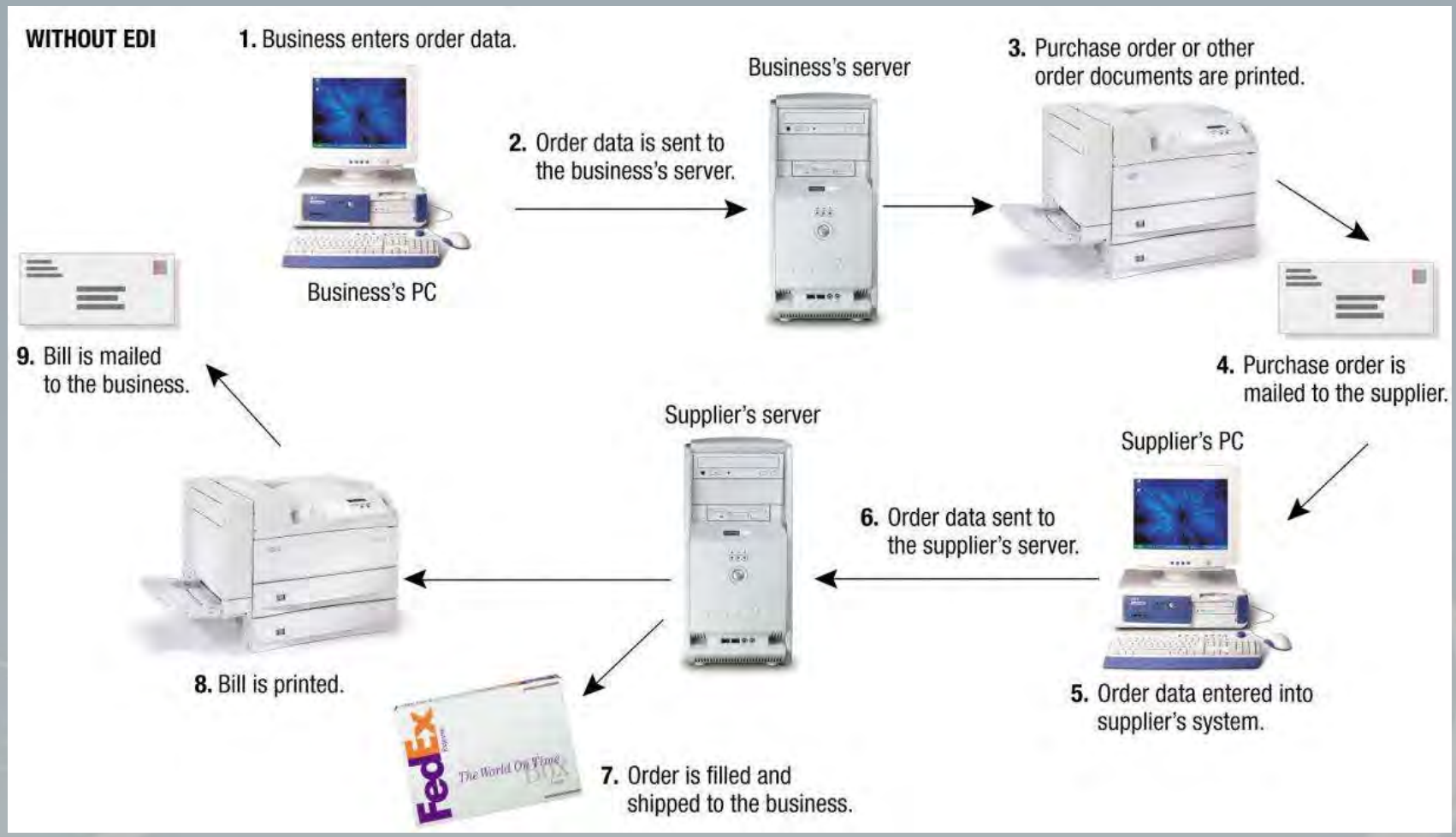


Information flow with EDI

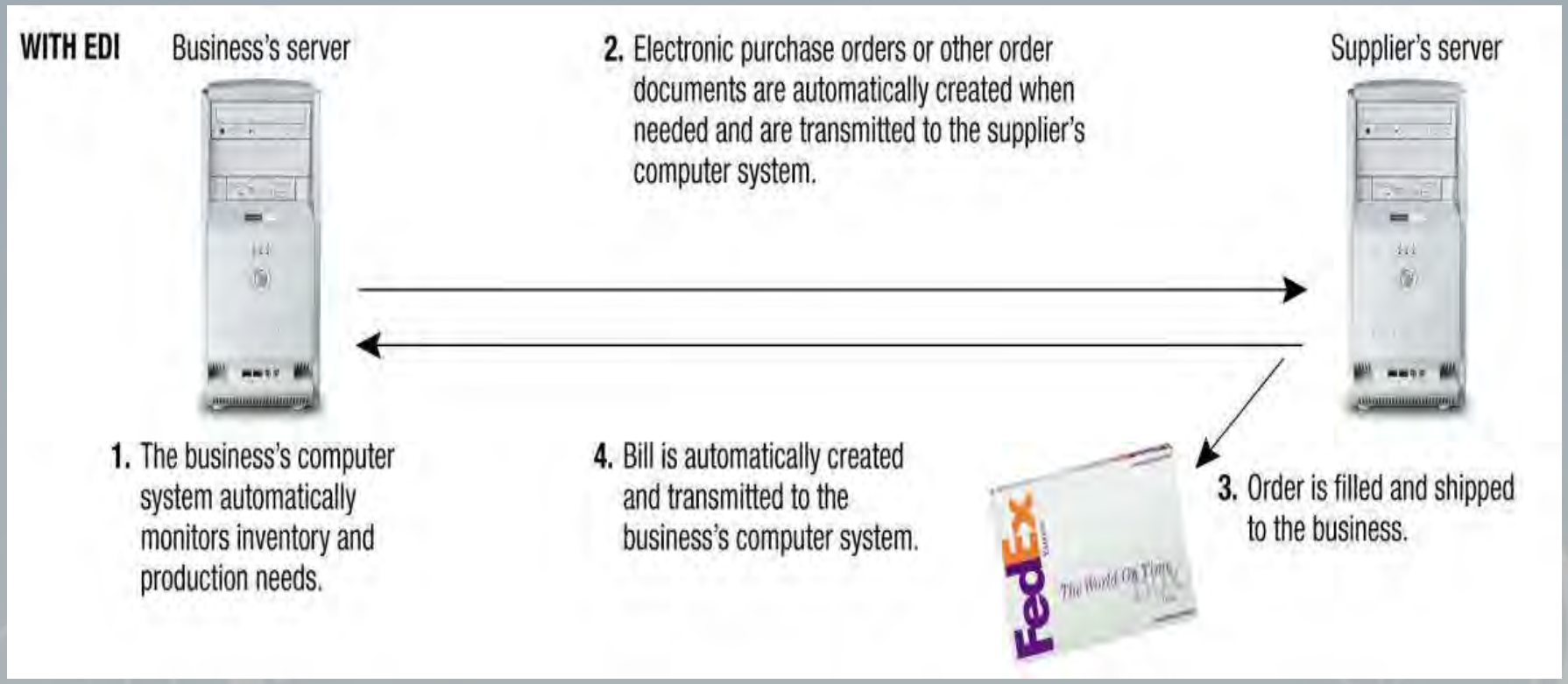
– Information flow with EDI are as follows:

1. Buyer sends purchase order to seller computer
2. Seller sends purchase order confirmation to buyer
3. Seller sends booking request to transport company
4. Transport company sends booking confirmation to seller
5. Seller sends advance ship notice to buyer
6. Transport company sends status to seller
7. Buyer sends Receipt advice to seller
8. Seller sends invoice to buyer
9. Buyer sends payment to seller EDI as a fast, inexpensive & safe method

Without EDI


WITHOUT EDI
1. Business enters order data.
Business's PC
2. Order data is sent to the business's server.
Business's server
3. Purchase order or other order documents are printed.
4. Purchase order is mailed to the supplier.
Supplier's PC
5. Order data entered into supplier's system.
6. Order data sent to the supplier's server.
Supplier's server
7. Order is filled and shipped to the business.
8. Bill is printed.
9. Bill is mailed to the business.

With EDI


WITH EDI
Business's server
2. Electronic purchase orders or other order documents are automatically created when needed and are transmitted to the supplier's computer system.
Supplier's server
1. The business's computer system automatically monitors inventory and production needs.
4. Bill is automatically created and transmitted to the business's computer system.
FedEx
3. Order is filled and shipped to the business.

EDI Standards

- EDI requires companies to agree on standards
  1. Compatible hardware and software
  2. Agreed upon electronic form format

How to Subscribe to EDI

- Larger companies purchase hardware and software
- Medium and small companies seek third-party service
  1. Value-added networking (VAN)
     - ***communications networks supplied and managed by third-party companies that facilitate electronic data interchange, Web services and transaction delivery by providing extra networking services***
  2. Managed network services available for a fee

Benefits of EDI

Cost Savings	◆ Reduction of employee hours involved in creation and handling of paper documents ◆ Reduction in the cost of funds transfer ◆ Reduction in the cost of storage space ◆ No mailing cost
Speed	◆ Forwarding of documents through a computer network is faster than mail.
Accuracy	◆ EDI minimizes the need for rekeying information. ◆ Communication is direct and easily verifiable. ◆ No mail is lost.
Security	◆ Information is less susceptible to interception and falsification.
System Integration	◆ EDI software can be interfaced with internal systems so that incoming data trigger applications and further automation of data processing.
Just-in-time Support	◆ Speeding up communication enhances intercompany just-in-time operations, which significantly reduces inventory costs. Only the necessary items are shipped by the vendor and arrive directly at the manufacturing or assembly line.

Cost savings

- Expenses associated with paper, printing, reproduction, storage, filing, postage and document retrieval are all reduced or eliminated when you switch to EDI transactions, lowering your transaction costs by at least 35%
- A major electronics manufacturer calculates the cost of processing an order manually at $38 compared to just $1.35 for an order processed using EDI
- Errors due to illegible faxes, lost orders or incorrectly taken phone orders are eliminated, saving your staff valuable time from handling data disputes

Speed and accuracy

- EDI can speed up your business cycles by 61%. Exchange transactions in minutes instead of the days or weeks of wait time from the postal service
- Improves data quality, delivering at least a 30—40% reduction in transactions with errors—eliminating errors from illegible handwriting, lost faxes/mail and keying and re-keying errors
- Using EDI can reduce the order-to-cash cycle time by more than 20%, improving business partner transactions and relationships

Increase in business *efficiency*

- Automating paper-based tasks allows your staff to concentrate on higher-value tasks and provides them with the tools to be more productive
- Quick processing of accurate business documents leads to less re-working of orders, fewer stock outs and fewer cancelled orders
- Automating the exchange of data between applications across a supply chain can ensure that business-critical data is sent on time and can be tracked in real time. Sellers benefit from improved cash flow and reduced order-to-cash cycles
- Shortening the order processing and delivery times means that organizations can reduce their inventory levels

EDI benefits come at the strategic business

- Enables real-time visibility into transaction status.
- turn enables faster decision-making and improved responsiveness to changing customer and market demands, and allows businesses to adopt a demand-driven business model rather than a supply-driven one
- Shortens the lead times for product enhancements and new product delivery
- Streamlines your ability to enter new territories and markets. EDI provides a common business language that facilitates business partner onboarding anywhere in the world

EDI Applications in Business

- Four different scenarios in industries that use EDI extensively:
  - 1. International or cross-border trade
  - 2. Electronic funds transfer
  - 3. Health care EDI for insurance claims processing
  - 4. Manufacturing & retail procurement

International or cross-border trade

- EDI has always been very closely linked with international trade.
- Trade efficiency, which allows faster, simpler, broader & less costly transactions.
- **Role of EDI in international trade**
  - EDI facilitates the smooth flow of information
  - It reduces paper work

- EDI benefits for international trade are
  - *Reduced transaction expenditures*
  - *Quicker movement of imported & exported goods*
  - *Improved customer service through “track & trace” programs*
  - *Faster customs clearance & reduced opportunities for corruption, a huge problem in trade*

Financial EDI or electronic funds transfer (EFT)

- Financial EDI comprises the electronic transmission of payments and remittance information between a payer, payee, and their respective banks.
- This section examines the ways business-to-business payments are made today and describes the various methods for making financial EDI payments.
- **Automated Clearinghouse (ACH) Transfers**
  - ACH transfers are used to process high volumes of relatively small-dollar payments for settlement in one or two business days
  - It provides services: preauthorized debits, such as repetitive bill payments; & consumer-initiated payments.

Health care EDI for insurance EDI

- Providing good & affordable health care is a universal problem
- EDI is becoming a permanent fixture in both insurance & health care industries as medical provider, patients & payers
- Electronic claim processing is quick & reduces the administrative costs of health care.
- Using EDI software, service providers prepare the forms & submit claims via communication lines to the value-added network service provider

- The company then edits sorts & distributes forms to the payer. If necessary, the insurance company can electronically route transactions to a third-party for price evaluation
- Claims submission also receives reports regarding claim status & request for additional information

Manufacturing & retail procurement using EDI

- These are heavy users of EDI
- In manufacturing, EDI is used to support just-in-time.
- In retailing, EDI is used to support quick response
- **Just-In-Time & EDI**
  - Companies using JIT & EDI calculates how many parts are needed each day based on the production schedule & electronically transmit orders.
  - Delivery has to be responsive, or it will cost too much in money & time.
  - Getting data to suppliers quickly
  - A major benefit of JIT & EDI is a streamlined cash flow.

- **Quick Response & EDI**
  - For the customer, QR means better service & availability of a wider range of products
  - For the retailer & supplier, QR may mean survival in a competitive marketplace
  - Much focus of QR is in reduction of lead times using event-driven EDI.
  - In QR, EDI documents include purchase orders, shipping notices, invoices, inventory position, catalogs, & order status

Security and privacy issues of EDI

- trade between countries and corporations, issues of legal admissibility and computer security are important.
- retain the services of a lawyer during the design of an EDI application so that the appropriate evidentiary/admissibility safeguards are implemented.
- **Legal Status of EDI Messages**
- **Digital Signatures and EDI**

Legal Status of EDI Messages

- The establishment of a framework is essential if EDI is to become widespread.
- It distinguishes three modes of communication types:
  - **instantaneous communication:**

    If the parties are face to face or use an instantaneous communication medium such as the telephone, an offer or acceptance is held operable when spoken.

- Delayed (U.S. Postal Service [**USPS]** and non-USPS).

  The "mailbox rule" provides that an acceptance communicated via USPS mail or via telegram, mailgram, and probably electronic messaging systems, is effectively communicated when dispatched, or physically deposited in a USPS and non USPS mailbox.

- Messaging systems combine features of both instantaneous and delayed communications.
- who assumes liability? If the U.S. mail or an overnight express service does not deliver a contract to the right addressee, it can be held responsible for any business losses caused by the error. Of course, liability also depends on the situation.
- In the case of EDI, however, the courts haven't decided who is liable if an EDI network fails to transmit a document or transmits a document to the wrong party. There is no legal precedence in this area (yet!).

Digital Signatures and EDI:

- The cryptographic community is exploring various technical uses of digital signatures by which messages might be time-stamped or digitally notarized to establish dates and times at which a recipient might claim to have had access or even read a particular message.
- If digital signatures are to replace handwritten signatures, they must have the same legal status as handwritten signatures

- Digital signatures should have greater legal authority than handwritten signatures.
- For instance, if a ten-page contract is signed by hand on the tenth page, one cannot be sure that the first nine pages have not been altered. If the contract was signed by digital signatures, however, a third party can verify that not one byte of the contract has been altered.

EDI for e-commerce

- companies have been able to improve only discrete processes such as automating the accounts payable function or the funds transfer process.
- Companies are realizing that to truly improve their productivity they need to automate their external processes as well as their internal processes. (New EDI)

- They present information management solutions that allow companies to link their trading community electronically
  - order entry, purchasing, accounts payable, funds transfer, and other systems interact with each other throughout the community to link the company with its suppliers, distributors, customers, banks, and transportation and logistics operations.
- Another goal of new EDI services is to reduce the cost of setting up an EDI relationship.
  - most successful EDI implementations are either in long-term partnerships or among a limited number of partners.

Traditional EDI:

- Traditional EDI replaces the paper forms with almost strict one-to-one mappings between parts of a paper form to fields of electronic forms called transaction sets.
- Traditional EDI covers two basic business areas:
  - Trade data interchange (TDI) encompasses transactions such as purchase orders, invoices, and acknowledgments.
  - Electronic funds transfer (EFT) is the automatic transfer of funds among banks and other organizations.
- Today, traditional EDI is divided into two :
  - old EDI and new EDI

Old EDI

- **Old EDI** refers to the current practice of automating the exchange of information pertinent to the business activity.
- Information that is generated by the business process of one computer is transferred electronically and effects a corresponding business process in another computer.
- Old EDI is also used to refer to the current EDI-standardization process (e.g., X12, EDIFACT) where tens of thousands of people in groups (or working committees) all around the world are attempting to define generic document interchanges (e.g., purchase orders) that allow every company to choose its own, unique, proprietary version (that is a subset of the original transaction set).

New EDI

- **New EDI** is really a refocus of the standardization process.
- With old EDI focused on the interchange structure, on the transaction set in X12 or the message in EDIFACT.
- With new EDI the structure of the interchanges is determined by the programmer who writes the business application program, not by the lengthy standards process.

Open EDI

- It provides a framework where two potential trading partners can whip out an EDI structure for their potential partnership in the short time frame that it takes them to draw up and negotiate the legal contracts.
- The increased interest in open EDT is a result of dissatisfaction with traditional EDI.
- Open EDI is a business procedure that enables electronic commerce to occur between organizations where the interaction is of short duration.


NETWORK
SECURITY

WHAT IS A NETWORK?

- A network has been defined as ``any set of interlinking lines resembling a net, *a network of roads*, an interconnected system, *a network of alliances*."
- a computer network is simply a system of interconnected computers.
- **What is the Internet?**
  - The Internet is the world's largest network *of networks* .
  - Internet is a network of *networks* -- not a network of hosts.

NETWORK SECURITY INTRODUCTION

- **Network Security**
  - process of taking physical and software preventative measures
  - protect the underlying networking infrastructure
  - from unauthorized access, misuse, malfunction, modification, destruction, or improper disclosure,
  - by creating a secure platform for computers, users and programs to perform their permitted critical functions within a secure environment.

- **Network security** consists of the policies adopted 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**

FACTOR AUTHENTICATION

- Network security starts with authenticating, commonly with a username and a password.
- one detail authenticating the user name—i.e., the password—this is sometimes termed one-factor authentication.
- two-factor authentication, something the user 'has' is also used (e.g., a security token or 'dongle', an ATM card, or a mobile phone);
- three-factor authentication, something the user 'is' also used (e.g., a fingerprint or retinal scan).

DIMENSIONS OF NETWORK SECURITY

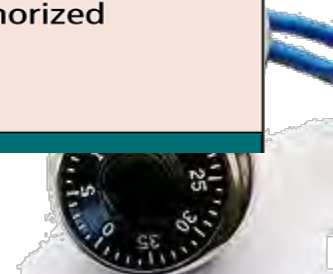
- Access
  - authorized users are provided the means to communicate to and from a particular network
- Confidentiality
  - Information in the network remains private
- Authentication
  - Ensure the users of the network are who they say they are
- Integrity
  - Ensure the message has not been modified in transit

- **Availability**
  - Information should be available wherever and whenever requirement within time limit specified.
- **Encryption**
  - Information should be encrypted and decrypted only by authorized user.
- **Auditability**
  - Data should be recorded in such a way that it can be audited for integrity requirements.
- **Non-repudiation**
  - Ensure the user does not denay that he used the network

CUSTOMER AND MERCHANT PERSPECTIVES ON THE DIFFERENT DIMENSIONS OF E-COMMERCE SECURITY

TABLE 5.1 CUSTOMER AND MERCHANT PERSPECTIVES ON THE DIFFERENT DIMENSIONS OF E-COMMERCE SECURITY

DIMENSIONS	CUSTOMER'S PERSPECTIVE	MERCHANT'S PERSPECTIVE
Integrity	Has information I transmit or receive been altered?	Has data on the site been altered without authorization? Is data being received from customers valid?
Nonrepudiation	Can a party to an action with me later deny taking the action?	Can a customer deny ordering products?
Authenticity	Who am I dealing with? How can I be assured that the person or entity is who they claim to be?	What is the real identity of the customer?
Confidentiality	Can someone other than the intended recipient read my messages?	Are messages or confidential data accessible to anyone other than those authorized to view them?
Privacy	Can I control the use of information about myself transmitted to an e-commerce merchant?	What use, if any, can be made of personal data collected as part of an e-commerce transaction? Is the personal information of customers being used in an unauthorized manner?
Availability	Can I get access to the site?	Is the site operational?



E-COMMERCE THREATS

- Intellectual property threats
- Client computer threats
- Communication channel threats
- Server threats

INTELLECTUAL PROPERTY THREATS

- use existing materials found on the Internet without the owner's permission
- Example:
  - music downloading
  - domain name (cybersquatting)
    - cybersquatting is registering, trafficking in, or using a domain name with bad-faith intent to profit from the goodwill of a trademark belonging to someone else
  - software pirating

CLIENT COMPUTER THREATS

- Trojan horse
  - Trojans appear to be benign programs to the user, but will actually have some malicious purpose.
  - Trojans usually carry some payload such as a virus
- Viruses
  - Viruses are self-replication programs that use files to infect and propagate.
  - Once a file is opened, the virus will activate within the system.

- Active contents
  - Active content may require browser plug-ins for execution.
  - For example, the RealPlayer plug-in allows Web browser users to watch videos online.
  - Active content is mainly used by websites to build animations as well as other interactive features.
  - Sadly, it may also be exploited to deliver and execute malicious code on users' computers.
  - Active content may automatically be downloaded into users' computers without their knowledge or consent. Also, it can be sent via instant messages and email.
    - Phishing
    - Malware
    - Spyware
    - Hacking
    - Adware

- Java applets, Active X controls, JavaScript, and VBScript, which are programs that interpret or execute instructions embedded in downloaded objects from a Web/commerce server
- Malicious active content can be embedded into seemingly innocuous Web pages
- **Cookies** remember user names, passwords, and other commonly referenced information

COMMUNICATION CHANNEL THREATS

- **Secrecy Threats:**
  - Secrecy is the prevention of unauthorized information disclosure. It requires sophisticated physical and logical mechanism to implement
  - Theft of sensitive or personal information (e-mail address, credit card number)is a significant danger in e-commerce
  - Sniffer programs can tap into a router of the Internet and record information while it passes from a client computer to a Web server.

- Integrity Threats:
  - Also known as active wiretapping
  - Unauthorized party can alter data such as changing the amount of a deposit or withdrawal in bank transaction over the Internet
  - A hacker can create a mechanism such that all transactions from a Web site redirects to a fake location.
- Necessity Threats:
  - Also known as delay or denial threats
  - Disrupt normal computer processing
    - Deny processing entirely
    - Slow processing to intolerably slow speeds such that customers get bored not to visit the site anymore.
    - Remove file entirely, or delete information from a transmission or file
    - Divert money from one bank account to another

- Backdoor
  - A **backdoor** is a method, often secret, of bypassing normal authentication in a product, computer system, cryptosystem or algorithm etc.
- Spoofing
  - a **spoofing attack** is a situation in which one person or program successfully masquerades as another by falsifying data, thereby gaining an illegitimate advantage.
- DoS and dDoS Attacks
  - Denial of service (DoS) attack: Hackers flood Web site with useless traffic to inundate and overwhelm network
  - Distributed denial of service (dDoS) attack: hackers use numerous computers to attack target network from numerous launch points
- Viruses:
  - self-replicating computer programs designed to perform unwanted events.

- Worms:
  - special viruses that spread using direct Internet connections.
- Trojan Horses:
  - disguised as legitimate software and trick users into running the program Security (unauthorized access)
- Passive unauthorized access
  - listening to communications channel for finding secrets.
  - May use content for damaging purposes
- Active unauthorized access
  - Modifying system or data
  - Message stream modification
  - Changes intent of messages, e.g., to abort or delay a negotiation on a contract •Masquerading or spoofing – sending a message that appears to be from someone else.

- Passive unauthorized access
  - listening to communications channel for finding secrets.
  - May use content for damaging purposes
- Active unauthorized access
  - Modifying system or data
  - Message stream modification
  - Changes intent of messages, e.g., to abort or delay a negotiation on a contract •Masquerading or spoofing – sending a message that appears to be from someone else.

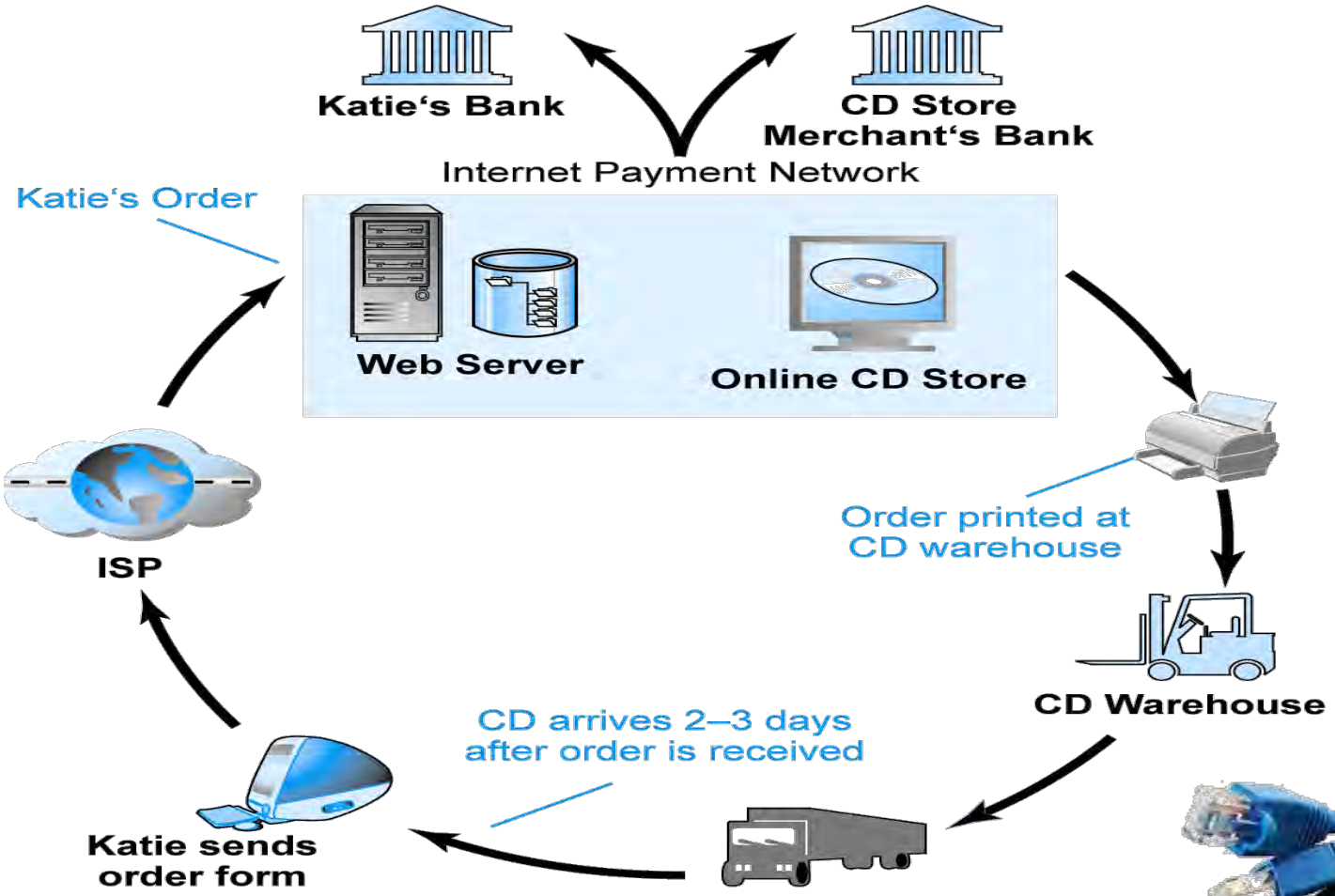
SERVER THREATS

- The more complex a Web server software becomes, the higher the probability that errors (bugs) exist in the code - security holes through which hackers can access.
- Web servers run at various privilege levels:
  - Highest levels provide greatest access and flexibility to a Web user (from a browser)
  - Lowest levels provide a logical fence around a running program
- Secrecy violations occur when the contents of a server's folder names are revealed to a Web browser

- Web site administrators can turn off the "Allow Directory Browsing" feature to avoid secrecy violations
- Cookies requested by a Web server, containing a user's Userid and Password in a client computer, should never be transmitted unprotected
- **Database Threats**
  - A company database systems store data on user, products, and orders for e-commerce
  - In addition, a company's valuable and private information could be stored in a company database
  - Security in a database is often enforced through defining the user "privileges" which must be enforced
  - Some databases are inherently insecure and rely on the Web server to enforce security measures

- Common Gateway Interface (CGI) Threats
  - CGIs are programs that present a security threat if misused
  - CGI programs can reside almost anywhere on a Web server and therefore are often difficult to track down
  - CGI scripts do not run inside a sandbox, unlike JavaScript

A TYPICAL E-COMMERCE TRANSACTION



VULNERABLE POINTS IN AN E-COMMERCE ENVIRONMENT

Security Risks

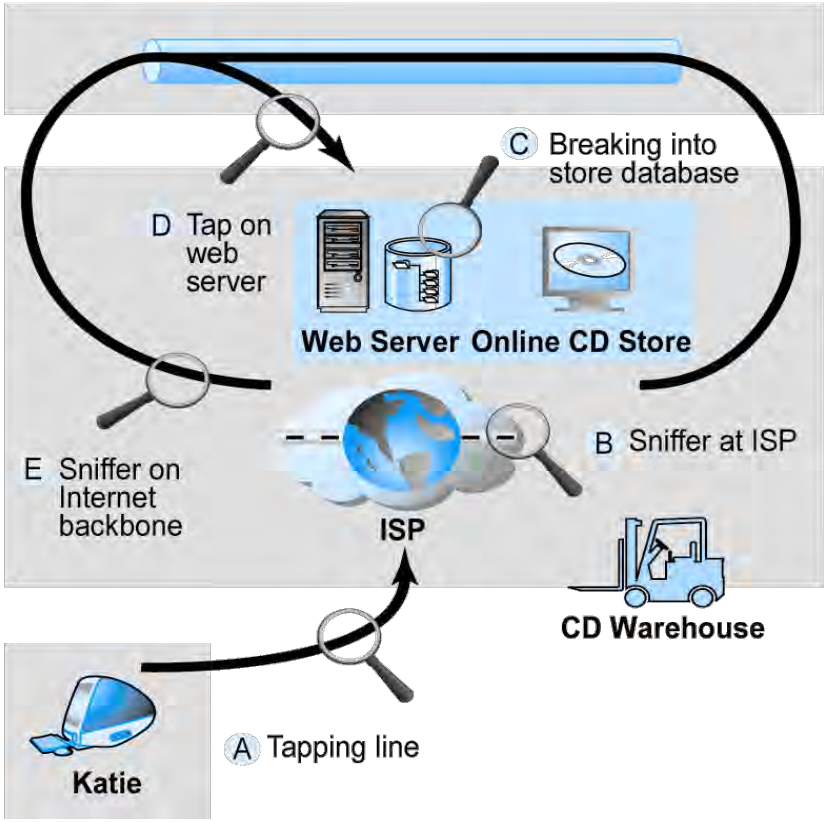
Internet communications

Servers

ISP
Merchant
Banks

Clients

Business
Home



Tapping and sniffing
Alteration of messages
Theft and fraud

DoS attack
Hacking
Malicious code attack
Theft and fraud
Line taps
Vandalism

Malicious code attack
Line taps
Physical loss of computer

MALICIOUS CODE

- Viruses: computer program that has ability to replicate and spread to other files; most also deliver a "payload" of some sort (may be destructive or benign); include macro viruses, file-infecting viruses, and script viruses
- Worms: designed to spread from computer to computer
- Trojan horse: appears to be benign, but then does something other than expected
- Bots: can be covertly installed on computer; responds to external commands sent by the attacker

PHISHING

- Any deceptive, online attempt by a third party to obtain confidential information for financial gain
  - Most popular type: e-mail scam letter
  - One of fastest growing forms of e-commerce crime

HACKING AND CYBERVANDALISM

- Hacker: Individual who intends to gain unauthorized access to computer systems
- Cracker: Used to denote hacker with criminal intent (two terms often used interchangeably)
- Cybervandalism: Intentionally disrupting, defacing or destroying a Web site
- Types of hackers include:
  - White hats
  - Black hats
  - Grey hats

CREDIT CARD FRAUD

- Fear that credit card information will be stolen deters online purchases
- Hackers target credit card files and other customer information files on merchant servers; use stolen data to establish credit under false identity
- One solution: New identity verification mechanisms

INSIGHT ON SOCIETY: "EVIL TWINS" AND "PHARMING": KEEPING UP WITH THE HACKERS? CLASS DISCUSSION

- What are "evil twins" and "pharming"
- What is meant by "social engineering techniques?"
- What is the security weakness in the domain name system that permits pharming?
- What steps can users take to verify they are communicating with authentic sites and networks?

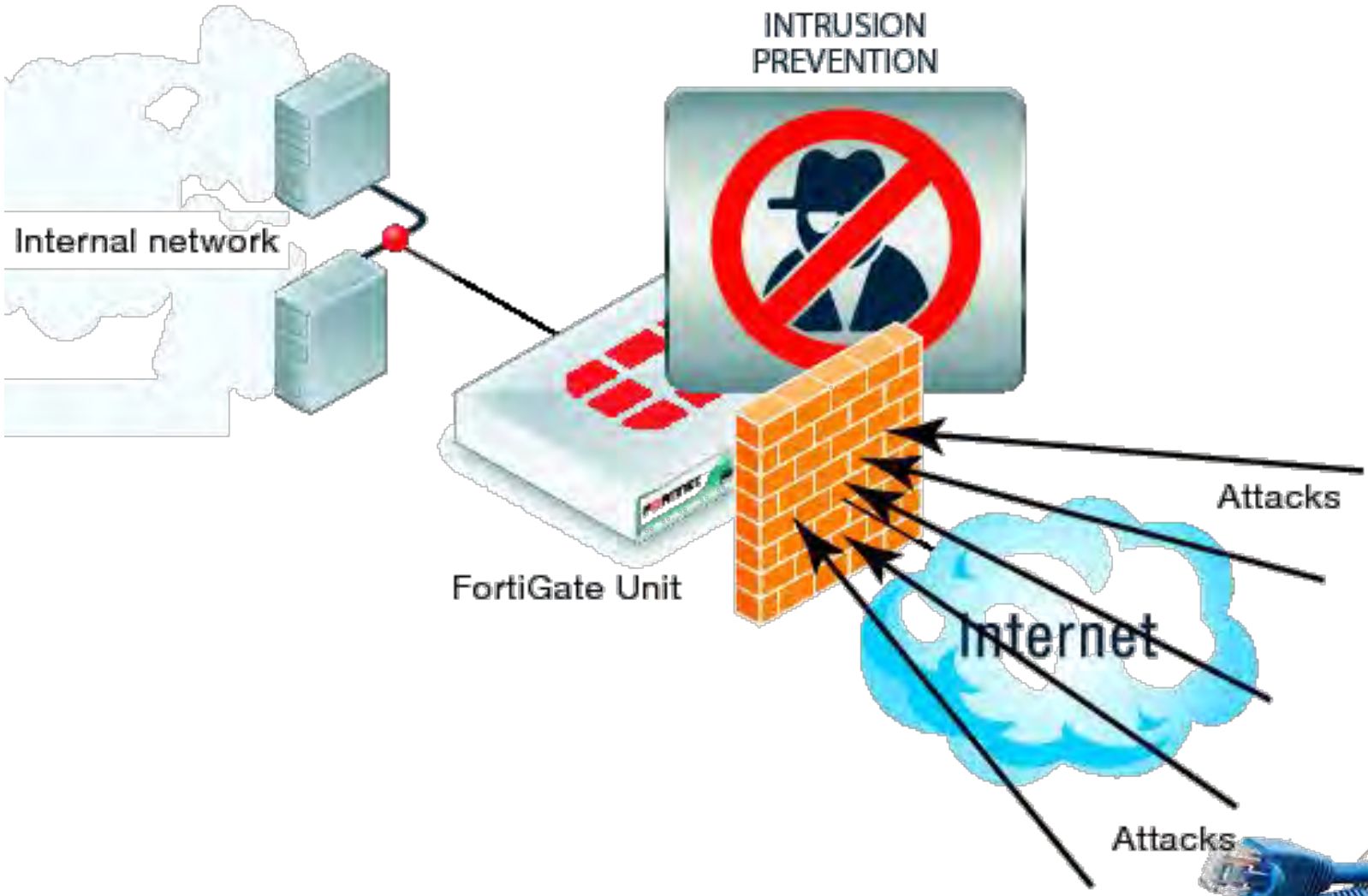
OTHER SECURITY THREATS

- Sniffing: Type of eavesdropping program that monitors information traveling over a network; enables hackers to steal proprietary information from anywhere on a network
- Insider jobs: Single largest financial threat
- Poorly designed server and client software: Increase in complexity of software programs has contributed to an increase is vulnerabilities that hackers can exploit

FIREWALL

WHAT IS A FIREWALL?

- A **choke point** of control and monitoring
- Interconnects networks with differing trust
- Imposes restrictions on network services
  - only authorized traffic is allowed
- Auditing and controlling access
  - can implement alarms for abnormal behavior
- Itself immune to penetration
- Provides **perimeter defence**

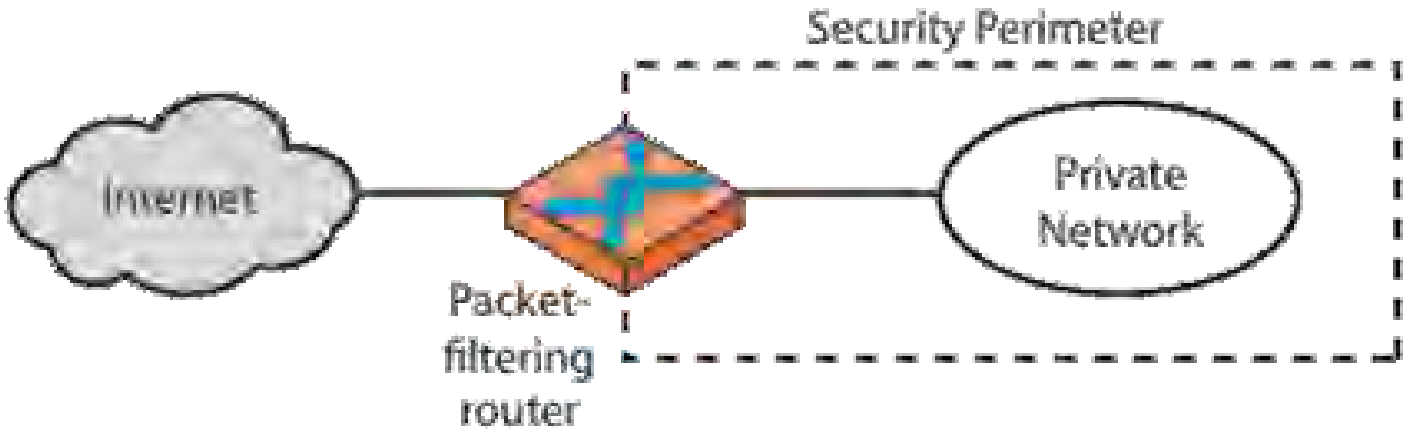

INTRUSION
PREVENTION
Internal network
FortiGate Unit
Attacks
Internet
Attacks

- Middle ground between protected and public nets
- Damage detection and limitation
- Uses
  - Block access
  - Selected prevention
  - Monitor
  - Record
  - Encryption

CLASSIFICATION OF FIREWALL

- Characterized by protocol level it controls in
  - Packet filtering
  - Circuit gateways
  - Application gateways
- Combination of above is dynamic packet filter

FIREWALLS – PACKET FILTERS



(a) Packet-filtering router

FIREWALLS – PACKET FILTERS

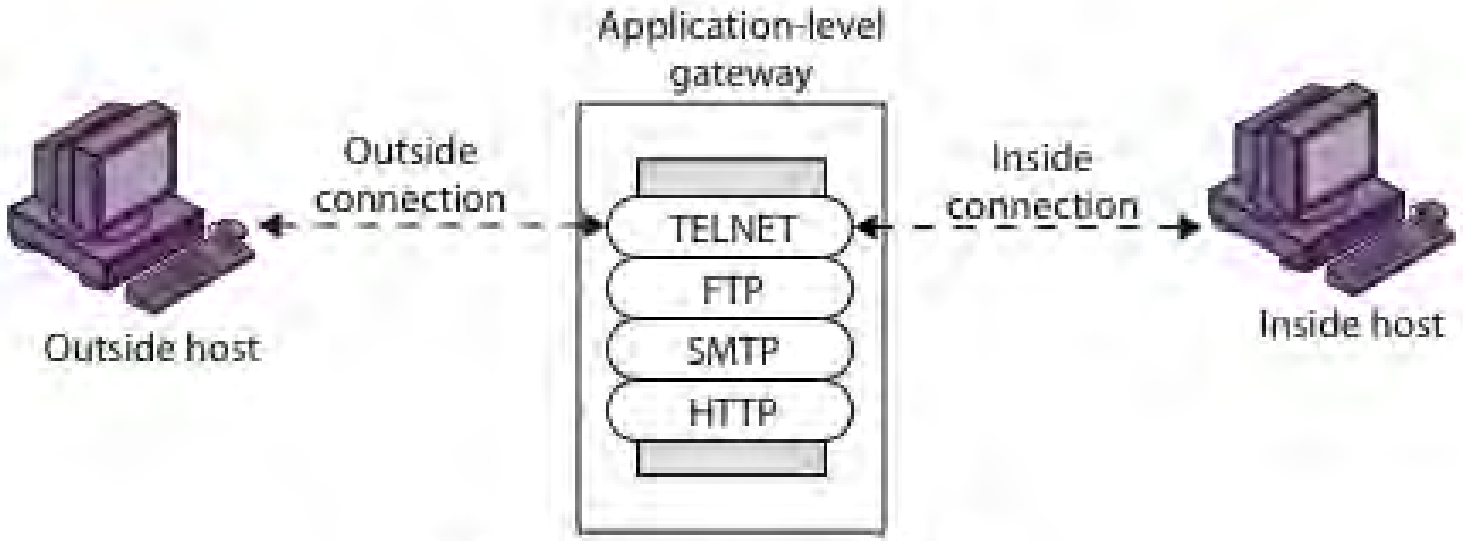
- Sometime called screening router
- It receives packets and evaluates them according to a set of rules that are usually in the form of access control lists
- These packets may be forwarded to their destinations, dropped, or dropped with a return message to the originator describing what happened.
- most frequently applied are
  - IP Source Address, Destination Address
    - all packets from source address 128.44.9.0 through 128.44.9.255 might be accepted, but all other packets might be rejected

- Source and destination port
  - all TCP packets originating from or destined to port 25
  - the simple mail transfer protocol, or SMTP, port
  - might be accepted, but all TCP packets destined for port 79—the finger port—might be dropped).
- Direction of traffic
  - inbound or outbound
- Type of protocol
  - IP, TCP, user datagram protocol, or internetwork packet exchange
- The packet's state
  - SYN, meaning synchronize, or ACK, which is the acknowledgement that a connection between hosts has already been established

FIREWALL GATEWAYS

- Firewall runs set of proxy programs
  - Proxies filter incoming, outgoing packets
  - All incoming traffic directed to firewall
  - All outgoing traffic appears to come from firewall
- Policy embedded in proxy programs
- Two kinds of proxies
  - Application-level gateways/proxies
    - Tailored to http, ftp, smtp, etc.
  - Circuit-level gateways/proxies
    - Working on TCP level

FIREWALLS - APPLICATION LEVEL GATEWAY (OR PROXY)

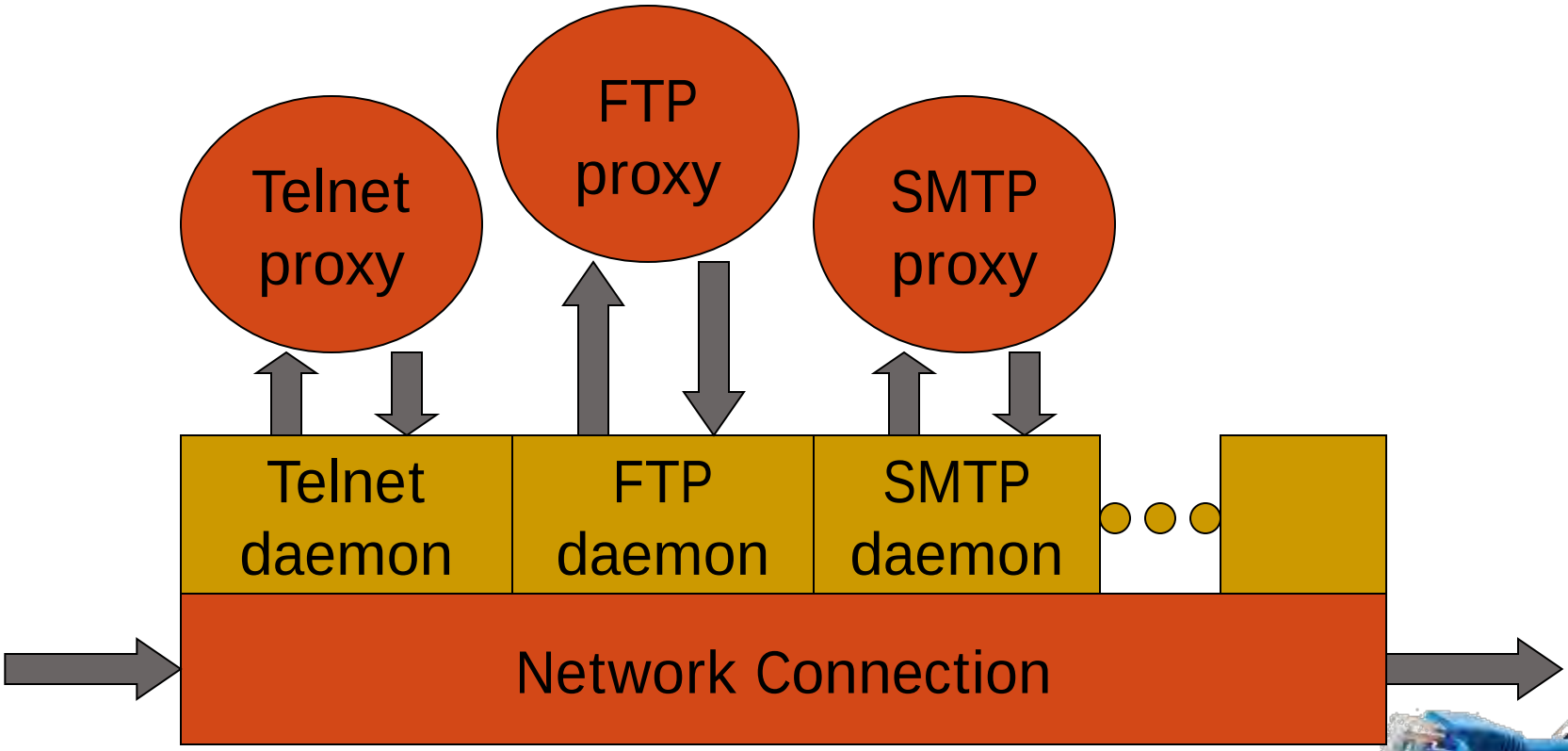


(b) Application-level gateway

APPLICATION-LEVEL FILTERING

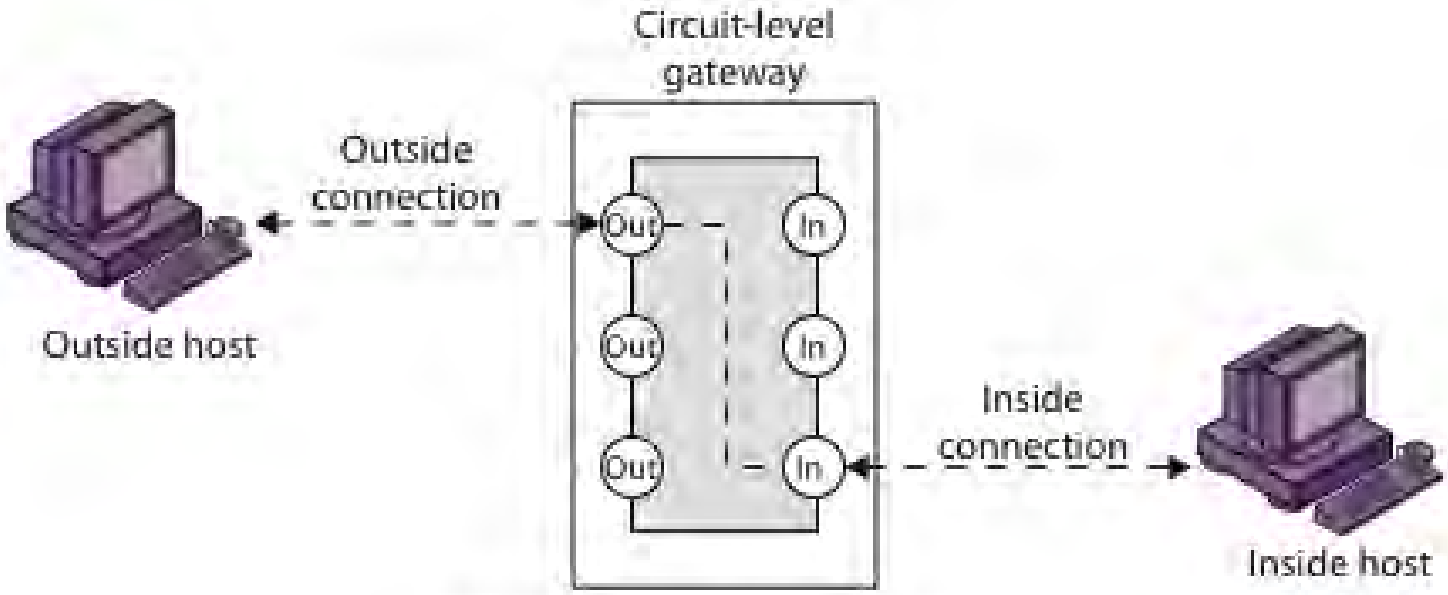
- Has full access to protocol
  - user requests service from proxy
  - proxy validates request as legal
  - then actions request and returns result to user
- Need separate proxies for each service
  - E.g., SMTP (E-Mail)
  - NNTP (Net news)
  - DNS (Domain Name System)
  - NTP (Network Time Protocol)
  - custom services generally not supported

APP-LEVEL FIREWALL ARCHITECTURE



Daemon spawns proxy when communication detected …

FIREWALLS - CIRCUIT LEVEL GATEWAY



(c) Circuit-level gateway

FIREWALLS - CIRCUIT LEVEL GATEWAY

- Applies security mechanisms when a TCP or UDP connection is established. Once the connection has been made, packets can flow between the hosts without further checking.
- circuit-gateway firewall, has been designed to remedy this limitation by producing a more seamless, transparent connection between clients and destinations using routines in special libraries.
- The connection is often described as a virtual circuit, because the proxy creates an end-to-end connection between the client and the destination application.

- Most circuit-gateway firewalls are implemented using SOCKS, a tool that includes a set of client libraries for proxy interfaces with clients.
- SOCKS receives an incoming connection from clients, and if the connections are allowed, it provides the data necessary for each client to connect to the application.
- Each client then invokes a set of commands to the gateway.
- The circuit-gateway firewall imposes all predefined restrictions, such as the particular commands that can be executed, and establishes a connection to the destination on the client's behalf.
- To users, this process appears transparent.

WHAT IS AN ANTI-VIRUS?

- **Antivirus software is a class of program that searches a hard drive and floppy disk for any known or potential viruses.**
- **Antivirus program runs in the Random Accesses Memory of a computer.**
- **Anti-virus software typically uses two different techniques to accomplish this:**
  - **Examining files to look for known viruses by means of a virus dictionary.**
  - **Identifying suspicious behavior from any computer program which might indicate infection.**
  - **Most commercial anti-virus software uses both of these approaches, with an emphasis on the virus dictionary approach.**

WHAT IS AN ANTI-VIRUS?

- Anti-virus is a software (computer program) that scans files or your computer's memory for certain patterns that may indicate an infection. The patterns it looks for are based on the signatures, or fingerprints, of known viruses.
- Once a virus is detected in the wild, the Anti-Virus companies then release these new patterns for your Anti-virus software to use.
- These updates come out daily by some vendors.
- Virus authors are continually releasing new and updated viruses, so it is important that you have the latest definitions installed on your computer.

WHAT IS AN ANTI-VIRUS?

- Once you have installed an anti-virus package, you should scan your entire computer periodically. Always leave your Anti-virus software running so it can provide constant protection.
- **Automatic scans-** Depending what software you choose, you may be able to configure it to automatically scan specific files or directories and prompt you at set intervals to perform complete scans.

WHAT IS AN ANTI-VIRUS?

- **Manual scans-** It is also a good idea to manually scan files you receive from an outside source before opening them.

This includes: Saving and scanning email attachments or web downloads rather than selecting the option to open them directly from the source. Scanning floppy disks, CDs, or DVDs for viruses before opening any of the files

HOW DOES AN ANTI-VIRUS WORKS?

- Anti-virus applications maintain a database of known viruses and compare scanned files that match the characteristics of known viruses.
- If a scanned files matches those characteristics of known viruses.
- If a scanned file matches those characteristics, it is quarantined (which means moved to a new, presumably safe location on disk and renamed, so you can find it should you ever need it) so that it cannot affect other files on your system.

HOW DOES AN ANTI-VIRUS WORKS?

- Signature detection is just one way of identifying viruses and is only effective if the virus database is up-to-date and contains the signature of a virus.
- Anti-virus programs also attempt to identify suspicious behavior include an application attempting to write to an executable file, altering needed system files, making suspicious registry entrees, or adding to the list of items that execute automatically upon system start up.

HOW DOES AN ANTI-VIRUS WORKS?

- Once the file is quarantined, the application can attempt to repair it, delete it, or prompt you for a decision on what to do about the file infected.
- This approach helps protect against unidentified or encrypted viruses and can alert you to suspicious behavior happening on your computer.
- This interesting is an area where anti-spyware/anti-adware and anti-virus software often notice the same kinds of activities, because they are typical for adware and spyware as well as malware

WHY DIDN'T MY ANTIVIRUS SOFTWARE WORK?

- It's crucial to keep your antivirus software current with the latest updates (usually called definition files) that help the tool identify and remove the latest threats.
- In addition, not all antivirus tools are the same; if you find that the one you use isn't working to your satisfaction, you should do some research and try an alternative.

DATA AND MESSAGE SECURITY

- Would you be willing to type in your credit card number knowing the risk?
- Even worse, would you expose your customers to that risk?
- In short, the lack of business transaction security is widely acknowledged as a major impediment to w
- Transaction security issues can be divided into two types:
  - **data** security
  - **message** security.

DATA SECURITY

- Also, computer industry trends toward distributed computing, and mobile computers, users face security challenges.
- Sniffer attacks begin when a computer is compromised and the cracker installs a packet sniffing program that monitors the network to which the machine is attached.
  - The sniffer program watches for certain kinds of network traffic, typically for the first part of any Telnet, FTP, or login sessions
  - The first part of the session contains the log-in ID, password, and user name of the person logging into another machine, all the necessary information a sniffer needs to log into other machines.

MESSAGE SECURITY

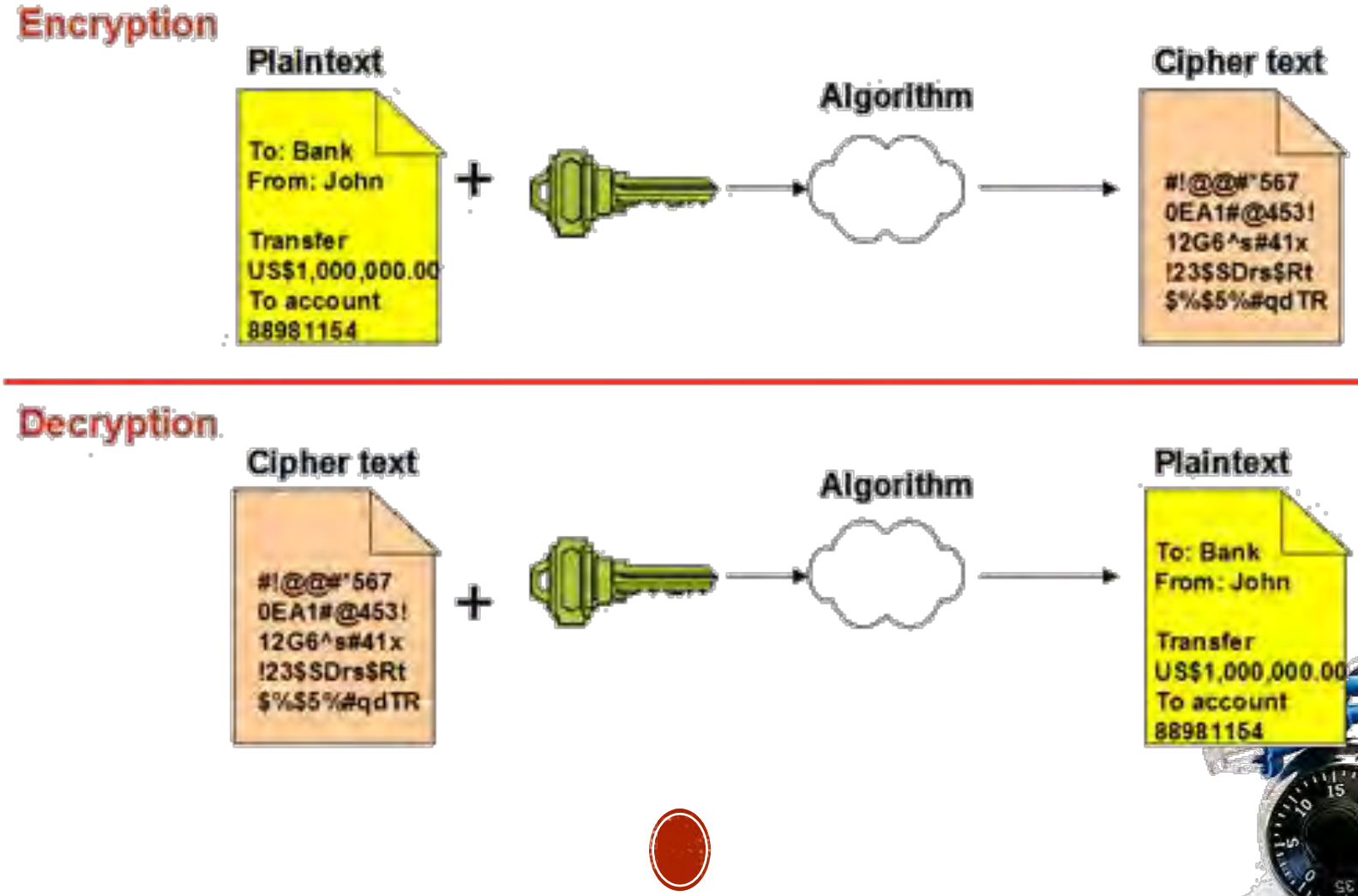
- Threats to message security fall into three categories:
  - confidentiality,
  - integrity, and
  - authentication.

ENCRYPTION TECHNIQUES FOR DATA AND MESSAGE SECURITY

- Encryption is a generic term that refers to the act of encoding data, in this context so that those data can be securely transmitted via the Internet.
- Encryption can protect the data at the simplest level by preventing other people from reading the data.
- Encryption technologies can help in other ways as well
  - establishing the identity of users ;
  - control the unauthorized transmission or forwarding of data;
  - verify the integrity of the data
  - ensure that users take responsibility for data that they have transmitted.

- Encryption can therefore be used either to keep communications secret or to identify people involved in communications
- Encryption Provide Following Security:
  - **Message Integrity**: provides assurance that the message has not been altered.
  - **No repudiation**: prevents the users from denying he/she sent the message
  - **Authentication**: provides verification of the identity of the person (or machine) sending the message.
  - **Confidentiality**: give assurance that the message was not read by others.
- There are two types of encryption:
  - **symmetric key** encryption and
  - **asymmetric key** encryption.

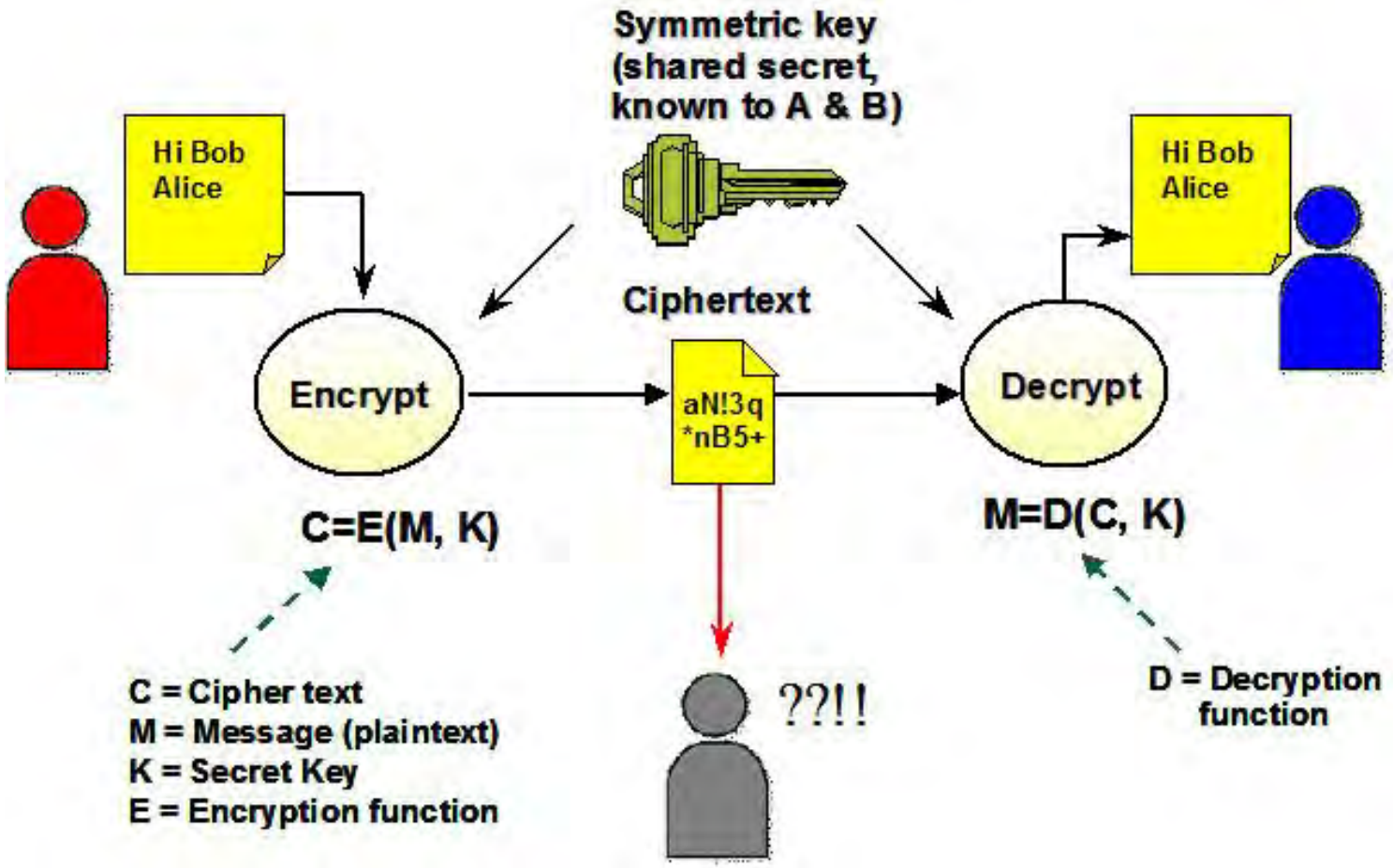
SYMMETRIC KEY ENCRYPTION (PRIVATE OR SECRET KEY ENCRYPTION):



- Encryption algorithms that use the same key for encrypting and for decrypting information are called **symmetric-key algorithms**.
- The symmetric key is also called a secret key because it is kept as a shared secret between the sender and receiver of information.
- Symmetric key encryption is much faster than public key encryption, often by 100 to 1,000times. Symmetric key technology is generally used to provide secrecy for the bulk encryption and decryption of information.
- Cryptography-based security technologies use a variety of symmetric key encryption algorithms to provide confidentiality.
- Symmetric algorithms have the advantage of not consuming too much computing power.

- People can use this encryption method as either a "**stream**" cipher or a "**block**" cipher, depending on the amount of data being encrypted or decrypted at a time.
- A stream cipher encrypts data one character at a time as it is sent or received,
- a block cipher processes fixed block (chunks) of data.
- Common symmetric encryption algorithms include Data Encryption Standard (DES), Advanced Encryption Standard (AES), and International Data Encryption Algorithm (IDEA).

ASYMMETRIC KEY ENCRYPTION(PUBLIC KEY ENCRYPTION):



- Encryption algorithms that use different keys for encrypting and decrypting information are most often called public-key algorithms but are sometimes also called ***asymmetric key algorithm***.
- Public key encryption requires the use of both a private key (a key that is known only to its owner) and a public key (a key that is available to and known to other entities on the network).
- A user's public key, for example, can be published in the directory so that it is accessible to other people in the organization.
- Information that is encrypted with the public key can be decrypted only with the corresponding private key of the set.

- Today, public key encryption plays an increasingly important role in providing strong, scalable security on intranets and the Internet. Public key encryption is commonly used to perform the following functions:
  - Encrypt symmetric secret keys to protect the symmetric keys during exchange over the network.
  - Create digital signatures to provide authentication and non-repudiation for online entities.
  - Create digital signatures to provide data integrity for electronic files and documents.

NETWORK SECURITY

Introduction to Network Security

A network security is defined as a circumstance, condition with the potential to cause economic hardship to data or network resources in the form of destruction, disclosure, modification of data, denial of service, and/or fraud, waste, and abuse.

The discussion of security concerns in electronic commerce can be divided into two broad types:

Client/server security uses various authorization methods to make sure that only valid user and programs have access to information resources such as databases. Access control mechanisms must be set up to ensure that properly authenticated users are allowed access only to those resources that they are entitled to use. Such mechanisms include password protection, encrypted smart cards, biometrics, and firewalls.

Data and transaction security ensures the privacy and confidentiality in electronic messages and data packets, including the authentication of remote users in network transactions for activities such as on-line payments. The goal is to defeat any attempt to assume another identity while involved with electronic mail or other forms of data communication. Preventive measures include data encryption using various cryptographic methods.

Client/Server Network Security

Client/server network security is one of the biggest headaches system administrators face as they balance the opposing goals of user maneuverability and easy access and site security and confidentiality of local information. According to the National Center for Computer Crime Data, computer security violations cost U.S. businesses half a billion dollars each year.

Network security on the Internet is a major concern for commercial organizations, especially top management. Recently, the Internet has raised many new security concerns. By connecting to the Internet, a local network organization may be exposing itself to the entire population on the Internet. As figure below illustrates, an Internet connection opens itself to access from other networks comprising the public Internet.

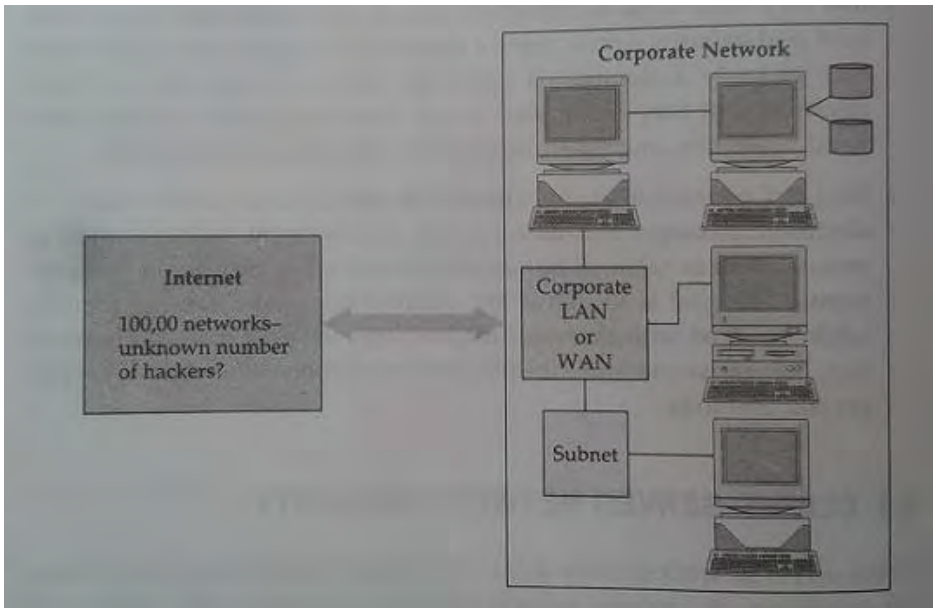


Fig: Unprotected Internet Connection

That being the case, the manager of even the most relaxed organization must pay some attention to security. For many commercial operations, security will simply be a matter of making sure that existing system features, such as passwords and privileges, are configured properly. They need to audit all access to the network. A system that records all log-on attempts—particularly the unsuccessful ones—can alert managers to the need for stronger measures. However, where secrets are at stake or where important corporate assets must be made available to remote users, additional measures must be taken. Hackers can use password guessing, password trapping, security holes in programs, or common network access procedures to impersonate users and thus pose a threat to the server.

Client–server network security problems manifest themselves in three ways:

1. **Physical security holes** result when individuals gain unauthorized physical access to a computer. A good example would be a public workstation room, where it would be easy for a wandering hacker to reboot a machine into single-user mode and tamper with the files, if precautions are not taken. On the network, this is also a common problem, as hackers gain access to network systems by guessing passwords of various users.
2. **Software security holes** result when badly written programs or "privileged" software are "compromised" into doing things they shouldn't. The most famous example of this category is the "sendmail" hole, which brought the Internet to its knees in 1988. A more recent problem was the "rlogin" hole in the IBM RS-6000 workstations, which enabled a cracker (a malicious hacker) to create a "root" shell or superuser access mode. This is the highest level of access possible and could be used to delete the entire file system, or create a new account or password file.

3. **Inconsistent usage holes** result when a system administrator assembles a combination of hardware and software such that the system is seriously flawed from a security point of view. The incompatibility of attempting two unconnected but useful things creates the security hole. Problems like this are difficult to isolate once a system is set up and running, so it is better to carefully build the system with them in mind. This type of problem is becoming common as software becomes more complex.

To reduce these security threats, various protection methods are used. At the file level, operating systems typically offer mechanisms such as access control lists that specify the resources various users and groups are entitled to access. Protection—also called authorization or access control— grants privileges to the system or resource by checking user-specific information such as passwords. The problem in the case of e-commerce is very simple: If consumers connect a computer to the Internet, they can easily log into it from anywhere that the network reaches.

That's the good news. The bad news is that without proper access control, anyone else can too. Over the years, several protection methods have been developed, including trust-based security, security through obscurity, password schemes, and biometric systems.

Trust-Based Security

Quite simply, trust-based security means to trust everyone and do nothing extra for protection. It is possible not to provide access restrictions of any kind and to assume that all users are trustworthy and competent in their use of the shared network. This approach assumes that no one ever makes an expensive breach such as getting root access and deleting all files (a common hacker trick). This approach worked in the past, when the system administrator had to worry about a limited threat. Today, this is no longer the case.

Security through Obscurity:

Most organizations in the mainframe era practiced a philosophy known as security through obscurity (STO)—the notion that any network can be secure as long as nobody outside its management group is allowed to find out anything about its operational details and users are provided information on a need-to-know basis. Hiding account passwords in binary files or scripts with the presumption that "nobody will ever find them" is a prime case of STO (somewhat like hiding the housekey under the doormat and telling only family and friends). In short, STO provides a false sense of security in computing systems by hiding information.

Password Schemes:

One straightforward security solution, a password scheme, erects a first level barrier to accidental intrusion. In actuality, however, password schemes do little about deliberate attack, especially when common words or proper names are

selected as passwords. For instance, network administrators at a Texas air force base discovered that they could crack about 70 percent of the passwords on their UNIX network with tools resembling those used by hackers. The simplest method used by most hackers is dictionary comparison— comparing a list of encrypted user passwords against a dictionary of encrypted common words EGCN941. This scheme often works because users tend to choose relatively simple or familiar words as passwords. To beat the dictionary comparison method, experts often recommend using a minimum of eight-character length mixed-case passwords containing at least one non-alphanumeric character and changing passwords every 60 to 90 days.

Biometric Systems:

Biometric systems, the most secure level of authorization, involve some unique aspect of a person's body. Past biometric authentication was based on comparisons of fingerprints, palm prints, retinal patterns, or on signature verification or voice recognition. Biometric systems are very expensive to implement: At a cost of several thousand dollars per reader station, they may be better suited for controlling physical access—where one biometric unit can serve for many workers—than for network or workstation access. Many biometric devices also carry a high price in terms of inconvenience; for example, some systems take 10 to 30 seconds to verify an access request.

Firewalls and Its Types

The most commonly accepted network protection is a barrier—a firewall between the corporate network and the outside world (untrusted network). The term firewall can mean many things to many people, but basically it is a method of placing a device—a computer or a router—between the network and the Internet to control and monitor all traffic between the outside world and the local network. Typically, the device allows insiders to have full access to services on the outside while granting access from the outside only selectively, based on log-on name, password, IP address or other identifiers as shown in figure below.

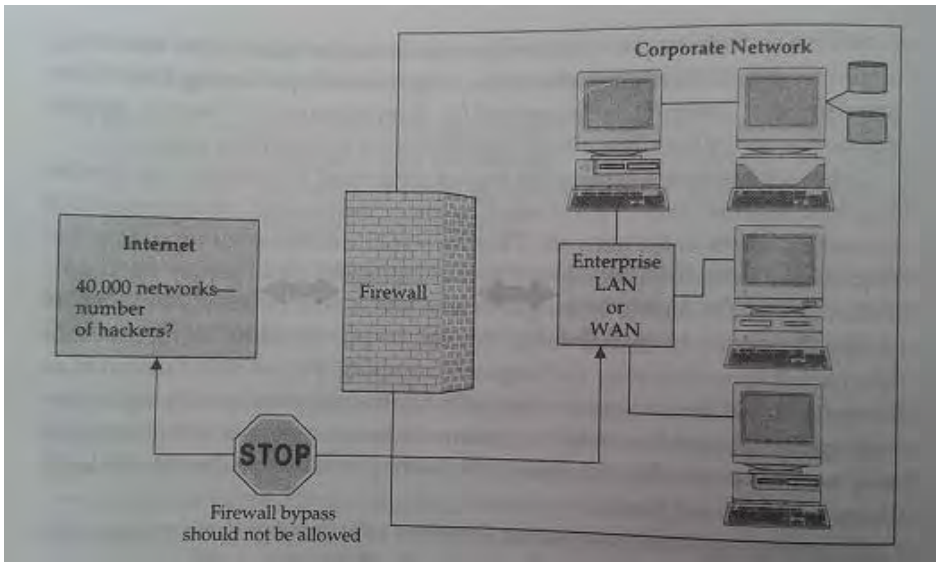


Fig: Firewall-secured Internet Connection

Generally speaking, a firewall is a protection device to shield vulnerable areas from some form of danger. In the context of the Internet, a firewall is a system—a router, a personal computer, a host, or a collection of hosts—set up specifically to shield a site or subnet from protocols and services that can be abused from hosts on the outside of the subnet. A firewall system is usually located at a gateway point, such as a site's connection to the Internet, but can be located at internal gateways to provide protection for smaller collection of hosts or subnets.

Firewalls come in several types and offer various levels of security. Generally, firewalls operate by screening packets and/or the applications that pass through them, provide controllable filtering of network traffic, allow restricted access to certain applications, and block access to everything else. The actual mechanism that accomplishes filtering varies widely, but in principle, the firewall can be thought of as a pair of mechanisms: one to block incoming traffic and the other to permit outgoing traffic. Some firewalls place a greater emphasis on blocking traffic, and others emphasize permitting traffic.

In short, the general reasoning behind firewall usage is that, without a firewall, network security is a function of each host on the network and all hosts must cooperate to achieve a uniformly high level of security. The larger the subnet, the less manageable it is to maintain all hosts at the same level of security. As mistakes and lapses in security become more common, break-ins can occur not as the result of complex attacks, but because of simple errors in configuration and inadequate passwords.

Types of Firewall (Firewalls in Practice)

Firewalls range from simple traffic logging systems that record all network traffic flowing through the firewall in a file or database for auditing purposes to more complex methods such as IP packet screening routers, hardened fire-wall hosts, and

proxy application gateways. The simplest firewall is a packet- filtering gateway or screening router. Configured with filters to restrict packet traffic to designated addresses, screening routers also limit the types of services that can pass through them.

More complex and secure are application gateways. They are essentially PCs or UNIX boxes that sit between the Internet and a company's internal network to provide proxy services to users on either side. For example, a user who wants to FTP in or out through the gateway would connect to FTP software running on the firewall, which then connects to machines on the other side of the gateway. Screening routers and application gateway firewalls are frequently used in combination when security concerns are very high.

IP Packet Screening Routers:

This is a static traffic routing service placed between the network service provider's router and the internal network. The traffic routing service may be implemented at an IP level via screening rules in a router or at an application level via proxy gateways and services. Figure below shows a secure firewall with an IP packet screening router.

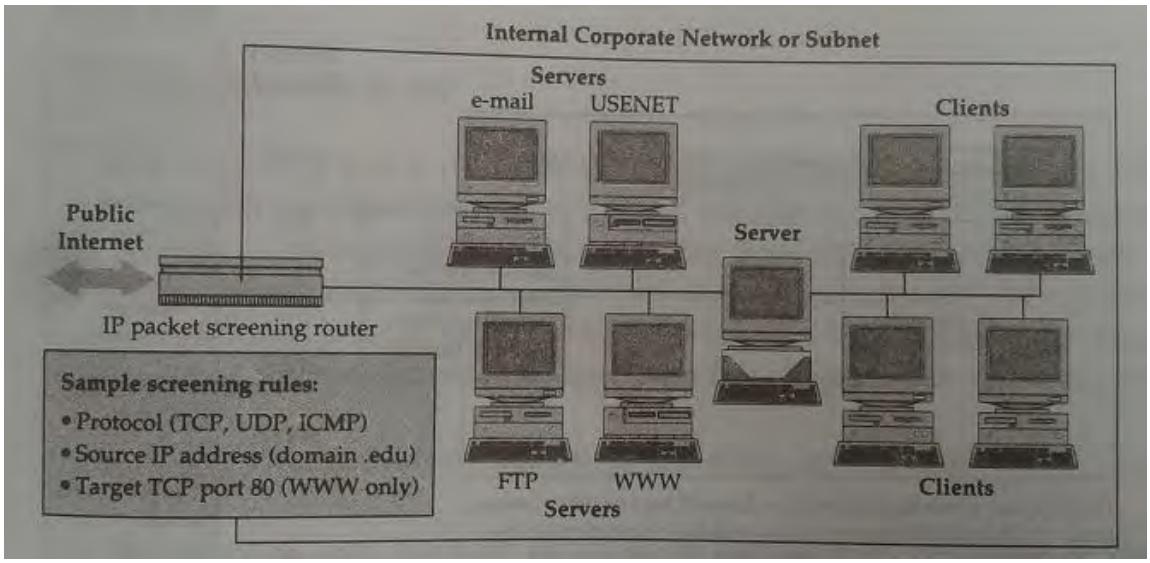


Fig: Secure firewall with IP packet screening router

The firewall router filters incoming packets to permit or deny IP packets based on several screening rules. These screening rules, implemented into the router are automatically performed. Rules include target interface to which the packet is routed, known source IP address, and incoming packet protocol (TCP, UDP, ICMP). ICMP stands for Internet Control Message Protocol, a network management tool of the TCP/IP protocol suite.

Although properly configured routers can plug many security holes, they do have several disadvantages. First, screening rules are difficult to specify, given the vastly diverse needs of users. Second, screening routers are fairly inflexible and do not easily extend to deal with functionality different from that preprogrammed by the

vendor. Lastly, if the screening router is circumvented by a hacker, the rest of the network is open to attack.

Proxy Application Gateways:

A proxy application gateway is a special server that typically runs on a firewall machine. Their primary use is access to applications such as the World Wide Web from within a secure perimeter as shown in figure below. Instead of talking directly to external WWW servers, each request from the client would be routed to a proxy on the firewall that is defined by the user. The proxy knows how to get through the firewall. An application- Level proxy makes a firewall safely permeable for users in an organization, without creating a potential security hole through which hackers can get into corporate networks. The proxy waits for a request from inside the firewall, forwards the request to the remote server outside the firewall, reads the response, and then returns it to the client. In the usual case, all clients within a given subnet use the same proxy. This makes it possible for the proxy to execute efficient caching of documents that are requested by a number of clients. The proxy must be in a position to filter dangerous URLs and malformed commands.

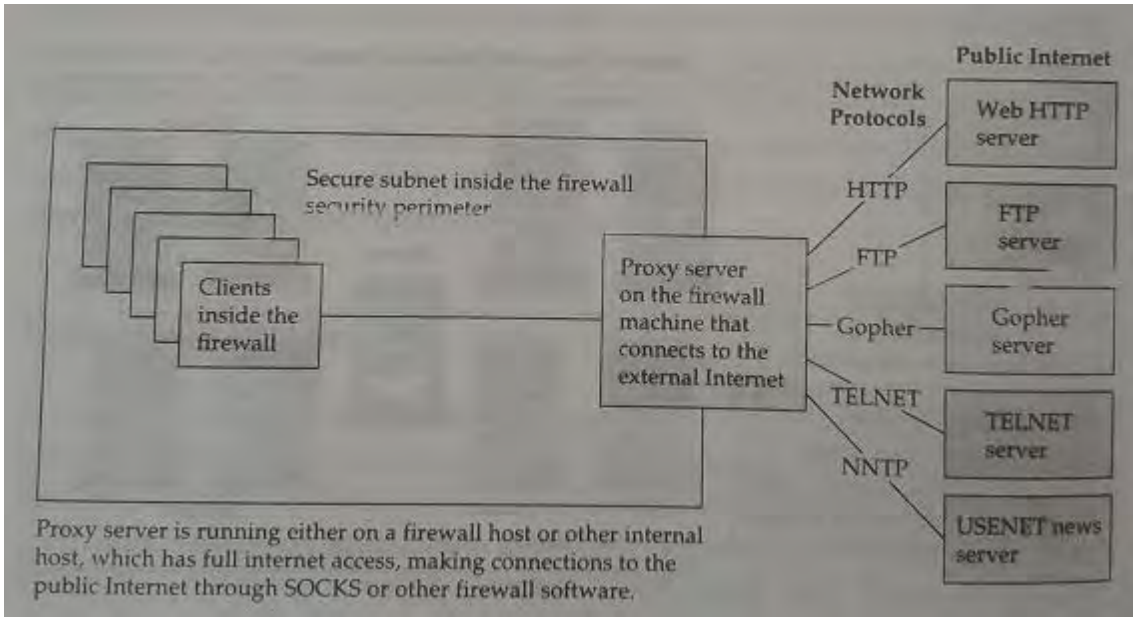


Fig: Proxy servers on the World Wide Web

Hardened Firewall Hosts: A hardened firewall host is a stripped-down machine that has been configured for increased security. This type of firewall requires inside or outside users to connect to the trusted applications on the firewall machine before connecting further. Generally, these firewalls are configured to protect against unauthenticated interactive log-ins from the external world. This, more than anything, helps prevent unauthorized users from logging into machines on the network.

The hardened firewall host method can provide a greater level of audit and security, in return for increased configuration cost and decreased 'level of service (because a proxy needs to be developed for each desired service).

Data and Message Security (Private or Secret and Public Key Cryptography)

The lack of data and message security on the Internet has become a high- profile problem due to the increasing number of merchants trying to spur commerce on the global network. For instance, credit card numbers in their plain text form create a risk when transmitted across the Internet where the possibility of the number falling into the wrong hands is relatively high.

Would you be willing to type in your credit card number knowing the risk? Even worse, would you expose your customers to that risk? In short, the lack of business transaction security is widely acknowledged as a major impediment to widespread e- commerce.

Historically, computer security was provided by the use of account passwords and limited physical access to a facility to bona fide users. As users began to dial in from their PCs and terminals at home, these measures were deemed sufficient. With the advent of remote users on internetworks, commercial transactions, mobile computers, and wireless technologies, simple password schemes are not sufficient to prevent attacks from sophisticated hackers.

Interestingly, the security problems plaguing network administrators resemble the problems facing transaction-based electronic commerce. Credit card numbers are similar to passwords in many ways. A growing threat on today's public (and sometimes even private) networks is the theft of passwords and other information that passes over them. Today's hacker has an array of tools to reach and manipulate information from remote sites as well as to engage in unauthorized eavesdropping. Unsuspecting and amateur users logging into remote hosts are the most vulnerable.

Transaction security issues can be divided into two types: **data** and **message** security. These are discussed below.

Data Security:

Electronic data security is of paramount importance at a time when people are considering banking and other financial transactions by PCs. Also, computer industry trends toward distributed computing, and mobile computers, users face security challenges. One major threat to data security is unauthorized network monitoring, also called packet sniffing.

Sniffer attacks begin when a computer is compromised and the cracker installs a packet sniffing program that monitors the network to which the machine is attached. The sniffer program watches for certain kinds of network traffic, typically for the first part of any Telnet, FTP, or login sessions— sessions that legitimate

users initiate to gain access to another system. The first part of the session contains the log-in ID, password, and user name of the person logging into another machine, all the necessary information a sniffer needs to log into other machines. In the course of several days, the sniffer could gather information on local users logging into remote machines. So, one insecure system on a network can expose to intrusion not only other local machines but also any remote systems to which the users connect.

The fact that someone can extract meaningful Information from network traffic is nothing new. Network monitoring can rapidly expand the number of systems intruders are able to access, all with only minimal impact on the systems on which the sniffers are installed and with no visible impact on the systems being monitored. Users whose accounts and passwords are collected will not be aware that their sessions are being monitored, and subsequent intrusions will happen via legitimate accounts on the machines involved.

Message Security:

Threats to message security fall into three categories:

1. confidentiality,
2. integrity, and
3. authentication.

1. Message Confidentiality-

Confidentiality is important for uses involving sensitive data such as credit card numbers. This requirement will be amplified when other kinds of data, such as employee records, government files, and social security numbers, begin traversing the network. Confidentiality precludes access to, or release of, such information to unauthorized users.

The environment must protect all message traffic. After successful delivery to their destination gateways, messages must be removed (expunged) from the public environment. All that remains is the accounting record of entry and delivery, including message length, authentication data, but no more. All message archiving must be performed in well-protected systems.

The vulnerability of data communications and message data to interception is exacerbated with the use of distributed networks and wireless links. The need for securing the communications link between computers via encryption is expected to rise.

2 . Message and System Integrity-

Business transactions require that their contents remain unmodified during transport. In other words, information received must have the same content and

organization as information sent. It must be clear that no one has added, deleted, or modified any part of the message.

While confidentiality protects against the passive monitoring of data, mechanisms for integrity must prevent active attacks involving the modification of data. Error detection codes or checksums, sequence numbers, and encryption techniques are methods to enhance information integrity. Encryption techniques such as digital signatures can detect modifications of a message. .

3. Message Sender Authentication/Identification-

For e-commerce, it is important that clients authenticate themselves to servers, that servers authenticate to clients, that both authenticate to each other. Authentication is a mechanism whereby the receiver of a transaction or message can be confident of the identity of the sender and/or the integrity of the message. In other words, authentication verifies the identity of an entity (a user or a service) using certain encrypted information transferred from the sender to the receiver.

Authentication in e-commerce basically requires the user to prove his or her identity for each requested service. The race among various vendors in the e-commerce today is to provide an authentication method that is easy to use, secure, reliable, and scalable. Third party authentication services must exist within a distributed network environment where a sender cannot be trusted to identify itself correctly to a receiver. In short, authentication plays an important role in the implementation of business transaction security.

Encryption Techniques for Data and Message Security (Private and Public Key Cryptography)

The success or failure of an e-commerce operation depends on different key factors, including but not limited to the business model, the team, the customers, the investors, the product, and the security of data transmissions and storage. Data security has taken on heightened importance since a series of high-profile "cracker" attacks have humbled popular Web sites, resulted in the impersonation of Microsoft employees for the purposes of digital certification, and the misuse of credit card numbers of customers at business-to-consumer e-commerce destinations. Security is on the mind of every e-commerce entrepreneur who solicits, stores, or communicates any information that may be sensitive if lost. Technologists are building new security measures while others are working to crack the security systems. One of the most effective means of ensuring data security and integrity is **encryption**.

Encryption is a generic term that refers to the act of encoding data, in this context so that those data can be securely transmitted via the Internet. Encryption can protect the data at the simplest level by preventing other people from reading the data. In the event that someone intercepts a data transmission and manages to

deceive any user identification scheme, the data that they see appears to be gibberish without a way to decode it. Encryption technologies can help in other ways as well, by establishing the identity of users (or abusers); control the unauthorized transmission or forwarding of data; verify the integrity of the data (i.e., that it has not been altered in any way); and ensure that users take responsibility for data that they have transmitted.

Encryption can therefore be used either to keep communications secret (defensively) or to identify people involved in communications (offensively). Encryption Provide Following Security:

- **Message Integrity**: provides assurance that the message has not been altered.
- **No repudiation**: prevents the users from denying he/she sent the message
- **Authentication**: provides verification of the identity of the person (or machine) sending the message.
- **Confidentiality**: give assurance that the message was not read by others.

There are two types of encryption: **symmetric key** encryption and **asymmetric key** encryption. Symmetric key and asymmetric key encryption are used, often in conjunction, to provide a variety of security functions for data and message security in e-commerce.

Symmetric Key Encryption (Private or Secret Key Encryption):

Encryption algorithms that use the same key for encrypting and for decrypting information are called symmetric-key algorithms. The symmetric key is also called a secret key because it is kept as a shared secret between the sender and receiver of information. Otherwise, the confidentiality of the encrypted information is compromised. Figure below shows basic symmetric key encryption and decryption.

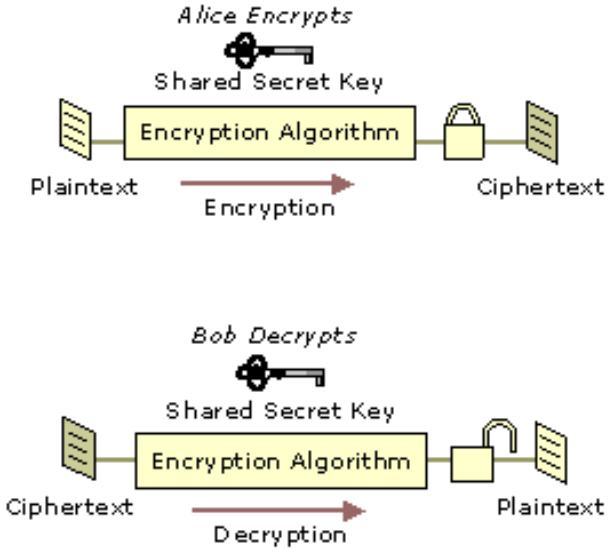


Fig: Encryption and Decryption with a Symmetric Key

Symmetric key encryption is much faster than public key encryption, often by 100 to 1,000times. Symmetric key technology is generally used to provide secrecy for the bulk encryption and decryption of information.

Cryptography-based security technologies use a variety of symmetric key encryption algorithms to provide confidentiality. Symmetric algorithms have the advantage of not consuming too much computing power. People can use this encryption method as either a "**stream**" cipher or a "**block**" cipher, depending on the amount of data being encrypted or decrypted at a time.

A stream cipher encrypts data one character at a time as it is sent or received, while a block cipher processes fixed block (chunks) of data. Common symmetric encryption algorithms include Data Encryption Standard (DES), Advanced Encryption Standard (AES), and International Data Encryption Algorithm (IDEA).

Asymmetric Key Encryption(Public Key Encryption):

Encryption algorithms that use different keys for encrypting and decrypting information are most often called public-key algorithms but are sometimes also called ***asymmetric key algorithm***. Public key encryption requires the use of both a private key (a key that is known only to its owner) and a public key (a key that is available to and known to other entities on the network). A user's public key, for example, can be published in the directory so that it is accessible to other people in the organization. The two keys are different but complementary in function. Information that is encrypted with the public key can be decrypted only with the corresponding private key of the set. Figure below shows basic encryption and decryption with asymmetric keys.

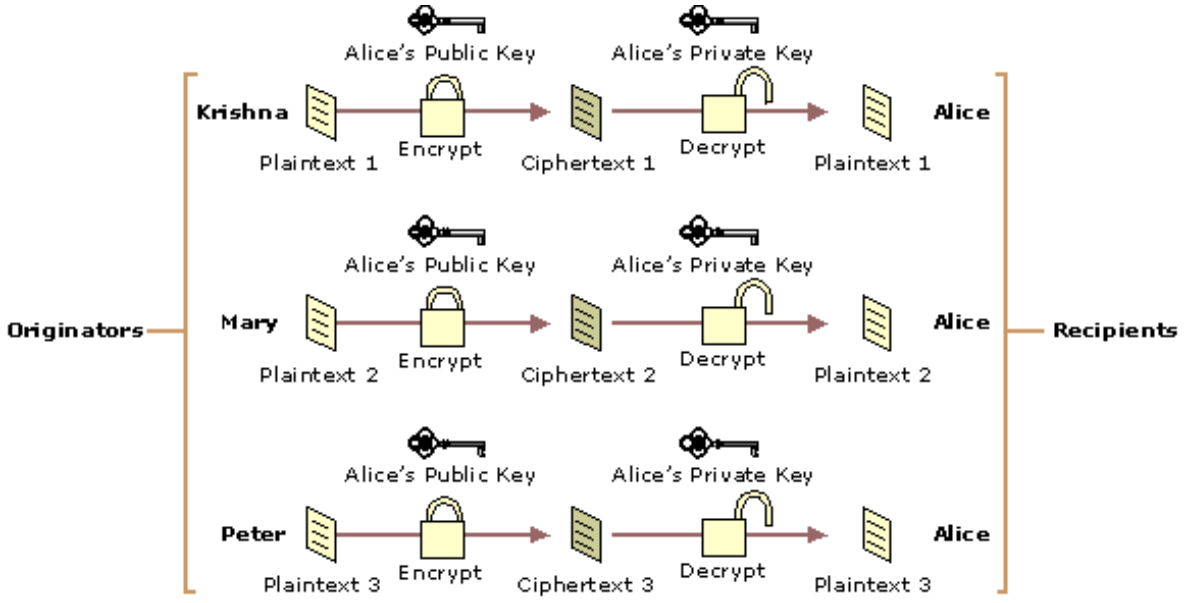


Fig: Encryption and Decryption with Asymmetric Keys

Today, public key encryption plays an increasingly important role in providing strong, scalable security on intranets and the Internet. Public key encryption is commonly used to perform the following functions:

- Encrypt symmetric secret keys to protect the symmetric keys during exchange over the network.
- Create digital signatures to provide authentication and non-repudiation for online entities.
- Create digital signatures to provide data integrity for electronic files and documents.

Algorithms that use public key encryption methods include RSA and Diffie-Hellman.

Common Cryptosystems

- **RSA Algorithm**: RSA is the most commonly used public key algorithm, although it is vulnerable to attack. Named after its inventors, Ron Rivest, Adi Shamir and Len Adleman, of the MIT, RSA was first published in 1978. It is used for encryption as well as for electronic signatures (discussed later). RSA lets you choose the size of your public key. The 512-bit keys are considered insecure or weak. The 768-bit keys are secure from everything but 1024-bit keys are secure from virtually anything.
- **Data Encryption Standards (DES)**: DES was developed by IBM in1974 in response to a public solicitation from the US Department of Commerce. It was adopted as a US federal standard in1977 and as a financial industry standard in1981. DES uses a 56-bit key to encrypt.
- **3DES**: A stronger version of DES, called 3DES or Triple DES, uses three 56-bit keys to encrypt each block. The first key encrypts the data block, the second key decrypts the data block, and the third key encrypts the same data block again. The 3DES version requires a 168-bit key that makes the process quite secure and much safer than plain DES.
- **RC4**: RC4 was designed by Ron Rivest RSA Data Security Inc. this variable-length cipher is widely used on the Internet as the bulk encryption cipher in the SSL protocol, with key length ranging from 40 to 128 bits. RC4 has a repudiation of being very fast. **e IDEA**: IDEA (International Data Encryption Algorithm) was created in Switzerland in1991. it offers very strong encryption using 1 128-bit key to encrypt 64-bit blocks. This system is widely used as the bulk encryption cipher in older version of Pretty Good Privacy(PGP)

Digital Signature

Just as handwritten signatures or physical thumbprints are commonly used to uniquely identify people for legal proceedings or transactions, so digital signatures are commonly used to identify electronic entities for online transactions. A digital

signature uniquely identifies the originator of digitally signed data and also ensures the integrity of the signed data against tampering or corruption.

One possible method for creating a digital signature is for the originator of data to create the signature by encrypting all of the data with the originator's private key and enclosing the signature with the original data. Anyone with the originator's public key can decrypt the signature and compare the decrypted message to the original message. Because only someone with the private key can create the signature, the integrity of the message is verified when the decrypted message matches the original. If an intruder alters the original message during transit, the intruder cannot also create a new valid signature. If an intruder alters the signature during transit, the signature does not verify properly and is invalid.

However, encrypting all data to provide a digital signature is impractical for following two reasons:

- The ciphertext signature is the same size as the corresponding plaintext, so message sizes are doubled, consuming large amounts of bandwidth and storage space.
- Public key encryption is slow and places heavy computational loads on computer processors.

Digital signature algorithms use more efficient methods to create digital signatures. The most common types of digital signatures today are created by signing **message digests** with the originator's private key to create a digital thumbprint of the data. Because only the message digest is signed, the signature is usually much shorter than the data that was signed. Therefore, digital signatures place a relatively low load on computer processors during the signing process, consume insignificant amounts of bandwidth. Two of the most widely used digital signature algorithms today are the **RSA digital signature** process and the **Digital Signature Algorithm** (DSA).

RSA Data Security Digital Signature Process:

In the RSA digital signature process, the private key is used to encrypt only the message digest. The encrypted message digest becomes the digital signature and is attached to the original data. Figure below illustrates the basic RSA Data Security digital signature process.

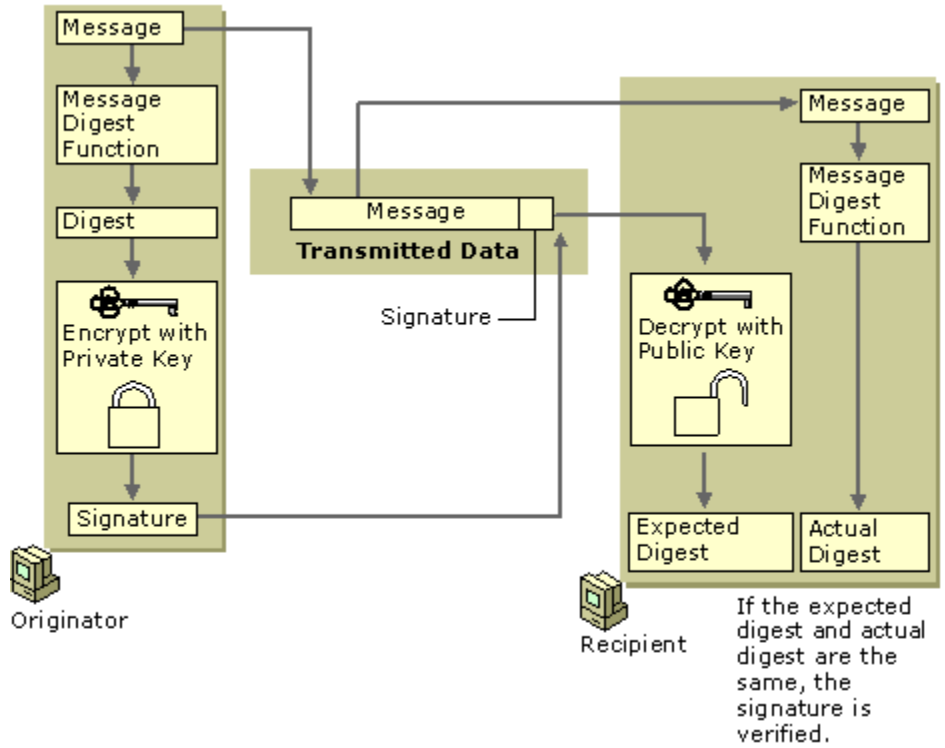


Fig: Basic RSA Data Security Digital Signature Process

To verify the contents of digitally signed data, the recipient generates a new message digest from the data that was received, decrypts the original message digest with the originator's public key, and compares the decrypted digest with the newly generated digest. If the two digests match, the integrity of the message is verified. The identification of the originator also is confirmed because the public key can decrypt only data that has been encrypted with the corresponding private key.

Digital Certificate and Certification Authority

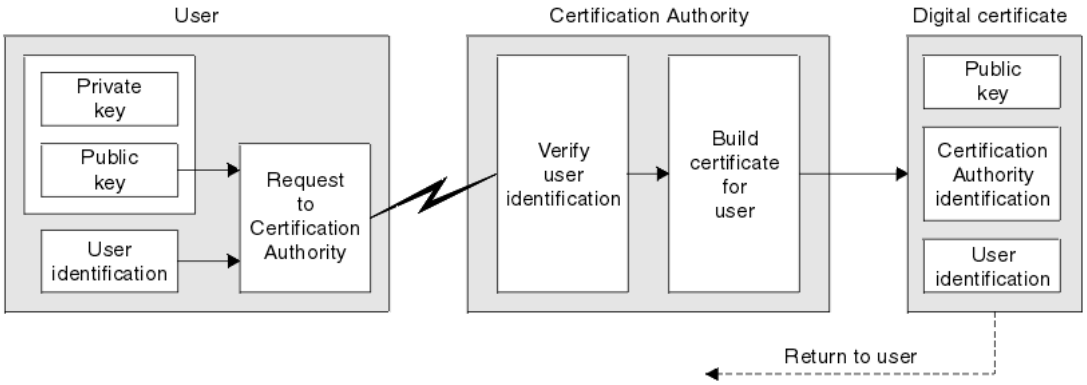
Digital certificates are electronic credentials that are used to assert the online identities of individuals, computers, and other entities on a network. **Digital certificates** function similarly to identification cards such as passports and drivers licenses. Most commonly they contain a public key and the identity of the owner. They are issued by certification authorities (CAs) that must validate the identity of the certificate-holder both before the certificate is issued and when the certificate is used. Common uses include business scenarios requiring authentication, encryption, and digital signing.

Most certificates in common use today are based on the X.509v3 certificate standard. X.509v3 stands for version 3 of the International Telecommunication Union Telecommunication Standardization Sector (ITU-T) recommendation X.509 for certificate syntax and format.

Typically, certificates contain the following information:

- The subject's public key value
- The subject's identifier information, such as the name and email address
- The validity period (the length of time that the certificate is considered valid)
- Issuer identifier information
- The digital signature of the issuer, which attests to the validity of the binding between the subject's public key and the subject's identifier information

Process to obtain a Certificate From CA: One can obtain a certificate for your business from commercial CAs. The Issuing entities of commercial CAs provide certificate with a cost. User can generate a Key pair of its own and generate a Certificate Signing Request (CSR) and then send the CSR to Issuing CA for a certificate. CSR contains the public key of the user and user identity information in a format that issuing CAs would normally expect as shown in figure below.



A **Certificate Authority (CA)** issues digital certificates that contain a public key and the identity of the owner. The matching private key is not made available publicly, but kept secret by the end user who generated the key pair. The certificate is also a confirmation or validation by the CA that the public key contained in the certificate belongs to the person, organization, server or other entity noted in the certificate. A CA's obligation in such schemes is to verify an applicant's credentials, so that users and relying parties can trust the information in the CA's certificates.

CAs use a variety of standards and tests to do so. In essence, the Certificate Authority is responsible for saying "yes, this person is who they say they are, and we, the CA, verify that". If the user trusts the CA and can verify the CA's signature, then he can also verify that a certain public key does indeed belong to whoever is identified in the certificate. Browsers maintain list of well known CAs root certificates. Aside from commercial CAs, some providers issue digital certificates to the public at no cost. Large institutions or government entities may have their own CAs.

Third Party Authentication

In third-party authentication systems, the password or encryption key itself never travels over the network. Rather, an "authentication server" maintains a file of obscure facts about each registered user. At log-on time, the server demands the entry of a randomly chosen fact— mother's maiden name is a traditional example— but this information is not sent to the server.

Instead, the server uses it (along with other data, such as the time of day) to compute a token. The server then transmits an encrypted message containing the token, which can be decoded with the user's key. If the key was properly computed, the user can decrypt the message. The message contains an authentication token that allows users to log on to network services.

There are many variations on this theme. For example, users can tell the authentication server with which remote computer they want to converse.

Kerberos:

Kerberos is a popular third-party authentication protocol. Kerberos is an encryption-based system that uses secret key encryption designed to authenticate users and network connections. It was developed at MIT's Project Athena in the 1980s and is named after the three-headed dog of Greek mythology that guards the entrance to Hades. Like its namesake, Kerberos is charged with preventing unauthorized access and does it so well that it is now a de facto standard for effecting secure, authenticated communications across a network.

The assumption of Kerberos is that the distributed environment is made up of unsecured workstations, moderately secure servers, and highly secure key-management machines. Kerberos provides a means of verifying the identities of requestor (a workstation user or a network server) on an unprotected network. The goal is to accomplish security without relying on authentication by the host computer, without basing trust on the IP addresses, without requiring physical security of all the hosts on the network, and under the assumption that IP packets on the network can be read, modified, and inserted at will. Kerberos performs authentication under these conditions as a trusted third-party authentication service by using conventional cryptography (secret key).

The authentication process proceeds as follows: Client A sends a request to the Kerberos authentication server (KAS) requesting "credentials" for a given server, B. The KAS responds with the following information, which is encrypted in A's key:

- A "ticket" for the server. This ticket contains B's key.
- A temporary encryption key (often called a "session key").

A then transmits—the client's identity and a copy of the session key, both encrypted in B's key—to B.

The session key (now shared 'by the client and server) is used to authenticate the client and used to authenticate the server in future transaction. The session key is then used to encrypt further communication between the two parties or to exchange a separate sub-session key to be used to encrypt further communication.

Using Certificates for Secure Web Communications (SSL)

Secure Sockets Layer (SSL) and **Transport Layer Security** (TLS) are protocols that are used to provide secure Web communications on the Internet or intranets. TLS is the standardized (on the Internet Engineering Task Force—IETF—level) version of SSL. TLS is also referred to as SSL version 3.1, whereas the most commonly used SSL version is 3.0. Both protocols can provide the following basic security services:

- **Mutual authentication.** Verifies the identities of both the server and client through exchange and validation of their digital certificates.
- **Communication privacy.** Encrypts information exchanged between secure servers and secure clients using a secure channel.
- **Communication integrity.** Verifies the integrity of the contents of messages exchanged between client and server, which ensure that messages haven't been altered en route.

Sample Scenario Example: Here's an example of an environment using SSL/TLS. When you use the Internet for online banking, it's important to know that your Web browser is communicating directly and securely with your bank's Web server. Your Web browser must be able to achieve Web server authentication before a safe transaction can occur. That is, the Web server must be able to prove its identity to your Web browser before the transaction can proceed.

Microsoft IE uses SSL to encrypt messages and transmit them securely across the Internet, as do most other modern Web browsers and Web servers.

Computer Authentication in VPNs

The use of certificates for authentication of VPN connections is the strongest form of authentication available with the Windows Server 2003 family. You must use certificate-based authentication for VPN connections.

Sample Scenario Example: Here's a short example of the use of certificates in a VPN scenario. When an employee logs in to the organization's network from home using a VPN, the VPN server can present a server certificate to establish its identity. Because the corporate root authority is trusted and the corporate root CA issued the certificate of the VPN server, the client computer can proceed with the connection and the employee knows their computer is actually connected to their organization's VPN server.

The VPN server must also be able to authenticate the VPN client before data can be exchanged over the VPN connection. Either computer-level authentication occurs

with the exchange of computer certificates or user-level authentication occurs though the use of a Point-to-Point Protocol (PPP) authentication method.

The client computer certificate can serve multiple purposes, most of which are based in authentication, allowing the client to use many organizational resources without needing individual certificates for each resource. For example, the client certificate might allow clients VPN connectivity, as well as access to the company store intranet site, product servers, and the human resources database where employee data is stored.

Secure Electronic Transmission (SET)

The **Secure Electronic Transmission** protocol imitates the current structure of the credit card processing system. SET makes banks by default one of the major distributors of certificates. When a user might change organizations or lose his or her key pair, or an e-commerce site using SSL may discontinue its operations; a certificate must be revoked before it expires. In all these cases, the certificate needs to be revoked before it expires so that it cannot be used intentionally or unintentionally.

The most important property of SET is that the credit card number is not open to the seller. On the other hand, the SET protocol, despite strong support from Visa and MasterCard, has not appeared as a leading standard.

The two major reasons for lack of widespread acceptance are followings:

1. The complexity of SET
2. The need for the added security that SET provides.

Though, this might change in the future as encryption technology becomes more commonly utilized in the e-business world.

Advantages of SET:

Some of the advantages of SET contain the following:

1. Information security: Neither anyone listening in nor a merchant can use the information passed during a transaction for fraud.
2. Credit card security: There is no chance for anybody to steal a credit card.
3. Flexibility in shopping: If a person has a phone he/she can shop.

Disadvantages of SET:

Some of the disadvantages of SET include its complexity and high cost for implementation.

UNIT 6: ELECTRONIC PAYMENT SYSTEMS

Introduction to Electronic Payment System (Requirements and Risks)

Electronic payment systems are becoming central to on-line business process innovation as companies look for ways to serve customers faster and at lower cost. Emerging innovations in the payment for goods and services in electronic commerce promise to offer a wide range of new business opportunities.

Electronic payment systems and e-commerce are intricately linked given that on-line consumers must pay for products and services. Clearly, payment is an integral part of the mercantile process and prompt payment (or account settlement) is crucial. If the claims and debits of the various participants—individuals, companies, banks, and nonbanks—are not balanced because of payment delay or, even worse default, then the entire business chain is disrupted. Hence an important aspect of e-commerce is prompt and secure payment, clearing, and settlement of credit or debit claims.

But on-line sellers face a problem: How will buyers pay for goods and services? What currency will serve as the medium of exchange in this new marketplace? Everyone agrees that the payment and settlement process is a potential bottleneck in the fast-moving electronic commerce environment if we rely on conventional payment methods such as cash, checks, bank drafts, or bills of exchange. Electronic replicas of these conventional instruments are not well suited for the speed required in e-commerce purchase processing. For instance, payments of small denominations (micropayments) must be made and accepted by vendors in real time for snippets(pieces) of information. Conventional instruments are too slow for micropayments and the high transaction costs involved in processing them add greatly to the overhead.

Therefore new methods of payment are needed to meet the emerging demands of ecommerce. These new payment instruments must be secure, have a low processing cost, and be accepted widely as global currency tender.

We will examine these demands by looking at the following issues:

- What form and characteristics of payment instruments—for example, electronic cash, electronic checks, credit/debit cards—will consumers use?
- In on-line markets, how can we manage the financial risk associated with various payment instruments—privacy, fraud, mistakes, as well as other risks like bank failures? What security features (authentication, privacy, anonymity) need to be designed to reduce these risks?

To answer these questions, we will draw on examples of various electronic payment systems that have been proposed, prototyped, or actually deployed (implemented).

Types of Electronic Payment Systems:

Electronic payment systems grow rapidly in banking, retail, health care, on-line markets, and even government—in fact, anywhere money needs to change hands. Organizations are motivated by the need to deliver products and services more cost effectively and to provide a higher quality of service to customers. Let's briefly describe the pertinent developments in various industries to provide an overall picture of electronic payment systems of the present.

Research into electronic payment systems for consumers can be traced back to the 1940s, and the first applications—credit cards—appeared soon after. In the early 1970s, the emerging electronic payment technology was labeled electronic funds transfer (EFT). EFT is defined as "any transfer of funds initiated through an electronic terminal, telephonic instrument, or computer or magnetic tape. EFT utilizes computer and telecommunication components both to supply and to transfer money or financial assets.

Work on EFT can be segmented into three broad categories:

1. Banking and financial payments

- Large-scale or wholesale payments (e.g., bank-to-bank transfer)
- Small-scale or retail payments (e.g., automated teller machines and cash dispensers)
- Home banking (e.g., bill payment)

2. Retailing payments

- Credit cards (e.g., VISA or MasterCard)
- Private label credit/debit cards (e.g., J.C. Penney Card)
- Charge cards (e.g., American Express)

3. On-line electronic commerce payments

- Token-based payment systems
    - Electronic cash (e.g., DigiCash)
    - Electronic checks (e.g.; NetCheque)
    - Smart cards or debit cards (e.g., Mondex Electronic Currency Card)
- Credit card-based payment systems

- Encrypted credit cards (e.g., World Wide Web form-based encryption) Third-party
- authorization numbers (e.g., First Virtual)

Retail payments and large-scale payments between banks and business are widely recognized as the pioneering efforts in electronic commerce that involve the extensive use of EDI for transferring payment information.

Risks Associated with Electronic Payment System:

Electronic payment is a popular method of making payments globally. It involves sending money from bank to bank instantly – regardless of the distance involved. Such payment systems use Internet technology, where information is relayed through networked computers from one bank to another. Electronic payment systems are popular because of their convenience. However, they also may pose serious risks to consumers and financial institutions.

Tax Evasion

Businesses are required by law to provide records of their financial transactions to the government so that their tax compliance can be verified. Electronic payment however can frustrate the efforts of tax collection. Unless a business discloses the various electronic payments it has made or received over the tax period, the government may not know the truth, which could cause tax evasion.

Fraud

Electronic payment systems are prone to fraud. The payment is done usually after keying in a password and sometimes answering security questions. There is no way of verifying the true identity of the maker of the transaction. As long as the password and security questions are correct, the system assumes you are the right person. If this information falls into the possession of fraudsters, then they can defraud you of your money.

Impulse Buying

Electronic payment systems encourage impulse buying, especially online. You are likely to make a decision to purchase an item you find on sale online, even though you had not planned to buy it, just because it will cost you just a click to buy it through your credit card. Impulse buying leads to disorganized budgets and is one of the disadvantages of electronic payment systems.

Payment Conflict

Payment conflicts often arise because the payments are not done manually but by an automated system that can cause errors. This is especially common when payment is done on a regular basis to many recipients. If you do not check your pay

slip at the end of every pay period, for instance, then you might end up with a conflict due to these technical glitches, or anomalies.

Digital Token based Electronic Payment Systems

None of the banking or retailing payment methods is completely adequate in their present form for the consumer-oriented e-commerce environment. Their deficiency is their assumption that the parties will at some time be in each other's physical presence or that there will be a sufficient delay in the payment process for frauds, overdrafts, and other undesirables to be identified and corrected. These assumptions may not hold for e-commerce and so many of these payment mechanisms are being modified and adapted for the conduct of business over networks.

Entirely new forms of financial instruments are also being developed. One such new financial instrument is "**electronic tokens**" in the form of electronic cash/money or checks. Electronic tokens are designed as electronic analogs of various forms of payment backed by a bank or financial institution. Simply stated, electronic tokens are equivalent to cash that is backed by a bank.

Electronic tokens are of three types:

1. **Cash or real-time**: Transactions are settled with the exchange of electronic currency. An example of on-line currency exchange is *electronic cash* (*e-cash*).
2. **Debit or prepaid**: Users pay in advance for the privilege of getting information. Examples of prepaid payment mechanisms are stored in smart cards and electronic purses that store electronic money.
3. **Credit or postpaid**: The server authenticates the customers and verifies with the bank that funds are adequate before purchase. Examples of postpaid mechanisms are *credit/debit* cards and *electronic checks*.

Electronic Cash (e-cash)

Electronic cash (e-cash) is a new concept in on-line payment systems because it combines computerized convenience with security and privacy that improve on paper cash. Its versatility opens up a host of new markets and applications. E-cash presents some interesting characteristics that should make it an attractive alternative for payment over the Internet.

E-cash focuses on replacing cash as the principal payment vehicle in consumer-oriented electronic payments. Although it may be surprising to some, cash is still the most prevalent consumer payment instrument even after thirty years of continuous developments in electronic payment systems. Cash remains the dominant form of payment for three reasons: (1) lack of trust in the banking

system, (2) inefficient clearing and settlement of noncash transactions, and (3) negative real interest rates paid on bank deposits.

Now compare cash to credit and debit cards. First, they can't be given away because, technically, they are identification cards owned by the issuer and restricted to one user. Credit and debit cards are not legal tender, given that merchants have the right to refuse to accept them. Nor are credit and debit cards bearer instruments; their usage requires an account relationship and authorization system. Similarly, checks require either personal knowledge of the payer or a check guarantee system. Hence, to really create a novel electronic payment method, we need to do more than recreate the convenience that is offered by credit and debit cards. We need to develop e-cash that has some of the properties of cash.

What is electronic cash? : Electronic cash is one of the instruments that can be used to conduct paperless transactions. Paperless transaction is a term used to describe financial exchanges that do not involve the physical exchange of currency. Instead, monetary value is electronically credited and debited. Often called e-cash or digital money , this financial instrument is commonly used to conduct distant transactions, such as those between parties on the Internet and those between parties in different countries.

In most cases, e-cash is equivalent to paper currency and can therefore be exchanged among individuals or spent for any types of goods or services that a person wishes to acquire. This financial instrument has played a large role in the increasing popularity of telecommuting, which is an arrangement that allows people to work together in distant places.

Digital currency can allow a freelancer in Nepal to be paid for work that the he did for a contractor in Canada. This is possible due to a monetary exchange system. The value of that money is then credited to someone else in another place. The paper currency the sender presents or which is taken from his account is not physically sent and given to the receiver. Electronic cash is exchanged in a similar way. One major difference, however, is that transactions can often be conducted without a live middle man.

People involved in electronic cash transfers may never acquire any paper currency. They may receive their funds electronically and they may use them electronically. This does not mean, however, that it is impossible to get paper currency from electronic cash.

In many instances, electronic money can be converted into paper currency quite easily. This is possible because e-cash is commonly held in an account that can be accessed in several ways. For example, many have debit cards that can be used at an automated teller machine (ATM). Sometimes, a person can request that all or a portion of the money held electronically be made available by check.

There are a number of advantages of electronic cash. One of them is that it eliminates the apprehension that many people feel about carrying and exchanging paper currency. Another advantage of electronic cash is that it is usually easily converted to another currency, making traveling and international business substantially easier.

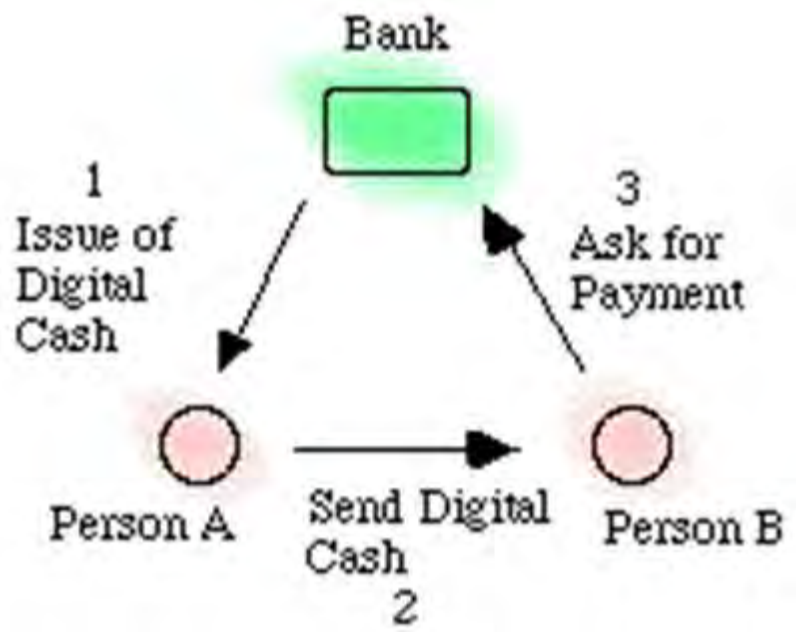


Fig: Transaction of Electronic Cash.

The figure shows the basic operation. User A obtains digital cash "coins" from her bank (and the bank deducts a corresponding amount from her account). The user is now entitled to use the coins by giving them to another user B, which might be a merchant. B receives e-cash during a transaction and see that it has been authorized by a bank. They can then pay the cash into their account at the bank.

Ideal properties of a Digital Cash system should be:

1. **Secure**. Alice should be able to pass digital cash to Bob without either of them, or others, able to alter or reproduce the electronic token.
2. **Anonymous**. Alice should be able to pay Bob without revealing her identity, and without Bob revealing his identity. Moreover, the Bank should not know who Alice paid or who Bob was paid by. Even stronger, they should have the option to remain anonymous concerning the mere existence of a payment on their behalf.
3. **Portable**. The security and use of the digital cash is not dependent on any physical location. The cash should be able to be stored on disk or USB memory stick, sent by email, SMS, internet chat, or uploaded on web forms. Digital cash should not be restricted to a single, proprietary computer network.

4. **Off-line capable**. The protocol between the two exchanging parties is executed offline, meaning that neither is required to be host-connected in order to proceed.
5. **Wide acceptability**. The digital cash is well-known and accepted in a large commercial zone. With several digital cash providers displaying wide acceptability, Alice should be able to use her preferred unit in more than just a restricted local setting.
6. **User-friendly**. The digital cash should be simple to use from both the spending perspective and the receiving perspective. Simplicity leads to mass use and mass use leads to wide acceptability. Alice and Bob should not require a degree in cryptography as the protocol machinations should be transparent to the immediate user.

Here is the summary of the pros and cons of the online electronic cash system:

Pros

- Provides fully anonymous and untraceable digital cash:
- No double spending problems (coins are checked in real time during the transaction).
- No additional secure hardware required

Cons

- Communications overhead between merchant and the bank.
- Huge database of coin records -- the bank server needs to maintain an ever-growing database for all the used coins' serial numbers.
- Difficult to scale, need synchronization between bank servers.
- Coins are not reusable

Electronic Checks:

When you write a check, you may assume that the piece of paper you write on will be deposited at a bank and processed manually. Electronic check conversion makes that process less and less likely. Instead of processing the piece of paper, some businesses prefer to turn your paper check into an electronic check.

> *How Electronic Checks Work? How does a piece of paper become an electronic check? The business you write the check to slips the check into a machine that reads information from your check. That information is all the business needs to collect money from your bank account.*

With E-Checks, a check imager is connected to a small printer through a credit card terminal directly at the point of sale. When a customer presents a check, the check

is scanned by the imager, the magnetic data (MICR) indicating the bank routing number and account number are read, and the dollar amount of the check is entered. The E-Check process verifies the check by comparing the check's bank account and the customer's driver's license with a national negative database to determine if the account has a fraud history, is closed, or has had insufficient funds (NSF) problems. If the check is approved, a receipt is printed for customer signature. The check and a copy of the signed receipt are returned to the customer. The captured data is used in the electronic transfer of money through the Automated Clearing House (ACH) system.

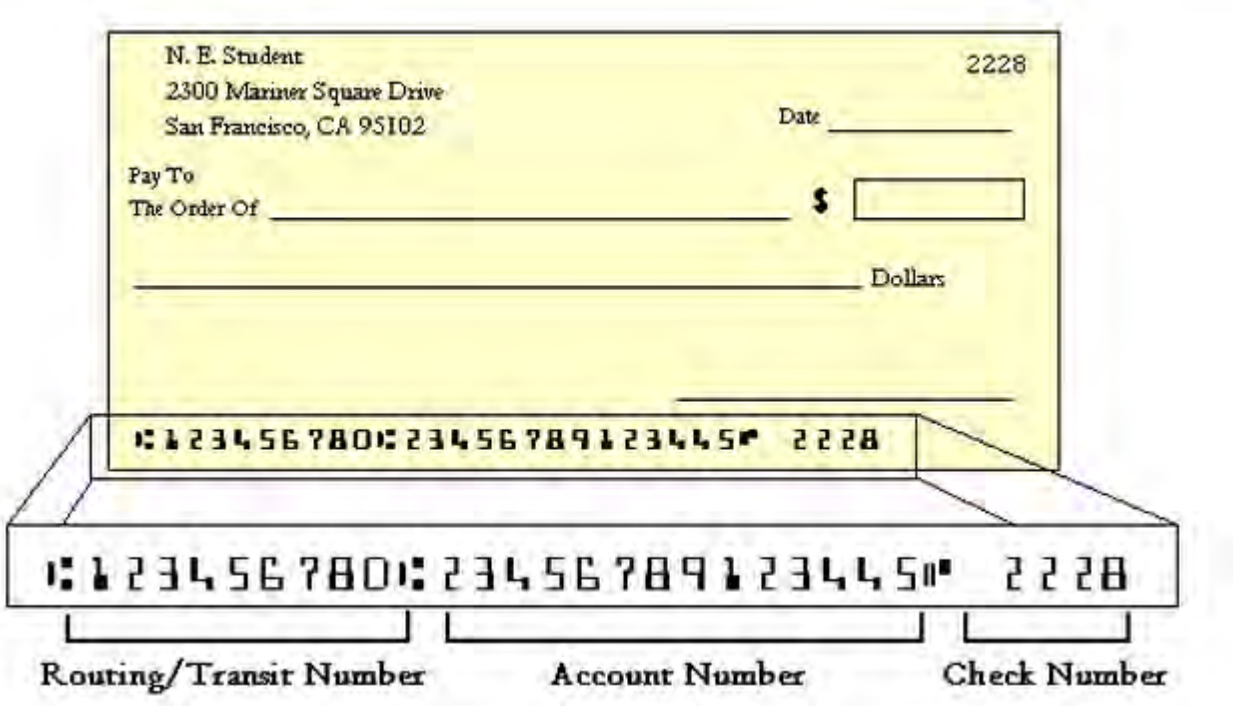


Fig: Electronic Check Format.

Merchant benefits of converting checks to an electronic form:

- Saves you time with your deposits - no more bank runs or long teller lines.
- Lowers traditional bank fees, like per item deposit and returned item fees.
- Funds you quickly, usually within 2 business days of the original transaction.
- Secures your customer's personal and bank account information by returning the original item to the check writer.
- Provides your customers complete transaction information for easy bank reconciliation, as well as providing sales information, like store name and location.
- Expandable equipment is simple and user friendly.

Impact of Electronic Checks: Electronic checks allow businesses to process payments more quickly. As a result, the money will come out of your checking account sooner than you might expect. You need to make sure you have enough

money in your account when you write a check, and you can't rely on 'float' time as much as you might have in the past. Keep a balanced checkbook and consider some type of overdraft protection plan.

Since you're paying electronically anyway, you now have even less reason to write checks the old fashioned way.

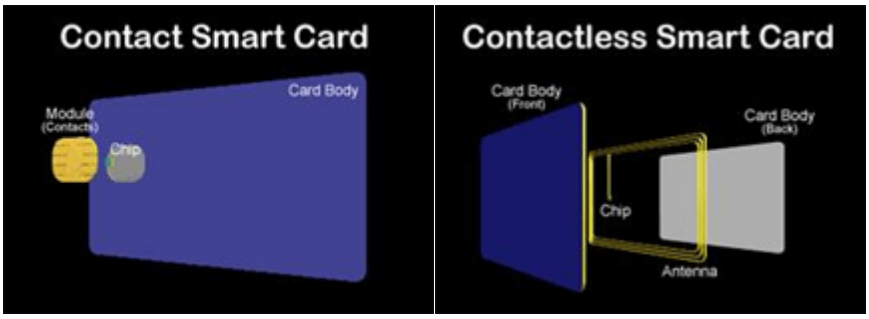
Where Electronic Check Conversion Happens? Your paper checks may be converted to electronic checks right in front of you, or it may happen when you mail a check to somebody to pay a bill. Either way, they're making an electronic check so that they can process your payment electronically.

Electronic Check Disclosure and Identification: Businesses are supposed to notify you that they're making an electronic check. If you're in a store, there should be a sign near the register that says they'll turn your paper check into an electronic check. If you're mailing in a check to pay a bill, the company probably disclosed their electronic check policy somewhere in the fine print of an agreement or on the back of your statement. If the cashier drops your check into a machine and hands it back to you when you make a purchase, they've used an electronic check.

Smart Cards

A smart card is a device that includes an embedded integrated circuit chip (ICC) that can be either a secure microcontroller or equivalent intelligence with internal memory or a memory chip alone. The card connects to a reader with direct physical contact or with a remote contactless radio frequency interface. With an embedded microcontroller, smart cards have the unique ability to store large amounts of data, carry out their own on-card functions (e.g., encryption and mutual authentication) and interact intelligently with a smart card reader.

Smart card technology is available in a variety of form factors, including plastic cards, fobs, subscriber identity modules (SIMs) used in GSM mobile phones and etc. **Smart Card Technology**: There are two general categories of smart cards: **contact** and **contactless** as shown in figure below**.**



A contact smart card must be inserted into a smart card reader with a direct connection to a conductive contact plate on the surface of the card (typically gold

plated). Transmission of commands, data, and card status takes place over these physical contact points.

A contactless card requires only close proximity to a reader. Both the reader and the card have antennae, and the two communicate using radio frequencies (RF) over this contactless link. Most contactless cards also derive power for the internal chip from this electromagnetic signal. The range is typically one-half to three inches for non-battery powered cards, ideal for applications such as building entry and payment that require a very fast card interface.

Two additional categories of cards are **dual-interface cards** and **hybrid cards**. A hybrid card has two chips, one with a contact interface and one with a contactless interface. The two chips are not interconnected. A dual-interface card has a single chip with both contact and contactless interfaces. With dual-interface cards, it is possible to access the same chip using either a contact or contactless interface with a very high level of security.

The chips used in all of these cards fall into two categories as well: microcontroller chips and memory chips. A memory chip is like a small floppy disk with optional security. Memory chips are less expensive than microcontrollers but with a corresponding decrease in data management security. Cards that use memory chips depend on the security of the card reader for processing and are ideal for situations that require low or medium security.

A microcontroller chip can add, delete, and otherwise manipulate information in its memory. A microcontroller is like a miniature computer, with an input/output port, operating system, and hard disk. Smart cards with an embedded microcontroller have the unique ability to store large amounts of data, carry out their own on-card functions (e.g., encryption and digital signatures) and interact intelligently with a smart card reader.

The selection of a particular card technology is driven by a variety of issues, including:

- Application dynamics
- Prevailing market infrastructure
- Economics of the business model
- Strategy for shared application cards

Smart cards are used in many applications worldwide, including:

- **Secure identity applications** - employee ID badges, citizen ID documents, electronic passports, driver's licenses, online authentication devices
- **Healthcare applications** - citizen health ID cards, physician ID cards, portable medical records cards

- **Payment applications** - contact and contactless credit/debit cards, transit payment cards
- **Telecommunications applications** - GSM Subscriber Identity Modules, pay telephone payment cards

Debit and Credit Cards

"A generation ago, it wasn't all that unusual to be out for dinner with friends or at the register with a cart full of groceries and realize you didn't have enough cash to cover the bill. But today, you're likely to pull out a debit or credit card and not think anything of it." It's hard now to imagine a time when those noncash options weren't available — especially if you were born in the 1970s or later. Credit cards have been around since the 1950s, and debit cards were introduced in the mid-1970s. By 2006 , there were 984 million bank issued Visa and MasterCard credit and debit cards in the United States alone.

Though the two types of cards may be used interchangeably, there are notable differences between them. Let's start with debit cards.

Debit Cards:

Debit cards are linked to your bank account so the money you spend is automatically deducted from your account. They provide a convenient alternative to cash, especially if you do a lot of shopping online. Debit cards can also help you budget. Use your card to pay your bills and day-to-day expenses and your monthly statement will provide a good snapshot of how much you spend per month and where it's going. There's another benefit as well: Unlike credit cards, your bank balance goes down with each debit card transaction, so you're less likely to overspend. (Many banks offer "overdraft protection" that allows you to exceed your balance. But you'll end up paying interest, and maybe extra fees, on the money you borrow from your overdraft account.)

With so many benefits to the debit card, why use a credit card at all? There are three main reasons: You can spend more than you have — or postpone paying, at least — and you typically get better rewards and better protection than you do with debit cards.

Credit Cards:

Credit cards basically allow you to use someone else's money (the card issuer's) to make a purchase while you pay the money back later. If you do so within the billing period — generally, 15 to 45 days — you can avoid paying any interest on it. The problem arises, of course, when you don't pay the balance in full and are charged interest as well. That can quickly add up . If it takes you two years to pay off a $500 balance, for example, and you're being charged 18 percent interest, you'll end up paying nearly $100 more in interest.

If you use them responsibly though, credit cards can offer other advantages. They help build your credit, as long as you pay your bills on time. Some also offer rewards that you can use to get gifts, cash back or discounts for products, services and special events. They also provide more protection if someone steals your card or bank information. If you notice a fraudulent charge on your credit card account, you can call the card issuer, make a dispute claim, and the charge should be removed from your balance. But if thieves steal your debit card information and use it, it may take weeks for the bank to investigate your claim and replace the lost funds. In the meantime, you may have to deal with a dwindling bank balance or bounced checks.

Federal law also protects you if you need to dispute charges on a credit card, but not if you use a debit card or other forms of payment. If you paid cash or used a debit card, the retailer already has your money. So you have a lot less leverage, and there's no guarantee you'll get that money back. But if you pay for something with your credit card and aren't happy with the purchase, your card issuer can legally withhold payment from the retailer until they resolve the dispute, and you won't be charged.

For most people, using both a debit card and credit card makes sense. The key is not to spend more than you have with either. If you can do that, you'll be able to enjoy the benefits that each provide.

Working Techniques of Credit Cards: Credit card payment processing for the e-commerce electronic payment system takes place in two phases: **authorization** (getting approval for the transaction that is stored with the order) and **settlement** (processing the sale which transfers the funds from the issuing bank to the merchant's account). The flow charts below represent the key steps in the process starting from what a customer sees when placing an order through completing the sale and finishing with the merchant processing the sale to collect funds.

Fig: Authorization Process of Credit Cards.

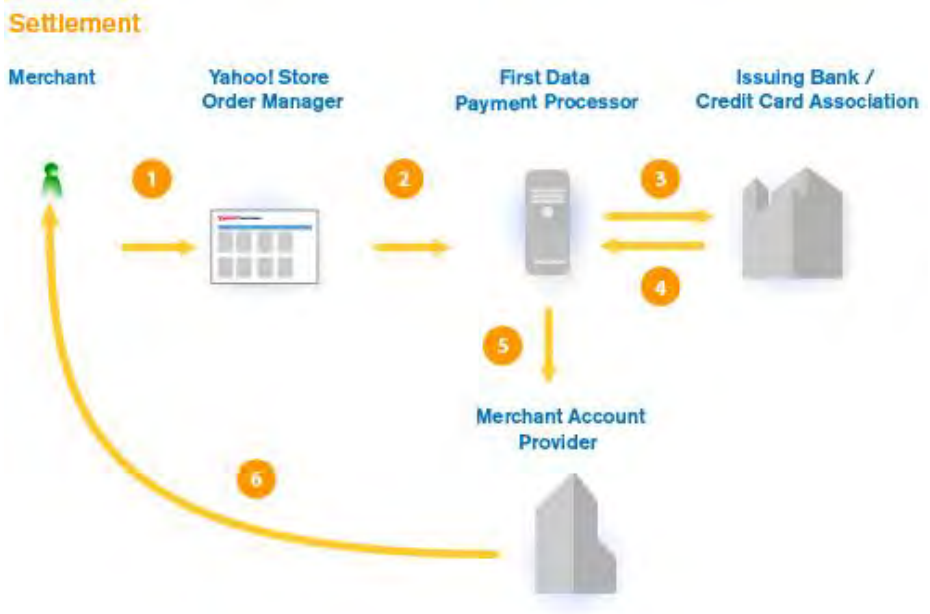


Fig: Settlement Process of Credit Cards.

Benefits and Limitations of Credit Cards:

Advantages and Disadvantages of Credit Cards are:

Advantages	**Disadvantages**
Convenience--Credit cards can save your time and trouble--no searching for an ATM or keeping cash on-hand.	**Overuse**--Revolving credit makes it easy to spend beyond your means.
Record keeping--Credit card statements can help you track your expenses. Some cards even provide year-end summaries that really help out at tax time.	**Paperwork**--You'll need to save your receipts and check them against your statement each month. This is a good way to ensure that you haven't been overcharged.
Low-cost loans--You can use revolving credit to save today (e.g., at a one-day sale), when available cash is a week away.	**High-cost fees**--Your purchase will suddenly become much more expensive if you carry a balance or miss a payment.
Instant cash--Cash advances are quick and convenient, putting cash in your hand when	**Unexpected fees**--Typically, you'll pay between 2 and 4 percent just to get the cash you need it. advance; also cash advances usually carry high interest rates.

Build positive credit--Controlled use of a credit card can help you establish credit for the first time or rebuild credit if you've had problems in the past--as long as you stay within your means and pay your bills on time.	**Deepening your debt**--Consumers are using credit more than ever before. If you charge freely, you may quickly find yourself in over your head--as your balance increases, so do your monthly minimum payments.
Purchase protection--Most credit card companies will handle disputes for you. If a merchant won't take back a defective product, check with your credit card company.	**Homework**--It's up to you to make sure you receive proper credit for incorrect or fraudulent charges.

UNIT 7: E-MARKET AND STRATEGY

Internet marketing

Internet marketing, or online marketing, refers to advertising and marketing efforts that use the Web and email to drive direct sales via electronic commerce, in addition to sales leads from Web sites or emails. Internet marketing and online advertising efforts are typically used in conjunction with traditional types of advertising like radio, television, newspapers and magazines.

> *Internet marketing is the process of building and maintaining customer relation-ships through online activities to facilitate the exchange of ideas, products, and services that satisfy the goals of both parties.*

Marketing efforts done solely over the Internet. This type of marketing uses various online advertisements to drive traffic to an advertiser's website. Banner advertisement pay per click (PPC), and targeted email lists are often methods used in Internet marketing to bring the most value to the advertiser. Internet marketing is a growing business mainly because more and more people use the internet every day. Popular search engines such as Google and Yahoo have been able to capitalize on this new wave of advertising.

Online advertising is a form of marketing and advertising which uses the Internet to deliver promotional marketing messages to consumers. It includes email marketing, search engine marketing (SEM), social media marketing, many types of display advertising (including web banner advertising), and mobile advertising.

In 2011, Internet advertising revenues in the United States surpassed those of cable television and nearly exceeded those of broadcast television. In 2013, Internet advertising revenues in the United States totaled $42.8 billion, a 17% increase over the $36.57 billion in revenues in 2012. U.S. internet ad revenue hit a historic high of $20.1 billion for the first half of 2013, up 18% over the same period in 2012. Online advertising is widely used across virtually all industry sectors.

Definition can be divided into five components:

A Process

Like a traditional-marketing program, an Internet-marketing program involves a process. The seven stages of the Internet-marketing program process are setting corporate and business-unit strategy, framing the market opportunity, formulating the marketing strategy, designing the customer experience, designing the marketing program, crafting the customer interface, and evaluating the results of the marketing program. These seven stages must be coordinated and internally

consistent. While the process can be described in a simple linear fashion, the marketing strategist often has to loop back and forth during the seven stages.

Building and Maintaining Customer Relationship

The goal of marketing is to build and create lasting customer relationships. Hence, the focal point shifts from finding customers to nurturing a sufficient number of committed, loyal customers.? Successful marketing programs move target customers through three stages of relationship building: awareness, exploration, and commitment. It is important to stress that the goal of Internet marketing is not simply building relationships with online customers. Rather, the goal is to build offline (as relevant) as well as online relationships. The Internet marketing program may well be part of a broader campaign to satisfy customers who use both online and offline services.

Online

By definition, Internet marketing deals with levers that are available in the world of the Internet. However, as noted above, the success of an Internet marketing program 'may rest with traditional, offline marketing vehicles. Consider, for example, the recruiting and job-seeking service Monster.com. Monster's success can be tied directly to the effectiveness of its television advertising and, in particular, its widely successful of the past two years.

Exchange

At the core of both online and offline marketing programs is the concept of exchange. In both the online and offline worlds, exchange is still the heart of marketing. In the new economy, firms must be very sensitive to cross-channel exchanges. That is, an online marketing program must be evaluated according to its overall exchange impact-not just the online exchange impact. Hence, online marketing may produce exchanges in retail stores. Firms must be increasingly sensitive to these cross channel effects if they are to measure the independent effects of online and offline marketing programs.

Satisfaction of Goals of both Parties

One of the authors of this book is a loyal user of the website weather.com. Each day he arises and checks the weather in his city as well as the weather in cities he will be traveling to during the week. He is clearly satisfied with and loyal to the site. To the extent that weather.com can monetize this loyalty-most likely, in the form of advertising revenue-both parties will be satisfied. However, if the firm is unable to meet its financial obligations to employees, suppliers, or shareholders, then the exchange is unbalanced. Customers are still happy, but the firm is unable to sustain its revenue model. Both parties must be satisfied for exchange to continue.

Internet marketing Tools

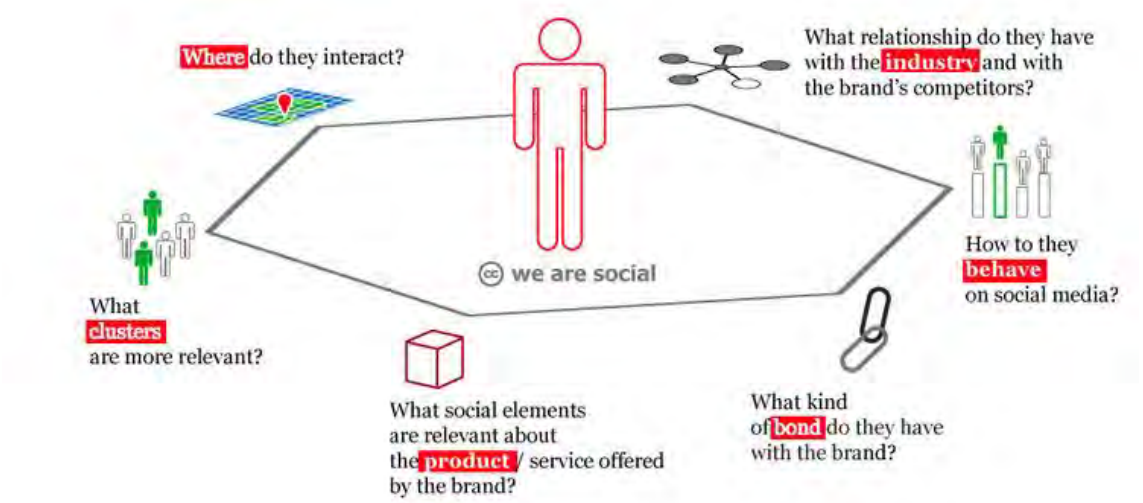
Apparently, the web can be used as a powerful internet marketing tool in a number of different ways to promote online businesses and reach target audience across the globe. There are several types of internet marketing strategies used by online marketers and many of them are simple and effective. Here is a list of some highly effective and most popular types of internet marketing techniques:

Search Engine Marketing

Search engine optimization (SEO) has become a crucial part of web commerce. Without the right use of SEO techniques and strategies, a business or a website may not be able to acquire good ranking on popular search engines, particularly Google. Due to continuous manipulation of SEO techniques in the last few years, many online directories and search engines have made several modifications in their search algorithms to provide best results to users, looking for relevant information for their query.

The main focus of search engine marketing strategies is to place certain highly searched keywords in particular places of several web pages of a website. It aims at providing relevant and useful content to your target market, while improving the overall rank of the website on search engines.

Social Media Marketing



Employment of social media marketing services is considered to be the most important and result-oriented marketing strategies for online businesses. These services give quick results and have profound effect on the overall functioning of a business. Social media marketing basically means promoting company or a website on different networking sites and popular media channels such as Twitter, LinkedIn, Facebook, Blogger etc. Promoting websites of businesses through social media marketing pricing ensure increased traffic, thereby resulting in good amount of profits.

The best thing about social media marketing is that it does not require you to make heavy investment, because making online company profiles on social networking sites is absolutely free. Having your business on social networking sites is an easy and simplest way to communicate and share your products with your target audience. .

Google AdSense Advertising

Google AdSense has grown rapidly in the past few years. It allows sites of all sizes to earn money via relevant advertising. To be specific, Google AdSense is a simple marketing strategy that allows advertisers to earn through their ads whenever a user clicks on them on visiting a website. Every website has ads related to its content. So, this gives the advertiser a wide customer base. It is a fast and simple way to advertise products on the internet and attract target audience.

E-mail Marketing

E-Mail marketing is one of the primary ways to strengthen the relationship with customer. In order to start the process, your customers should sign up for newsletters so they can be repeatedly reminded about new products, launches, and other deals being offered by the company on a regular basis. E-mail marketing encourages customer loyalty, and can offer amazing benefits to customers if they choose to become a subscriber.

Apart from these, there are many other different types of internet marketing tools you may consider as well. All of them effectively designed to attract users, increase search engine ranking, and brand building. There are some amazing options that you can find to market your business on the internet.

Depending on the nature of your business, you would need to choose particular types of internet marketing tools and techniques to produce best possible results. Irrespective of the method you choose, you can always hire professional services by neueseocanada.com to promote your business and implement efficient marketing strategies. A professional would know all the right paths to lead to you your business goals in a smooth and effective manner. A professional company will win more customers and bring your website at the top of the result page.

Benefits of internet Marketing

Data Collection

Every time a customer transacts with the company online, that transaction is captured. The firm can use this data in a number of ways. Firstly information can be analyzed to find out most popular products/services sold. Secondly the data can be used to assist in segmenting their customers, profiling them and sending customers promotional material based on past buying habits.

There has been much controversy over the amount of information that is being collected online by various companies in particular social networking sites and whether customers should be able to opt out of that information being shared to third party users.

Personalization of The Web Experience

When customers log into their accounts businesses can make their web experience almost unique. From offering special offers to that particular customer, offering add on to their recent purchase, much like Amazon.com does, or by allowing the customer to personalize their own products, like Nike does with their trainers . Personalization allows the firm to form stronger bonds online with customers and form long term online relationships ensuring customers come back regularly.

Competitor Analysis

The internet allows businesses to analyse their competitor's online strategy. A firm can keep abreast of new products that are released, react to price changes, or use the internet to discover secondary data on their competitors. The internet allows a firm to react quickly to a change in their competitors strategy, and try to provide a service that allows them to match or beat their competitors.

Cost Reduction

One of the major benefits of setting up or moving a business online is the cost advantages of doing so. A firm can save a number of costs. These include:

- **Staffing costs**: Fewer staff are needed online then in the high street thus reducing costs.
- **Premises**: The company will not need retail outlet just a centralised office and possibly warehouse space, saving on potential retail costs.
- **Disintermediation**: The channel of distribution is shorter online as the consumer has the opportunity to buy directly like with Dell. As one of the intermediaries is cut out this process is known as disintermediation.
- **Financial management**: As consumers pay for the product before it is dispatched, this improves the cash flow for the company, making sure for the firm that they can pay their suppliers and other costs on time.

Broad and Global Reach

What is more important to business owners and marketers than to get their products and services across to wide prospects base! With internet, online businesses, both medium and large-scale, are accessible to millions of online users. Your advertisement reaches global prospects through various online marketing strategies like email marketing, social media marketing, pay-per-click (PPC)

advertisement. Prospects translate to money and as such, the more reach your marketing claims, the more the prospects. When numbers of prospects skyrocket, you have opportunity for more customers and sales and you make more money which is the ultimate goal of every business.

All-Hour Based Marketing

Internet marketing is 24/7 based. Your marketing campaigns run 24 hours a day, 7 days a week. You aren't constrained with opening hours, neither are you to consider overtime payment for staff. Regional or international time variation/difference doesn't affect the availability or reachability of your online ad copy campaign and offer. Anytime an individual opens a computer connected to the internet, S/he's tendency to see your marketing campaign as opposed to usual traditional offline marketing. Customers search the products offered at their convenient time as long as they like – no hasten, no fear of closing. The users own the opening and closing hours for shopping.

Internet Marketing is Time-Effective

Internet marketing is fast and easy to start. You can set up a campaign at any time convenient for you. For instance, email marketing which is one of the best internet marketing strategies can be set up in a matter of hours. Within few minutes, you set up the auto-responder and start marketing even with a list of one subscriber.

Advertising to Target Markets

Internet marketing earns the advantages of ads targeting based on numerous factors such as gender, age, location, interest and hobbies. Advertising and marketing campaign could be targeted by filtering these demographic factors. Two or more factors can be combined to establish target market. Decision can be made to target advertising on female aged between 22-35 in the united state for a particular product or niche while elderly people can be targeted for another service.

If you want to market a retirement saving program, you might target young people(who has long saving span) while retirement planning programme might be more appropriate for older people who have worked close to the retirement age.

Targeting can be very difficult in traditional advertisement like television, radio, magazine, newspaper if at all achievable. On the web, you can create interest-based targeting, behavioural-targeting PPC in Google and other PPC advertising networks.

Limitation of Internet marketing

1. Online Marketing is not free as the cost of hardware, software, wed site design, online distribution costs, maintenance of your site and yes time, all should be factored into the cost of providing your product and service

2. Still, the internet is considered as a source of information gathering for the majority of your customers. Many people are there who still prefer the live interaction when they buy. This may deter customers from buying if you have a small business with one location
3. Over 50% of households shop online and this number is continued to grow, you are reaching less than two out of three households
4. So many scams on the internet
5. Timing of updates is critical so it's easy to have outdated information on your site
6. Is your website safe? Because of the fear of website's security, many of the visitors will not want to use their credit card to make a purchase if they don't know that your site is secure.
7. No replacement is there for good old fashioned customer service. The majority of online marketers lack inquiry response programs and customer service. Therefore, your many online visitors will already have painted your website as poor service before contacted you. Also, the majority of sites have poor navigation that makes it tough for the visitor to find what they are looking for. Many sites were created without a customer service point of view.
8. A lot of competition for your product already out there. When your visitor finds you then it means they have been checked many links already. Until and unless they can find what they are looking for quickly, they are gone.

Model for e-marketing strategy development.

The four stages are:

1. **Strategic analysis**. Continuous scanning of the micro and macro-environment of an organization are required with particular emphasis on the changing needs of customers, actions and business models of competitor and opportunities afforded by new technologies. Techniques include resource analysis, demand analysis and competitor analysis, applications portfolio analysis, SWOT analysis and competitive environment analysis.

2. **Strategic objectives**. Organisations must have a clear vision on whether digital media will complement or replace other media and their capacity for change. Clear objectives must be defined and in particular goals for the online revenue contribution should be set.

3. **Strategy definition**. We will discuss strategy definition by asking eight questions. These will be considered in next month's article:

- Decision 1. Target market strategies.

- Decision 2. Positioning and differentiation strategies.
- Decision 3. Resourcing - Internet marketing priorities – significance to organization.
- Decision 4. CRM focus and financial control
- Decision 5. Market and product development strategies.
- Decision 6. Business and revenue models including product development and pricing strategies.
- Decision 7 Organisational restructuring required.
- Decision 8. Channel structure modifications.

4. Strategy implementation

Includes devising and executing the tactics needed to achieve strategic objectives. This includes relaunching a web site, campaigns associated with promoting the site and monitoring the effectiveness of the site.

The Seven Stage Cycle Of internet Marketing

1. Setting Corporate and Business-Unit Strategy
2. Analyze the Market Opportunity
3. Formulating the Marketing Strategy
4. Designing the Customer Experience
5. Designing the Marketing Program
6. Building and Nurturing Customer Relationships
7. Evaluating the Marketing Program