

### **Motivation for Controls**

- It is very important to ensure the reliability of reports produced by an information system
- If unreliability is seen by users the entire credibility of the system is lost
- Ensuring reliability is not difficult for small systems but when a system has to handle massive data it is a challenge
- Systematic controls are thus essential when a system is designed

### **Motivation for Audits**

- Many organizations are now entirely dependent on computer based information system
- These information systems contain financial data and other critical procedures
- It is essential to protect the systems against frauds and ensure that sound accounting practices are followed
- It is necessary to trace the origin and fix responsibilities when frauds occur
- Audit methods primary purpose is to ensure this.

### **Motivation for Testing**

- Systems contain many individual subsystems
- Usually sub-systems and programs are individually tested
- However when a whole system is integrated unforeseen errors may be seen
- Thus before releasing a system the entire operational system should be tested for correctness and completeness

### **Motivation for Security**

- Systems contain sensitive data about the organization and also about persons working in the organization
- Sensitive data should be protected from spies, thieves or disgruntled employees.
- Thus access should be carefully controlled and provided only on a need to know basis
- When computers are networked corruption/erasure may take place due to viruses
- Services may be disrupted due to denial of service attacks
- Thus systems should be designed with appropriate security measures.

**Motivation for Disaster Recovery**

- Organizations depend on Information systems for their entire operations
- It is thus essential to ensure continuity of service when unforeseen situations such as disk crashes, fires, floods and such disasters take place.
- Thus it is essential to ensure quick recovery from disasters and ensure continuity of service.

**2.1 Control of Information System**

- Methods, policies and procedures
- Ensures Protection of Organization's assets
- Ensures accuracy and reliability of records and operational adherence(support) to management standards

**GENERAL CONTROLS**

- Establish framework for controlling design, security and use of computer programs
- Include software, hardware, computer operations, data security, implementation and administration controls

**APPLICATION CONTROLS**

- Unique to each computerized application
- Include input, processing, and output controls

SECURITY PROFILE 1	
User: Personnel Dept. Clerk	
Location: Division 1	
Employee Identification Codes with This Profile:	00753, 27834, 37665, 44116
Data Field Restrictions	Type of Access
All employee data for Division 1 only	Read and Update
• Medical history data	None
• Salary	None
• Pensionable earnings	None

SECURITY PROFILE 2	
User: Divisional Personnel Manager	
Location: Division 1	
Employee Identification Codes with This Profile:	27321
Data Field Restrictions	Type of Access
All employee data for Division 1 only	Read Only

PROTECTING THE DIGITAL FIRM

The **Digital Firm** is a general term for organizations that have enabled core business relationships with employees, customers, suppliers, and other external partners through **digital** networks

- **On-line transaction Processing:**

Transactions entered online are immediately processed by computer

- **Fault –tolerance computer systems:**

Contain extra hardware, software, and power supply components

- **High availability computing:**

Tools and technologies enabling system to recover from a crash

- **Disaster recovery plan**

Runs business in event of computer outage (a period when a power supply or other service is not available or when equipment is closed down)

- **Load Balancing:**

Distributes large number of requests for access among multiple servers

- **Mirroring:**

Duplicating all processes and transactions of server on backup server to prevent any interruption

- **Clustering:**

Linking two computers together so that a second computer can act as a backup to the primary computer or speed up processing

## 2.2 Audit of Information System

An information system audit, often performed by external auditors, can help organizations assess the state of their information systems controls to determine necessary changes and to help ensure the information systems' availability, confidentiality, and integrity.

- The response to the strengths and weakness identified in the IS Audit is often determined by the potential risks an organization faces. Thus major component of the IS audit is a risk assessment, which aims at determining what type of risk the organization's IS infrastructure faces, the critically of those risks to the infrastructure, and the level of risks the organization is willing to tolerate.

- Once the risk has been assessed, auditors have to evaluate the organization's internal controls. During such audits the auditor tries to gather evidence regarding effectiveness of the controls.
- However testing all controls under all possible conditions is very inefficient and often infeasible. Thus, auditors frequently rely on computer assisted auditing tools (CAAT), which is specific software to test applications and data, using Test data or Simulations.

### **Auditing Technology for Information Systems**

- A. Review of Systems Documentation
- B. Test Data
- C. Integrated-Test-Facility (ITF) Approach
- D. Parallel Simulation
- E. Audit Software
- F. Embedded Audit Routines
- G. Mapping
- H. Extended Records and Snapshots

#### **A. Review of Systems Documentation**

The auditor reviews documentation such as narrative descriptions, flowcharts, and program listings. In desk checking the auditor processes test or real data through the program logic.

#### **B. Test Data**

The auditor prepares input containing both valid and invalid data. Prior to processing the test data, the input is manually processed to determine what the output should look like. The auditor then compares the computer-processed output with the manually processed results.

#### **C. Integrated Test Facility (ITF) Approach**

A common form of an ITF is as follows:

- A dummy ITF center is created for the auditors.
- Auditors create transactions for controls they want to test.

- Working papers are created to show expected results from manually processed information.
- Auditor transactions are run with actual transactions.
- Auditors compare ITF results to working papers.

#### **D. Parallel Simulation**

- The test data and ITF methods both process test data through real programs. With parallel simulation, the auditor processes real client data on an audit program similar to some aspect of the client's program. The auditor compares the results of this processing with the results of the processing done by the client's program.

#### **E. Audit Software**

- Computer programs that permit computers to be used as auditing tools include:
  1. Generalized audit software
- Perform tasks such as selecting sample data from file, checking computations, and searching files for unusual items.
  2. P.C. Software
- Allows auditors to analyze data from notebook computers in the field.

#### **F. Embedded Audit Routines**

##### **1. In-line Code – Application program performs**

Audit data collection while it processes data for normal production purposes.

##### **2. System Control Audit**

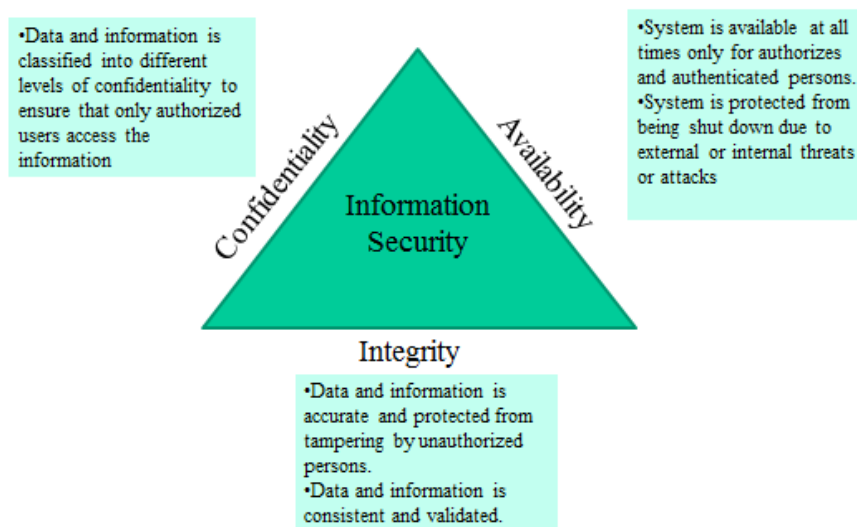
Review File (SCARF) – Edit tests for audit transaction analysis are included in program. Exceptions are written to a file for audit review.

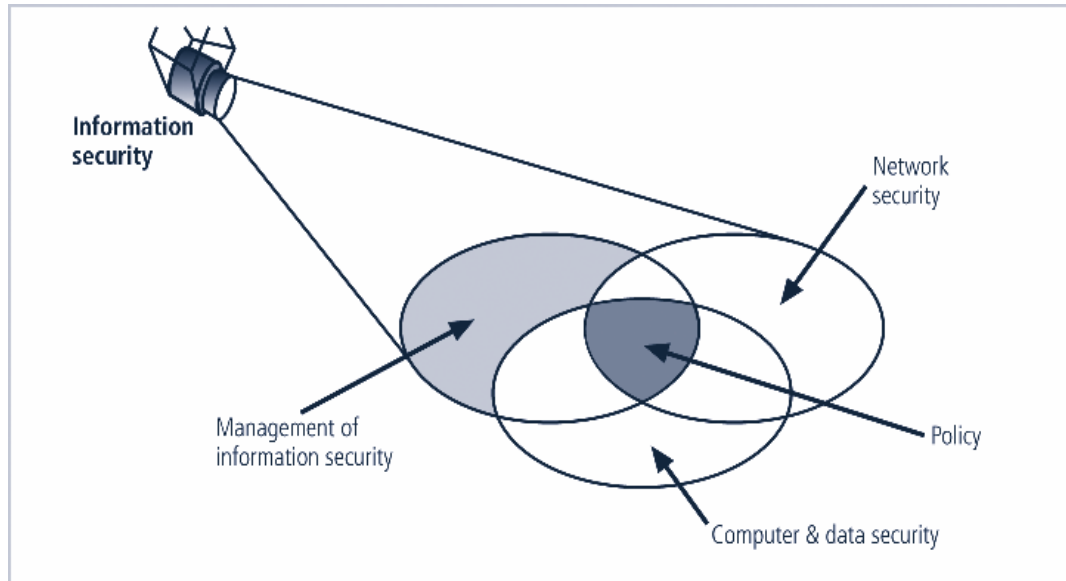
### 2.3 Security of Information System

Information System Security refers to precautions taken to keep all aspects of information system (e.g. all hardware, software, network equipment and data) safe from unauthorized use or access.

- The protection of information and its critical elements, including systems and hardware that use, store, and transmit that information
- Necessary tools: policy, awareness, training, education, technology
- C.I.A. triangle was standard based on confidentiality, integrity, and availability
- C.I.A. triangle now expanded into list of critical characteristics of information
- Confidentiality: Making sure that those who should not see information
- Integrity: Making sure that the information hasn't been changed from its original
- Availability: Making sure that the information is available for use when you need it.

#### Information Security C.I.A triangle





Components of Information Security

### Primary Threats to Information System Security

**(a) Accidents and Natural Disasters**

Power outages, inexperienced or careless computer operators

**(b) Employees and Consultants**

People within organizations who have access to electronic files.

**(c) Links to Outside Business Contacts**

Electronic information can be at risk when it travels between or among business affiliates as part of doing business

**(d) Outsiders**

Hackers and crackers who penetrate networks and computer systems to snoop or cause damage .

**(e) Unauthorized Access**

**(f) Information Modification**

**(g) Denial of Service:**

**(h) Computer Viruses/Worms**

**(i) Spyware, Spam and Cookies**

### How to Protect Data /Programs

- Regular back up of data bases everyday/or week depending on the time critically and size

- Incremental back up at shorter intervals.
- Backup copies kept in safe remote locations-particularly necessary for disaster recovery
- Duplicate systems run and all transactions mirrored if it is very critical system and cant tolerate any disruption before storing in disk
- Physical locks
- Password System
- Biometric authentication(Fig: Finger Print)
- Encrypting sensitive data /programs
- Identification of all persons who read or modify data and logging it in a file
- Training employees on data care/handling and security
- Antivirus software
- Firewall protection when connected to internet

### Layered Security

- Layered security, in its simplest form, consists of stacking security solutions, one on top of the other, to protect a computer from current, and zero day malware attacks.
- Malware: It refers to software programs designed to damage or do other unwanted actions on a computer system.  
Examples of malware include viruses, worms, Trojan horses and spyware.
- To providing adequate computer system protection.
- Gaps exist in protection capabilities in even the most sophisticated security applications.

### 2.4 Consumer Layered Security Approach

- **Backup:** Consider where you would be if your layered security strategy failed. If you've ever lost critical data to a malware infection, no doubt you already consider it of primary importance.
- Free backup utilities are readily available
  - ❖ Hard Drive Cloning is Easy with Free Ease us Disk Copy
  - ❖ Free Drive Image XML- the best way to backup data



- **Firewall** – is an application, or a hardware appliance, designed to block unauthorized access to your computer from the Internet, at the same time permitting authorized communication.
- **Anti-malware** – A front line antimalware application is absolutely critical to avoid system infection.
- **Antivirus** – An antivirus application is another critical component in a layered defense strategy to ensure that if a malicious program is detected, it will be stopped dead in its tracks!
- **Web Browser Security** – Install a free Internet Browser add-on such as WOT(Web of Trust). WOT tests web sites you are visiting for spyware, spam, viruses, browser exploits, unreliable online shops, phishing, and online scams, helping you avoid unsafe web sites.
- Extended validation (EV) SSL certificates
- Multifactor authentication (Multifactor authentication (MFA) is a security system that requires more than one method of authentication from independent categories of credentials to verify the user's identity for a login or other transaction.)
- Single Sign-on (SSO) (Single sign-on (SSO) is a session/user authentication process that permits a user to enter one name and password in order to access multiple applications.)
- Fraud detection and risk based authentication
- Transaction signing and encryption
- Secure Web and e-mail
- Open fraud intelligence network

### 2.5 Enterprise Layered Security Strategy

- A modern enterprise security strategy uses a layered identity approach as the underpinning of its security. All enterprise systems, applications, information systems, facilities, buildings and rooms are assigned as enterprise risk.
- As the user digitally or physically approaches higher risk applications or a physical location the stronger authentication is used.
- As consider the enterprise firewall and the use of Id and passwords for login.

- This could take the form of digital certificates, security tokens, smart cards and biometrics. It could also take the form of transactional security.
- While the user may successfully use their Id and password, the transaction security software would examine the IP address that the user is coming in from, their geographic position, the time of day, the type of physical computer the user is using and their behavioral pattern.
- If any of these differ from the past, then system alarm bells may start ringing resulting in the user being asked more personal questions, the action being stopped.
- Workstation application whitelisting(Application whitelisting is a computer administration practice used to prevent unauthorized programs from running)
- Workstation system restore solution
- Workstation and network authentication
- File ,disk and removable media encryption
- Remote access authentication
- Network folder encryption
- Secure boundary and end-to-end messaging
- Content control and policy-based encryption
- Practice of combining multiple mitigation security controls to protect resources and data also known as layered defense.

## **2.6 Extended Validation(EV) and SSL Certificate**

EV Certificates provide a higher level of validation and are available to all business and government entities, but are not available to individuals. The EV process is more rigorous and detailed than for any other Certificate and will require additional steps, which may include obtaining signatures from several people within the applying company, legal verification of the business's existence, etc.

An extended validation (EV) certificate is a data security/anti-fraud measure recommended in 2006 by the Certificate Authority/Browser Forum (CAB Forum): an open voluntary association of certification authorities and software developers.

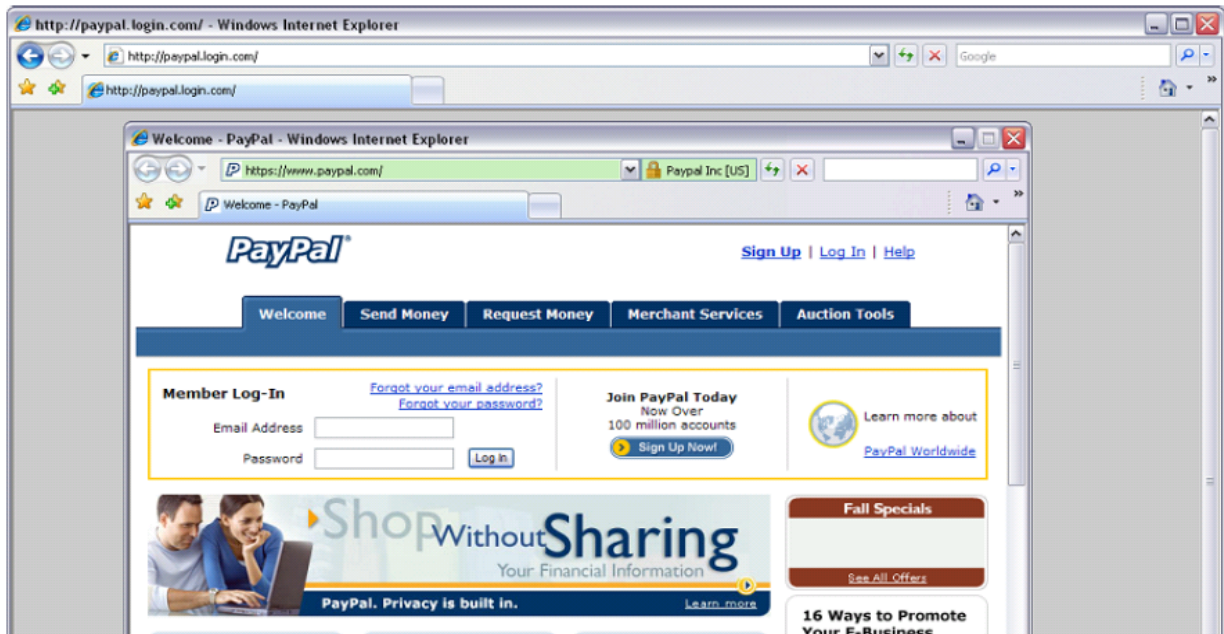
The first version of the *Extended Validation SSL Certificate Guidelines* was ratified in June 2007.

- The forum has recommended the introduction of a new security measure primarily to combat phishing: websites that mimic legitimate websites to harvest personal information including credit card numbers and bank account access details.
- The EV identity verification process requires the applicant to prove exclusive rights to use a domain, confirm its legal, operational and physical existence, and prove the entity has authorized the assurance of the Certificate.
- EV Certificates provide a higher level of validation and are available to all business and government entities, but are not available to individuals.
- The EV process is more rigorous and detailed than for any other Certificate and will require additional steps, which may include obtaining signatures from several people within the applying company, legal verification of the business's existence, etc.

**(a) Primary Purposes The primary purposes of an EV Certificate are to:**

- To identify the legal entity that controls a website which provide a reasonable assurance to the user of an Internet browser that the website which the user is accessing is controlled by a specific legal entity identified in the EV Certificate by name, address of Place of Business, and Registration Number.
- To enable encrypted communications with a website which facilitate the exchange of encryption keys in order to enable the encrypted communication of information over the Internet between the user of an Internet browser and a website.

**Designed for Banks and Large E-commerce sites**

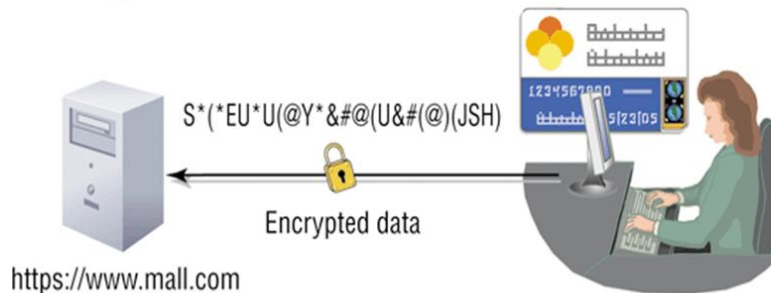


### Secure Sockets Layer (SSL)

- Digital certificates combined allows for encrypted communications to occur between Web browser and Web server

#### FIGURE • Secure Sockets Layer (SSL)

SSL encrypts data sent over the Web and verifies the identity of the Web server.



- SSL (Secure Sockets Layer) is the transaction security protocol used by websites to protect online communications.
- The most common use of SSL is to provide protection for confidential data, such as personal details or credit card information, entered into a website.

- Ecommerce security cannot be an after-thought in your business plans. Today's online shoppers look for the visual cues provided by SSL Certificates, such as the closed padlock and the “https”.

### Extended Validation SSL Certificate

- **Show your customers that your site is secure.** Our Extended Validation SSL Certificate features our instant verification green address bar, so your customers can easily see that they're protected. Provide your customers with the highest level of online assurance.
- **When customers see their address bar change to green, they know they can trust your business.** That's because the inspection process for an Extended Validation SSL is more extensive than for any other type of security certificate, verifying your organization's identity, the validity of your request and the overall legitimacy of your business.
- **How can I recognize websites using EV SSL Certificates?**

A website using EV SSL Certificate will activate highly visible indicators directly on the browser address bar:

- The green address bar, https:// and the padlock icon
- The name of the Organization that owns the website and the name of the Certification Authority that issued the EV SSL Certificate.

### Websites using EV SSL Certificates



### 2.7 Remote access Authentication

- Remote access authentication is the process whereby computer users can securely communicate with a network. A shared theme to all of these methods is the use of a digital certificate that contains information that identifies the user to a server and provides their credentials. Remote access authentication protocols make it safer to conduct business online as well as use ATMs.

#### **RADIUS**

- Most modern wireless networks do user authentication using Remote Authentication Dial-In User Service (RADIUS) protocol. RADIUS handles the overall authentication process of the user's session on the wireless device as well as also handling the authorization and auditing. The RADIUS system takes the (EAP) Extensible Authentication Protocol Authentication Method, challenges the user with the appropriate authentication method, receives the authentication response and then verifies it.
- If the authentication is successful, the RADIUS server will then authorize IP addresses, the tunneling protocol used to create virtual private networks. Further, the RADIUS server keeps tracks of when a user session begins and ends. For senior executives, who do require quite open access to the applications and information systems via their wireless device .
- Issue them with something like a secureID from (Rivest-Shamir-Adleman)RSA one time password generator and have the executives be required to enter this in order to authenticate their wireless device to the network. RSA algorithm

### 2.8. Content Control and Policy Based Encryption

- The Policy Based Encryption gateway automatically encrypts specific emails based on company-defined policies – that is, a set of rules designed to analyze all email, and encrypt any email that matches the pre-defined conditions.
- The concept of policy-based encryption is a promising paradigm for trust establishment and authorization in large-scale open environments like the Internet and Mobile Networks. On policy-based encryption which allow to encrypt a message according to a policy so that only entities fulfilling the policy are able to decrypt the message.
- More generally, policy-based encryption belongs to an emerging family of encryption schemes sharing the ability to integrate encryption with access control structures.
- A policy-based encryption scheme has to fulfill two primary requirements: on one hand, provable security under well-defined attack models.

- On the other hand, efficiency, especially when dealing with the conjunctions and disjunctions of credential-based conditions.
- It's a service that encrypts specific emails based on policy
  - Set of rules designed to analyze all email
- PBE uses the Email Content Control rules to identify which email needs to be encrypted
- The PBE Service is managed through the same control panel that you use to manage your Anti-Virus
- PBE Service is closely integrated with the Email Content Control Service

**Policy Based Encryption (PBE) Benefits**

1. Atomically applies email encryption based on the organization's email security policies
2. Data loss prevention AND email messages security policies are consistently and accurately applied.
3. Eliminates email encryption key management, backup and administration burdens
  - uses software-as-a service(SaaS)infrastructure

**Content Control Encryption**

- Services for the security of email content in an organization
- Email content like:
  - Credit card no, account information, etc.
  - Organization vital information, customer vital information

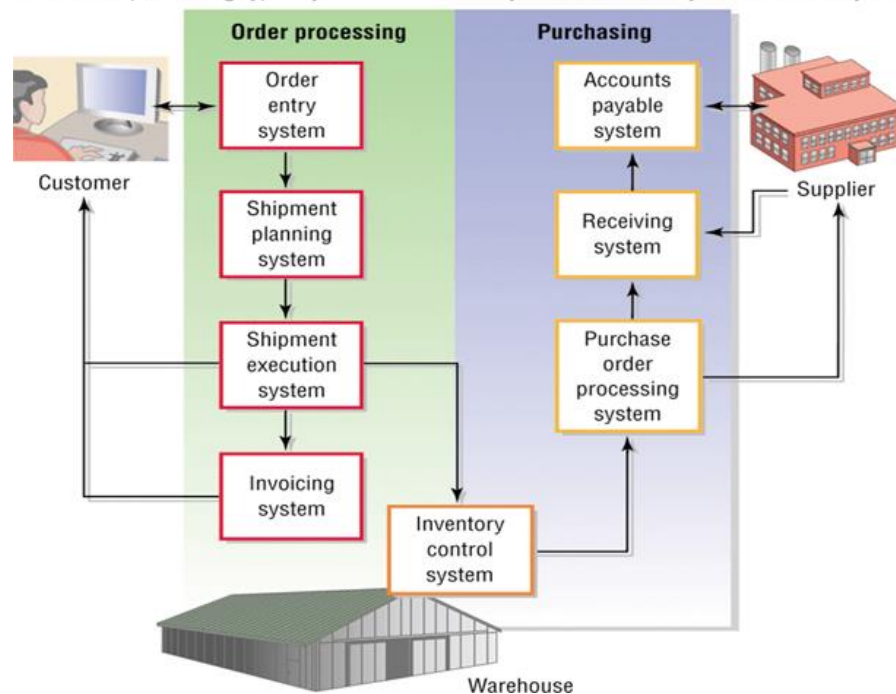
**2.9 Example of Security in E-Commerce Transaction**


- Electronic commerce
  - Systems that support electronically executed business transactions
  - The fundamental purpose of e-commerce is to execute online transactions
- E-commerce is not new; however, recent rapid development of the Internet is surely responsible for the popularity of e-commerce.
- The new way of commerce through the Internet creates vast opportunities, but at the same time, it poses challenges.
- Business-to-consumer e-commerce (B2C)
  - Connects individual consumers with sellers , cutting out the middleman
  - E.g. Amazon.com
- Business-to-business e-commerce (B2B)



- Supports business transactions on across private networks, the Internet, and the Web
- Consumer-to-consumer e-commerce (C2C)
  - Connects individual sellers with people shopping for used items
  - E.g. ebay.com

Transaction processing typically makes use of many interconnected systems and subsystems






### Secure credit card payment

This is a secure 128-bit SSL encrypted payment.


**\* Credit card number**  
The 16 digits on the front of your credit card.



**\* Expiration date**  
The date your credit card expires. Find this on the front of your credit card.

 /

**\* Security code (or "CVC" or "CVV")**  
The last 3 digits displayed on the back of your credit card.



**What happens now?**  
This is step 1 of 2. On the next page you can review your cart and product information. We will not bill you until you confirm the order on the next page.

[Next step »](#)