Chapter -2

Control, Audit and Security of Information system

Information System *(CT 751)* **BCT IV/II**

By: Shayak Raj Giri

Outline

Control, Audit and Security of Information system

- Control of information system
- Audit of information system
- Security of information system
- Consumer layered security strategy
- Enterprise layered security strategy
- Extended validation and SSL certificate
- Remote access authentication
- Content control and policy based encryption
- Example of security in e-Commerce transaction

Introduction

- **Security:**
  - Policies, procedures and technical measures used to prevent unauthorized access, alteration, theft, or physical damage to information systems
- **Controls:**
  - Methods, policies, and organizational procedures that ensure safety of organization's assets; accuracy and reliability of its accounting records; and operational adherence to management standards
- **Audit**
  - Determines if existing security measures and controls are effective

Learning Goals

- Why controls are necessary in Information systems
- Methods of controlling Information systems
- How controls are introduced in Information systems
- Why Information systems need auditing
- How are systems audited
- The methods used to test Information systems
- How the security of an Information system is ensured

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.
- Information systems handle massive amounts of data – accidents such as not including some data can cause serious damage.
- Incorrect data entry can lead to high monetary losses.
- Credibility in the information system may be lost if errors are found in operational systems.

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 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.

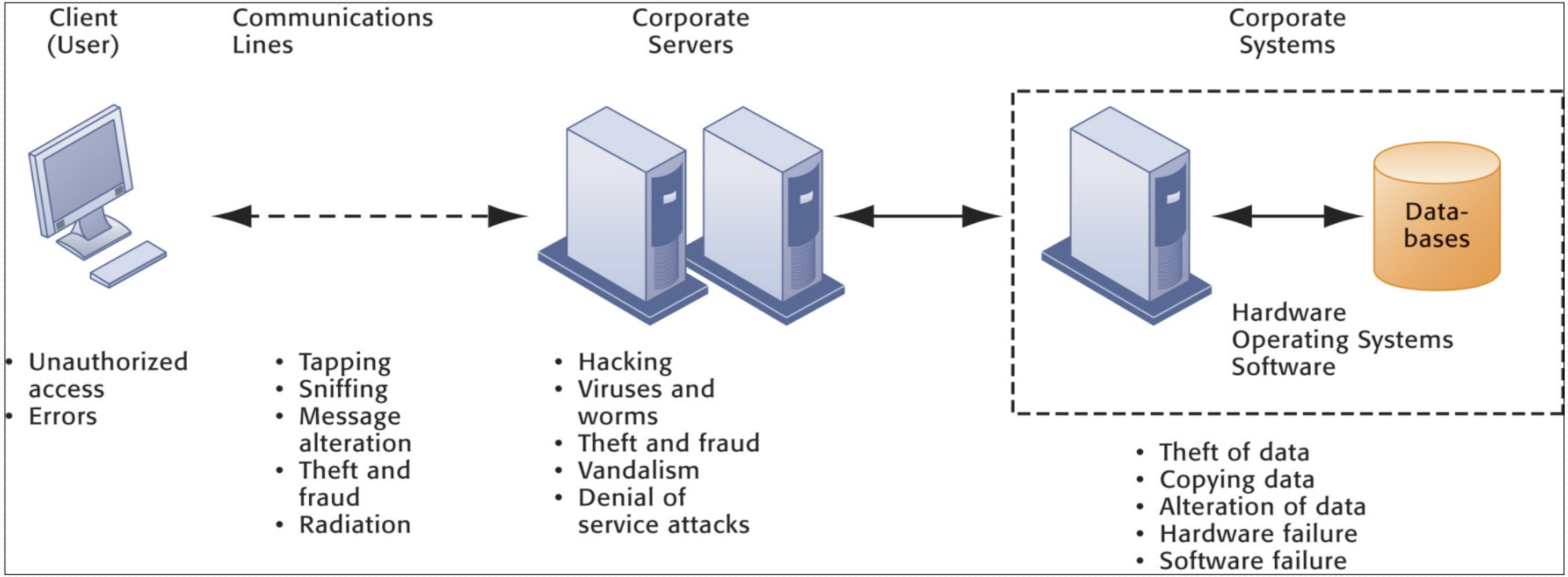
Motivation For Disaster Recovery

- 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.

Why systems are vulnerable

- **Hardware problems**
  - Breakdowns, configuration errors, damage from improper use or crime
- **Software problems**
  - Programming errors, installation errors, unauthorized changes
- **Disasters**
  - Power failures, flood, fires, etc.
- **Use of networks and computers outside of firm's control -** When data are available over a network, there are even more vulnerabilities
  - E.g., with domestic or offshore outsourcing vendors

Contemporary Security Challenges and Vulnerabilities



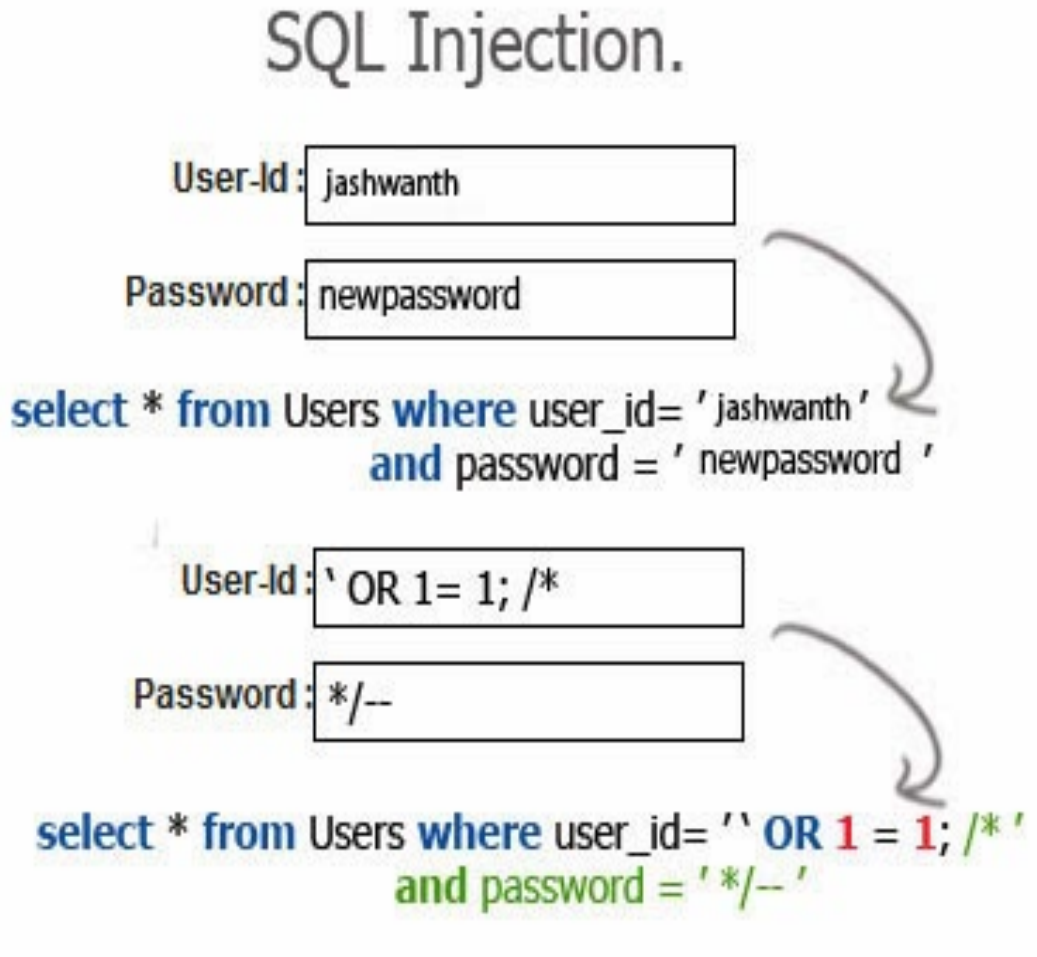
The architecture of a Web-based application typically includes a Web client, a server, and corporate information systems linked to databases. Each of these components presents security challenges and vulnerabilities. Floods, fires, power failures, and other electrical problems can cause disruptions at any point in the network.

System Vulnerability and Abuse

- **Internet vulnerabilities -** Internet is so huge that when abuses do occur, they can have an enormously widespread impact. And when the Internet becomes part of the corporate network, the organization's information systems are even more vulnerable to actions from outsiders.
  - **Network open to anyone**
  - **Size of Internet means abuses can have wide impact**
  - **Use of fixed Internet addresses with permanent connections to Internet eases identification by hackers**
  - **E-mail attachments**
  - **E-mail used for transmitting trade secrets**
  - **IM messages lack security, can be easily intercepted**

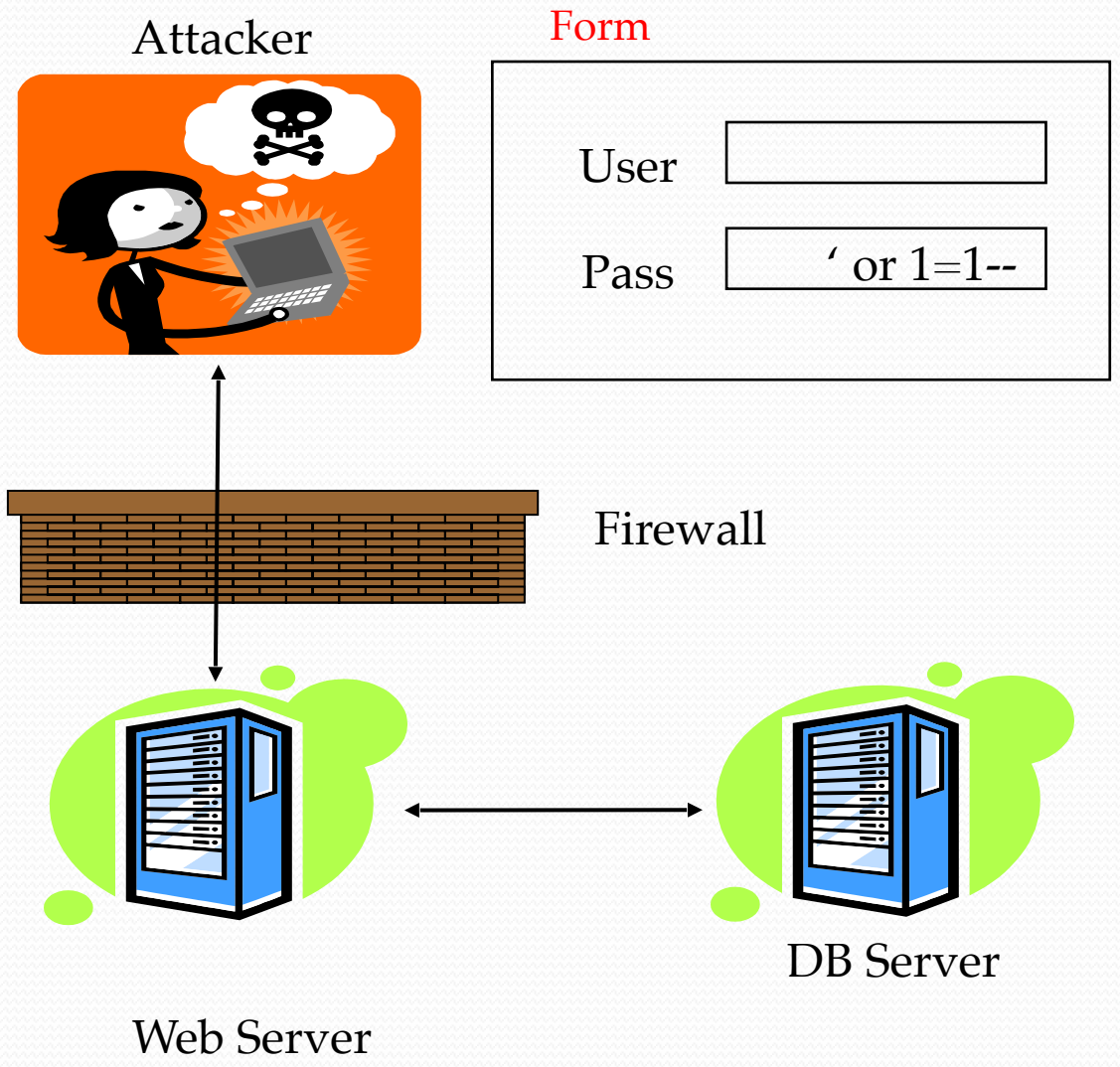
What is a SQL Injection Attack?

- Many web applications take user input from a form.
- Often this user input is used literally in the construction of a SQL query submitted to a database.
- A SQL injection attack involves placing SQL statements in the user input.
- In order to run malicious SQL queries agains a database server, an attacker must first find an input within the web application that is included inside of an SQL query.



SQL Injection

1. App sends form to user.
2. Attacker submits form with SQL exploit data.
3. Application builds string with exploit data.
4. Application sends SQL query to DB.
5. DB executes query, including exploit, sends data back to application.
6. Application returns data to user.



System Vulnerability and Abuse

- **What is Malware?**
- The word Malware is short for *malicious software*, and is a general term used to describe all of the viruses, worms, spyware etc.
- **Worms:**
- Worm does not harm or corrupt any files but still they are much dangerous then virus. They spread rapidly and their replicating nature create unnecessary spaces, files, shortcuts etc; consumes hard drive , thus, slowing down the machine.
- **Virus**
- Viruses also have the ability to replicate themselves, but they do damage files on the computer they attack.

System Vulnerability and Abuse

- **Trojan**
- Trojans are not like viruses or worms, and they are not meant to damage or delete files on your system. Their principal task is to provide to a backdoor gateway for malicious programs or malevolent users to enter your system and steal your valuable data without your knowledge and permission.
- **Adware**
- Adware are used to display advertisements on your computer's desktop or inside individual programs. They generally come attached with free-to-use software.
- **Spyware**
- Spyware programs also come attached with freeware. They track your browsing habits and other personal details and send it to a remote user. They can also facilitate installation of unwanted software from the internet.

System Vulnerability and Abuse

- **Spam**
- You get very irritated when you receive unwanted emails from unknown senders; these are called spams or junk emails. And the process of flooding the internet with the same message is called Spamming, done for the purpose of commercial advertising.
- **Ransomware**
- Ransomware is a type of malware that can alter the normal operation of your machine. It encrypts the data and prevents you from using your computer partially or wholly. Ransomware programs also display warning messages asking for money to get your device back to normal working condition.
- **Hackers , Attacks and Computer Crime**

Establishing a Framework for Security and Control

Information systems controls

- **General controls**
- Controls are methods, policies, and organizational procedures that ensure safety of organization's assets; accuracy and reliability of its accounting records; and operational adherence to management standards. There are two main types of controls, **general controls and application controls.**
  - **Types of general controls**
    - Software controls
    - Hardware controls
    - Computer operations controls
    - Data security controls
    - Implementation controls
    - Administrative controls

Application controls

- Specific controls unique to each computerized application, such as payroll or order processing.
- Include both automated and manual procedures.
- Ensure that only authorized data are completely and accurately processed by that application.
- **Types of application controls:**
  - **Input controls -** input authorization, data conversion, data editing, and error handling
  - **Processing controls -** establish that data are complete and accurate during updating
  - **Output controls -** ensure that the results of computer processing are accurate, complete, and properly distributed

The Role of Auditing

- **MIS audit -** determines if existing security measures and controls are effective
  - Examines firm's overall security environment as well as controls governing individual information systems.
  - Reviews technologies, procedures, documentation, training, and personnel .
  - May even simulate disaster to test response of technology, IS staff, other employees.
  - Lists and ranks all control weaknesses and estimates probability of their occurrence.
  - Assesses financial and organizational impact of each threat.

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

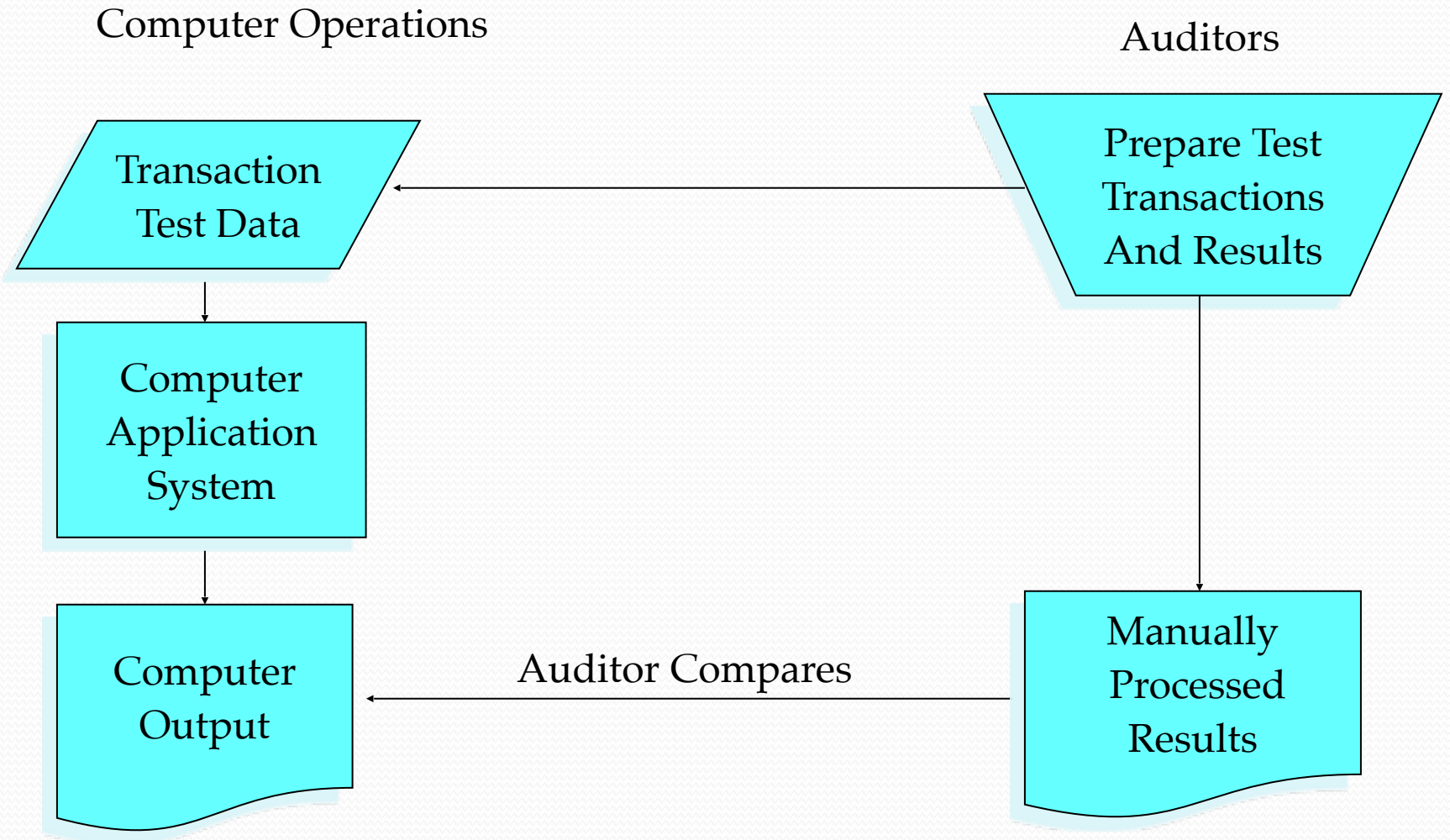
A. Review of Systems Documentation

- The auditor reviews documentation such as narrative descriptions, flowcharts, and program listings.

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.

Illustration of Test Data Approach

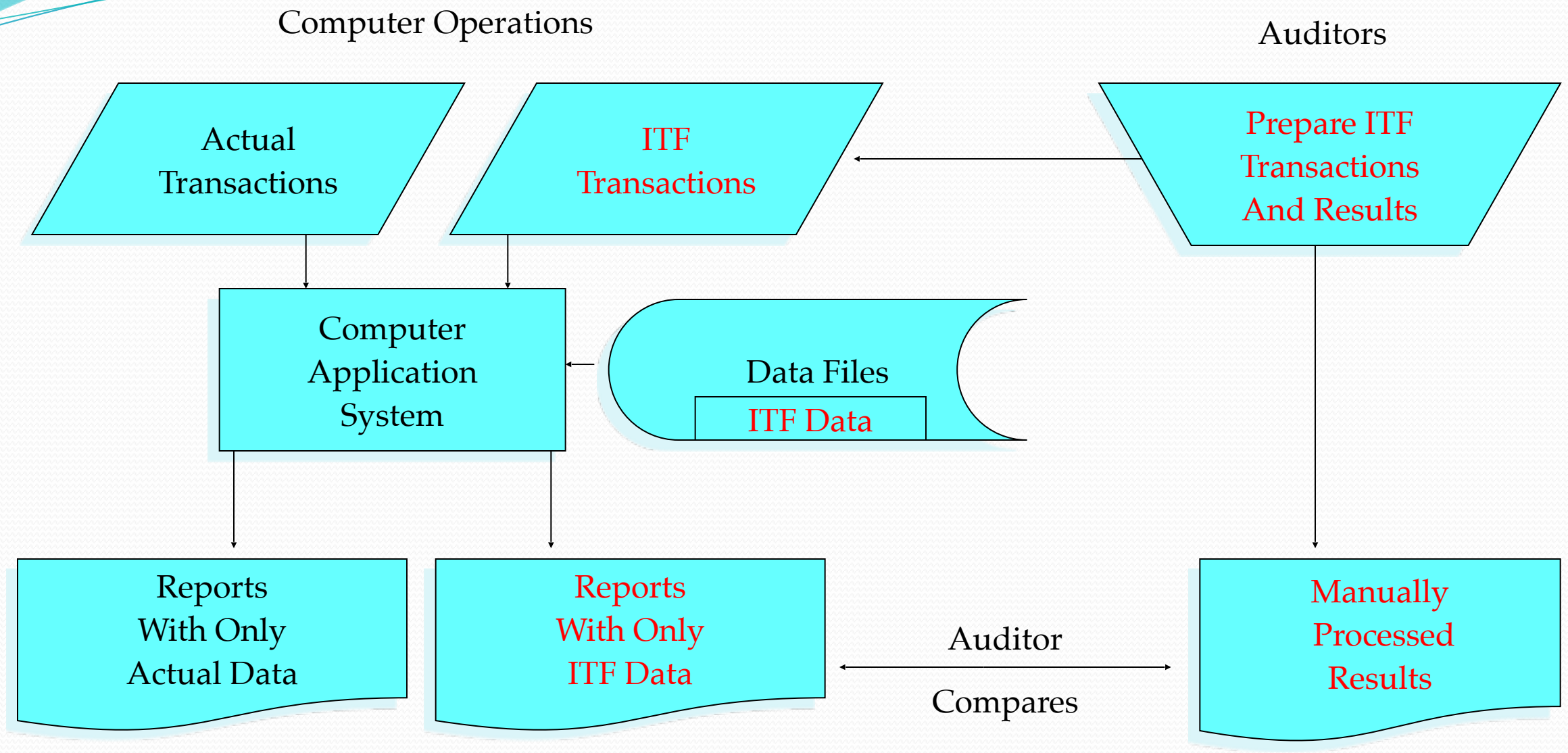


C. Integrated Test Facility (ITF) Approach

A common form of an ITF is as follows:

1. A dummy ITF center is created for the auditors.
2. Auditors create transactions for controls they want to test.
3. Working papers are created to show expected results from manually processed information.
4. Auditor transactions are run with actual transactions.
5. Auditors compare ITF results to working papers.

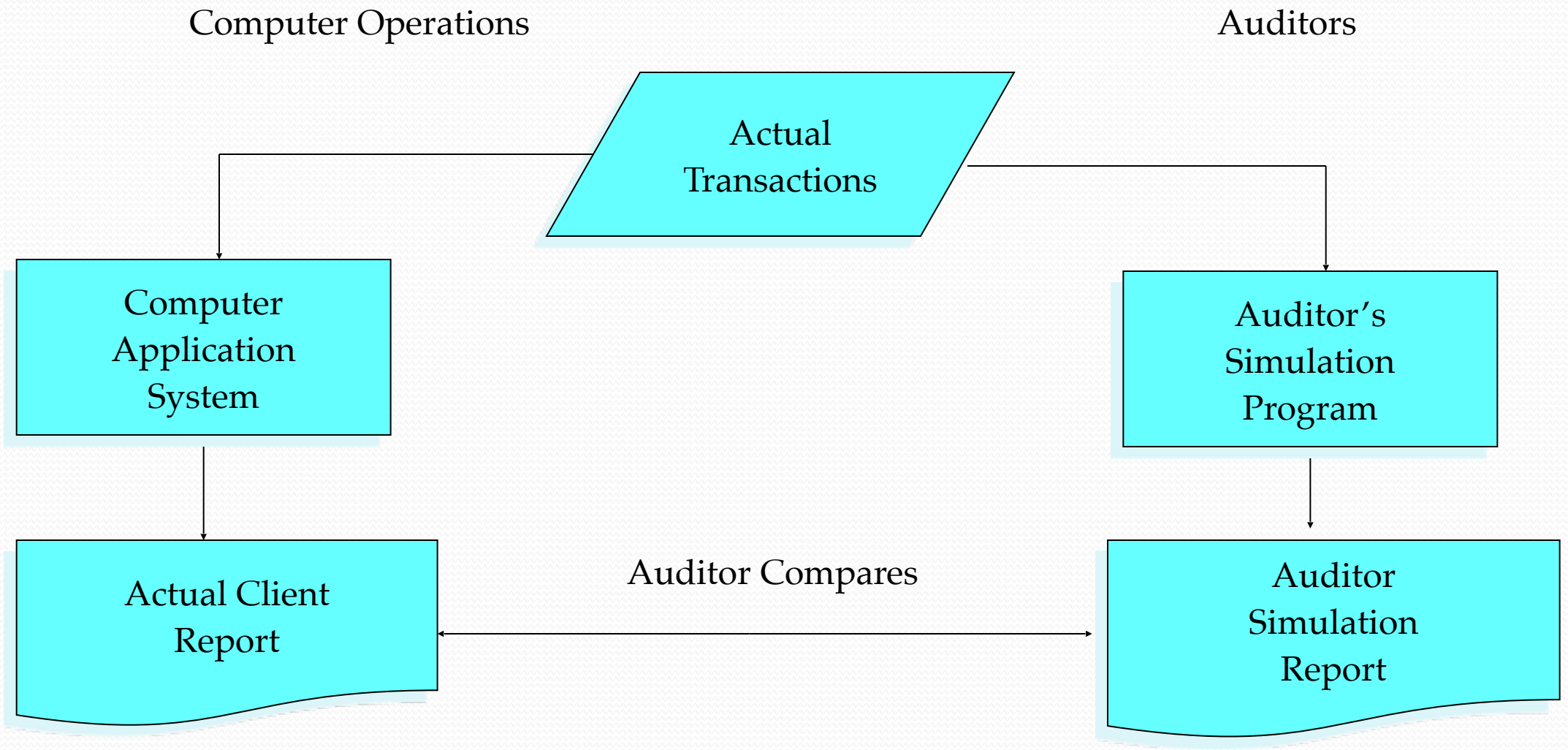
Illustration of ITF Approach



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.

Illustration of Parallel Simulation



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.

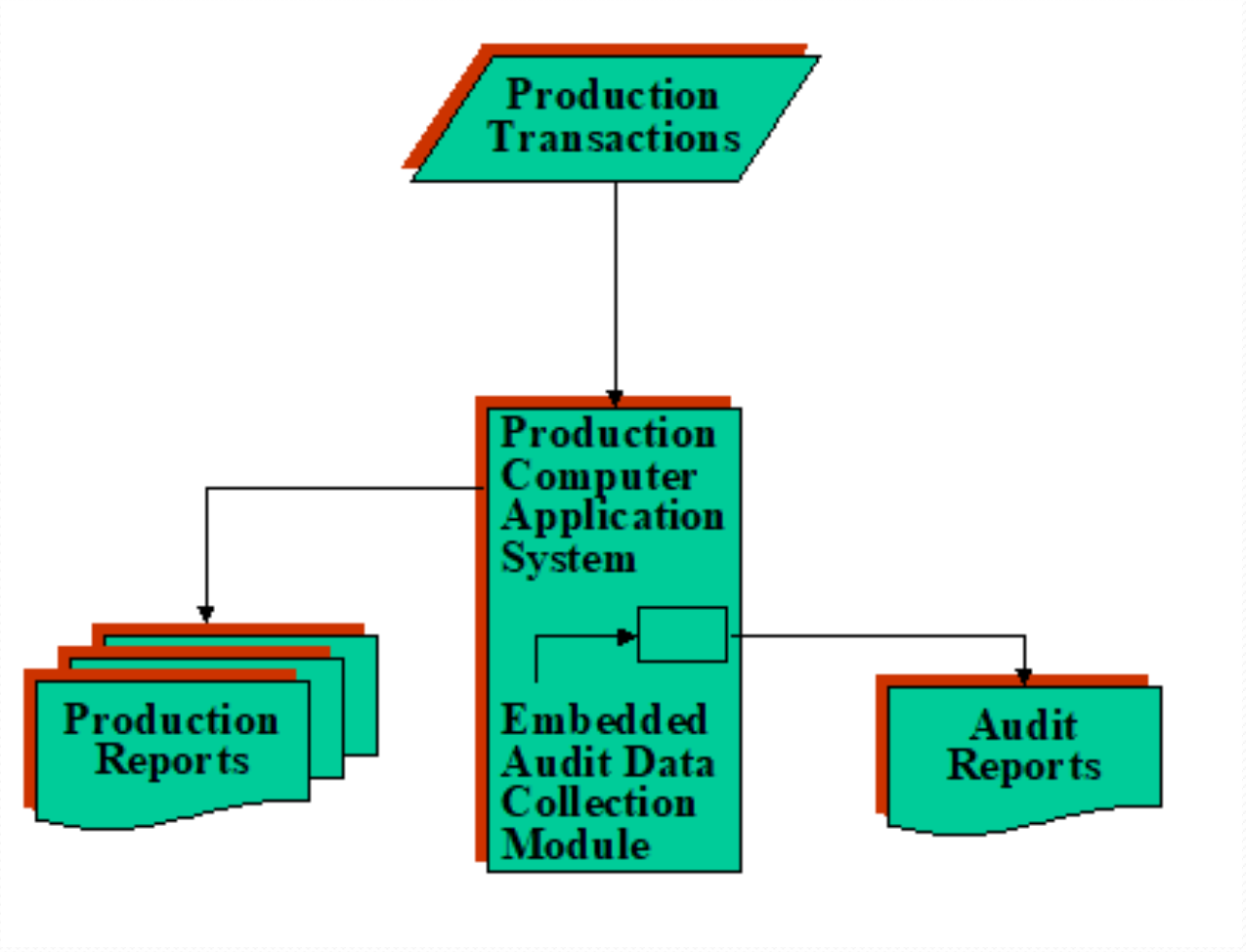
2. P.C. Software

   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.

Embedded audit routine



What is Security?

- "The quality or state of being secure—to be free from danger"
- A successful organization should have multiple layers of security in place: [**Types of Security**]
  - Physical security
  - Personal security
  - Operations security
  - Communications security
  - Network security
  - Information security

Types of Security

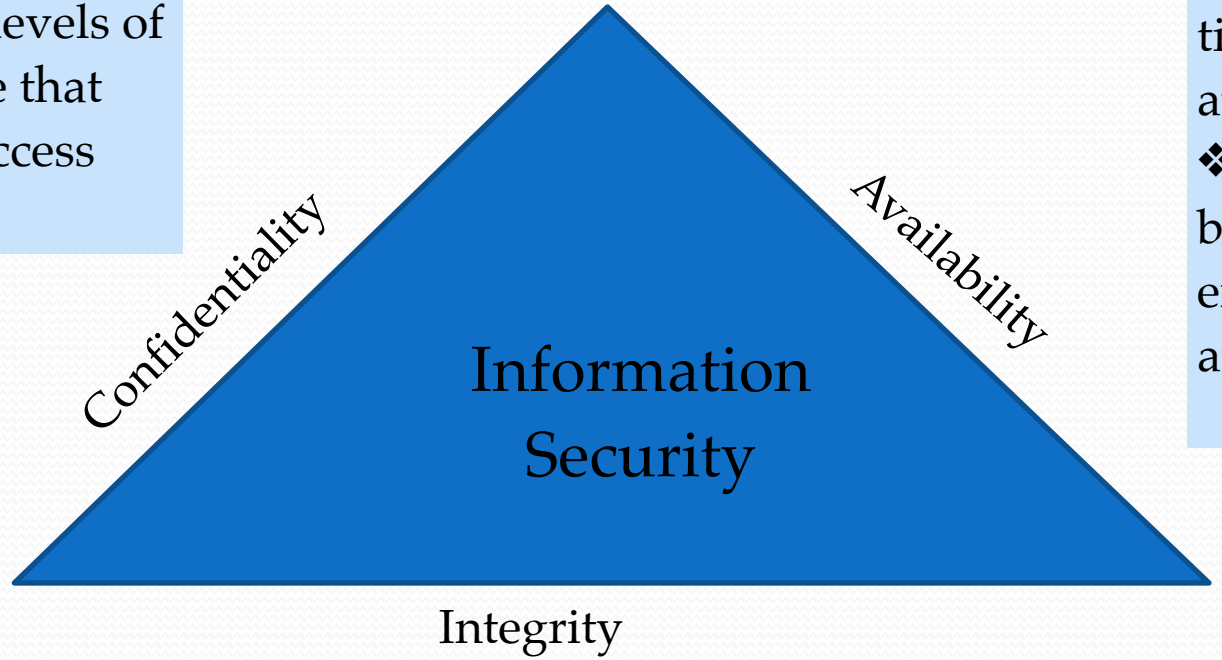
- Physical Security: To Protect physical items, object or areas.
- Personal Security: To protect the individual or group of individuals who are authorized.
- Operation Security: To protect the details of a particular operation or activities.
- Communication Security: To protect communication media, technology and content.
- Network Security: To protect networking components, connections and contents.
- Information Security: To protect information assets.

What is Information Security?

- 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.

Information Security C.I.A triangle [Security Goal]

❖Data and information is classified into different levels of confidentiality to ensure that only authorized users access the information.



❖System is available at all times only for authorized and authenticated persons.
❖System is protected from being shut down due to external or internal threats or attacks

❖Data and information is accurate and protected from tampering by unauthorized persons.
❖Data and information is consistent and validated.

Confidentiality

- Confidentiality, keeping information secret from unauthorized access, is probably the most common aspect of information security: we need to protect confidential information. An organization needs to guard against those malicious actions that endanger the confidentiality of its information.

Integrity

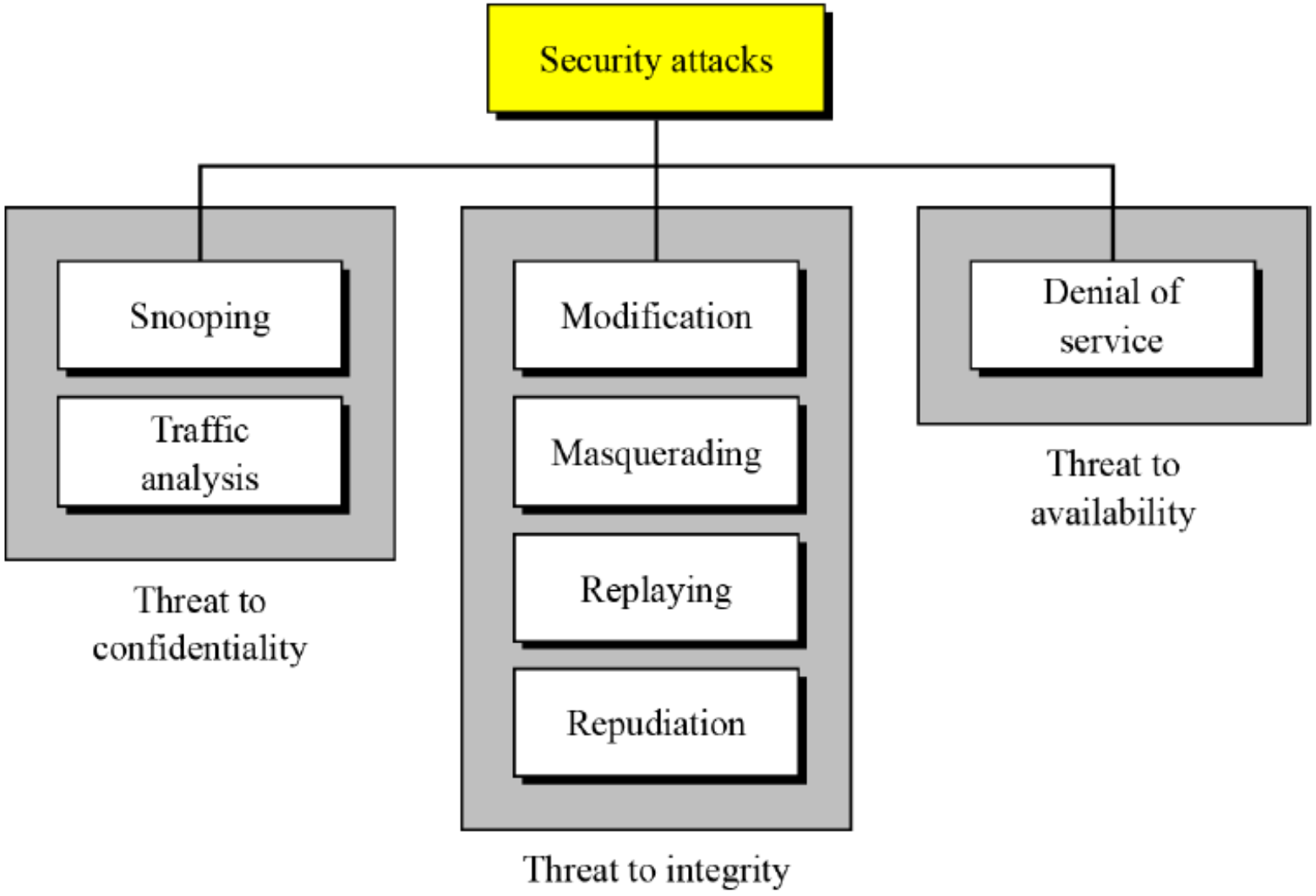
Information needs to be changed constantly. In a bank, when a customer deposits or withdraws money, the balance of their account needs to be changed. Integrity means that changes should be done only by authorized users and through authorized mechanisms.

Availability

- The information created and stored by an organization needs to be available to authorized users and applications.
- Information is useless if it is not available.
- Information needs to be changed constantly, which means that it must be accessible to those authorized to access it.
- Unavailability of information is just as harmful to an organization as a lack of confidentiality or integrity.
- Imagine what would happen to a bank if the customers could not access their accounts for transactions.

Security Attacks

The three goals of security can be threatened by security attacks.



Attacks threatening confidentiality

- In general, two types of attack threaten the confidentiality of information: snooping and traffic analysis. Snooping refers to unauthorized access to or interception of data. Traffic analysis refers other types of information collected by an intruder by monitoring online traffic.

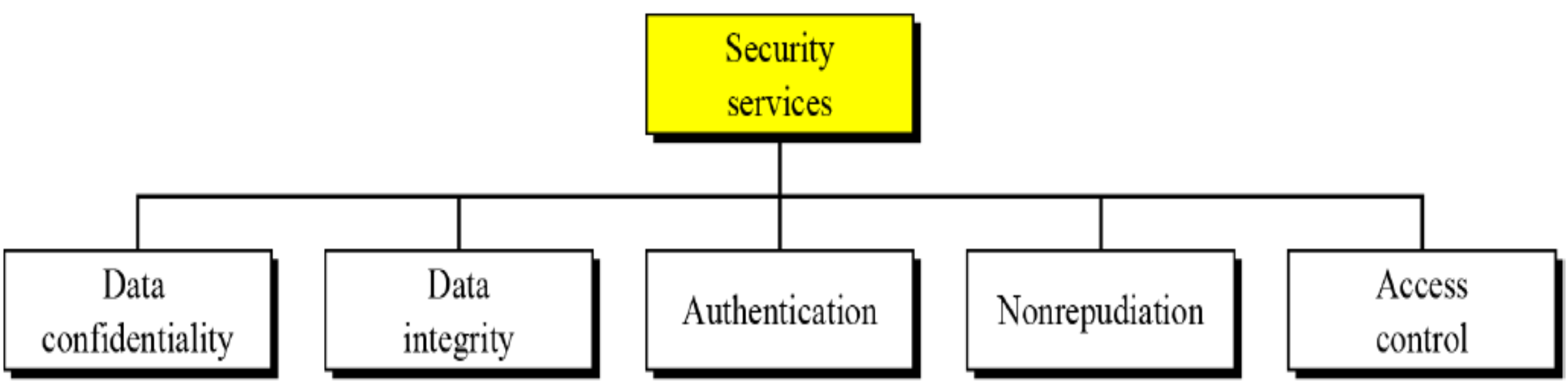
Attacks threatening integrity

- The integrity of data can be threatened by several kinds of attack: modification, masquerading, relaying and repudiation.

Attacks threatening availability

- Denial of service (DoS) attacks may slow down or totally interrupt the service of a system.
- The attacker can use several strategies to achieve this.
- They might make the system so busy that it collapses, or they might intercept messages sent in one direction and make the sending system believe that one of the parties involved in the communication or message has lost the message and that it should be resent.

Security Services



Standards have been defined for security services to achieve security goals and prevent security attacks.

Techniques

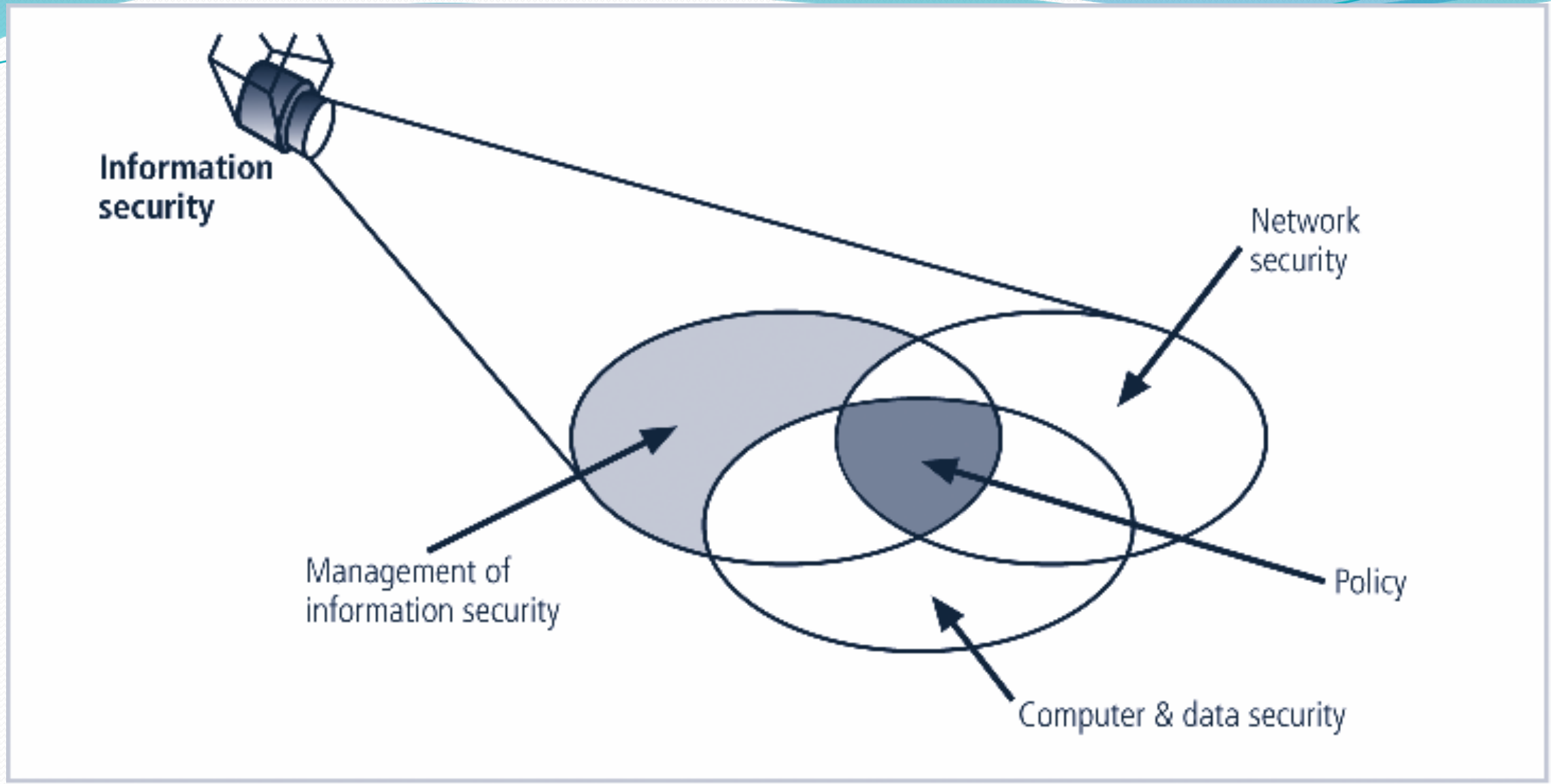
- The actual implementation of security goals needs some help from mathematics.
- Two techniques are prevalent today: one is very general—*cryptography and one is specific— steganography.*

- **Cryptography**
- Some security services can be implemented using cryptography. Cryptography, a word with Greek origins, means “secret writing”.

- **Steganography**
- The word steganography, with its origin in Greek, means “covered writing”, in contrast to cryptography, which means “secret writing”.

Critical Characteristics of Information

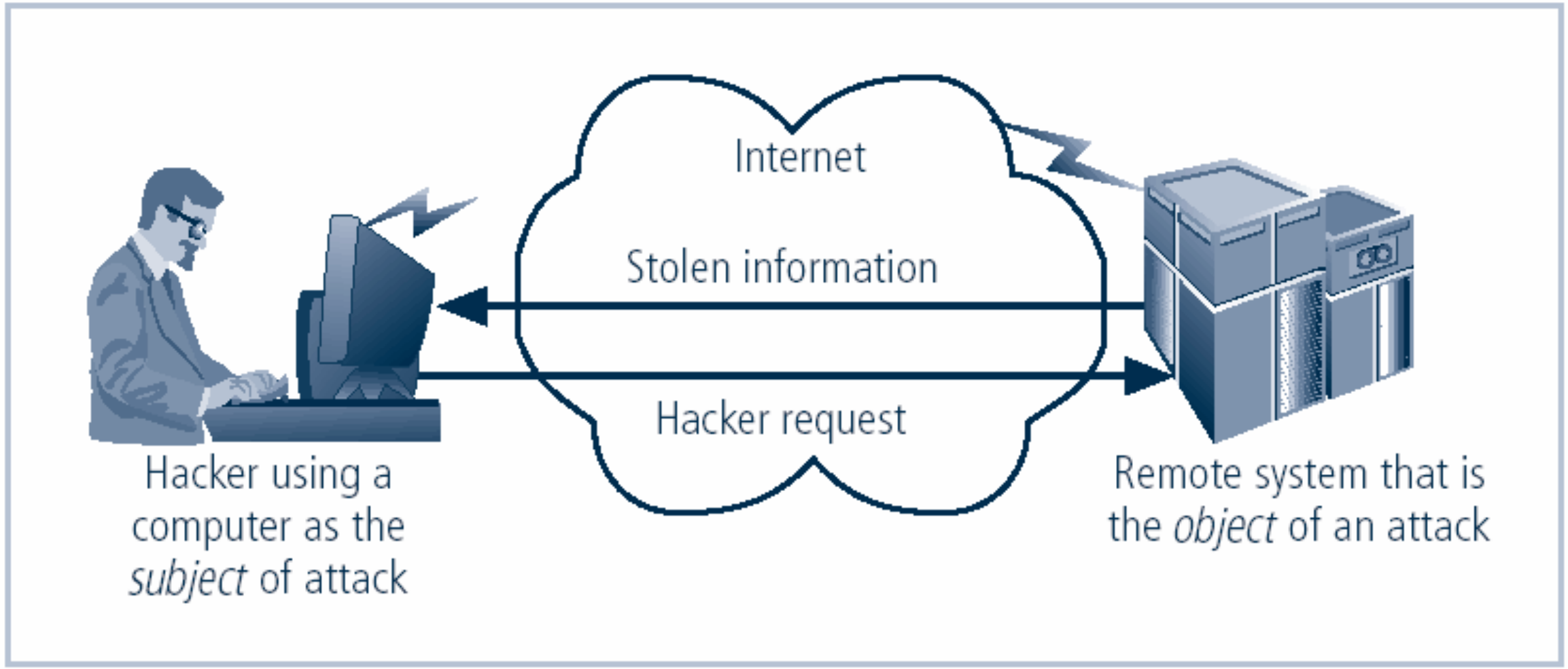
- The value of information comes from the characteristics it possesses:
  - Availability
  - Accuracy
  - Authenticity
  - Confidentiality
  - Integrity
  - Utility
  - Possession



Components of Information Security

Securing Components

- Computer can be subject of an attack and/or the object of an attack
  - When the **subject of an attack,** computer is used as an active tool to conduct attack.
  - When the **object of an attack,** computer is the entity being attacked.



Computer as the Subject and Object of an Attack

Layered Security

- **Layered security**, also known as **layered defense**, (also called defense in depth) describes the practice of combining multiple mitigating security controls to protect resources and data.
- Layered security refers to security systems that use multiple components to protect operations on multiple levels, or layers.
- It involves security protocols at the **system or network levels, at the application level, or at the transmission level.**
- Layered security efforts attempt to address problems with **different kinds of hacking or phishing, denial of service attacks and other cyber attacks, as well as worms, viruses, malware** etc.

Why do we need it?

- To provide adequate computer system protection.
- Gaps exist in protection capabilities in even the most sophisticated security applications.

A 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

Consumer Layered

- **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 communications.
- **Antimalware** – A front line antimalware application is absolutely critical to avoid system infection.
- **Antivirus** – An antivirus is a computer program used to prevent, detect, and remove computer virus.
- **Secure Web and e-mail**

Consumer Layered

- **Web Browser Security** – Most common portal for users to access the Internet.
- Enhancing its usability and ubiquity.
- User-friendly features such as recording browsing history, saving credentials and enhancing visitor engagement through the use of cookies have all helped the browser become a "one stop shopping" experience.
- However, the browser also has the potential to betray the user.
- Some issues are:

1. **Accessing browser history**
2. **Harvesting saved login credentials**
3. **Obtaining auto fill information**
4. **Analyzing cookies**
5. **Exploring the browser cache**

Enterprise Layered Security Strategy

- Workstation application whitelisting
- 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

Enterprise Layered Security

- 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.

Implementing a Layered Identity Strategy: Enterprise Layered

- 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.

Extended Validation (EV) Certificate

- An extended validation (EV) certificate **is a data security or anti-fraud measure** recommended in 2006 by the Certificate Authority Browser Forum.
- Extended Validation (EV) certificates are single-domain SSL (Secure Socket Layer) certificates **that offer the highest degree of authentication and SSL protection.**
- To ensure this, they require more evaluation and documentation checks for applicant websites than other certificate types.
- 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 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.

What is an Extended Validation Certificate?

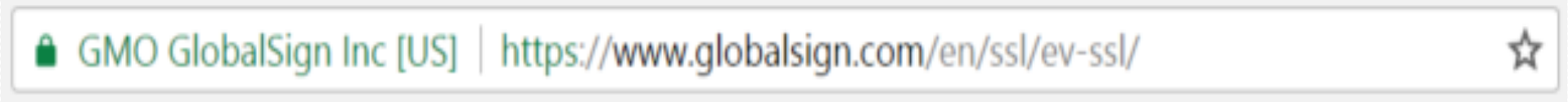
- An Extended Validation SSL Certificate (also known as EV SSL for short) is the highest form of SSL Certificate on the market. While all levels of SSL – Extended Validation (EV), Organization Validated (OV), and Domain Validated (DV) – provide encryption and data integrity, they vary in terms of how much identity verification is involved and how the certificates display in browsers.
- During verification of an EV SSL Certificate, the owner of the website passes a thorough and globally standardized identity verification process.
- This verified identity information is included within the certificate, with some pieces, including business name and country, presented directly in the browser window.

The primary purposes of an EV Certificate

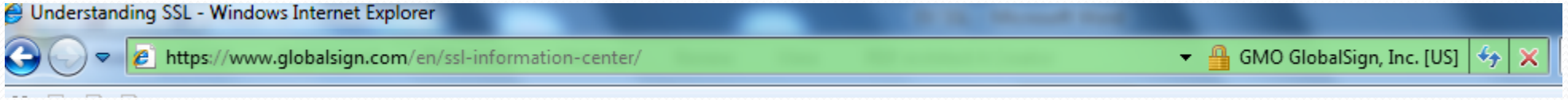
- To identify the legal entity that controls a website which provide a reasonable assurance to the user of an Internet browser that the website which the user is accessing is controlled by a specific legal entity identified in the EV Certificate by name, address of Place of Business, and Registration 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.
- EV Certificates provide a higher level of validation and are available to all business and government entities, but are not available to individuals.

Examples of EV SSL Certificates in Browsers

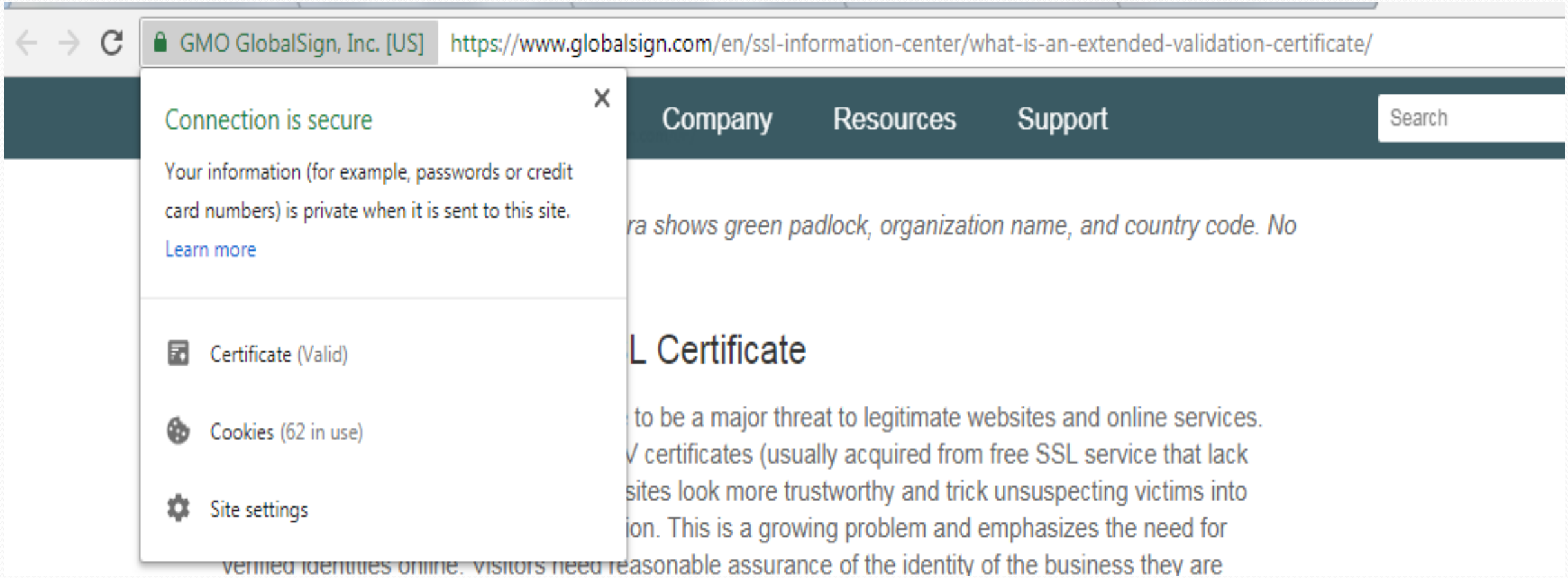
- The website using an EV SSL Certificate activates highly visible indicators directly on the browser address bar, namely the padlock, HTTPS, and the verified company name and country.
- These indicators are always changing and evolving as new browser versions are released.
- Website with EV SSL Certificate on Chrome shows padlock, HTTPS, organization name and office location country code in green font.



- Website with EV SSL Certificate on IE shows green bar, padlock, HTTPS,

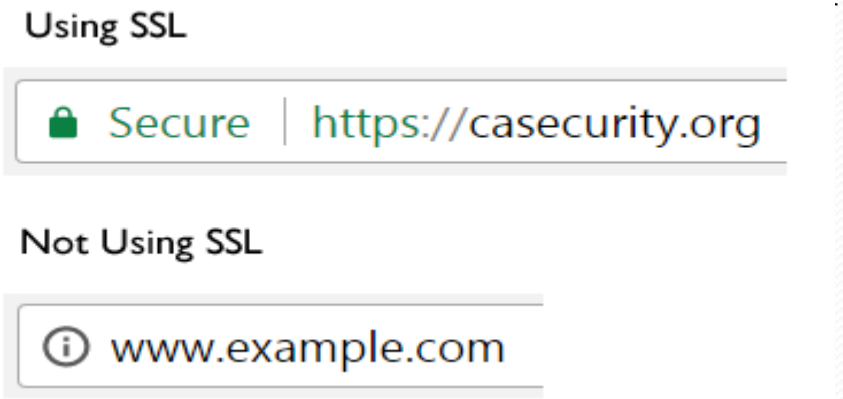


Examples of EV SSL Certificates in Browsers



Secure Sockets Layer (SSL)

- Secure Sockets Layer (SSL) was the most widely deployed cryptographic protocol to provide security over internet communications before it was preceded by TLS (Transport Layer Security) in 1999.
- SSL provides a secure channel between two machines or devices operating over the internet or an internal network.
- One common example is when SSL is used to secure communication between a web browser and a web server.
- This turns a website's address from HTTP to HTTPS, the 'S' standing for 'secure'.



SSL Certificate

Secure Sockets Layer (SSL)

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

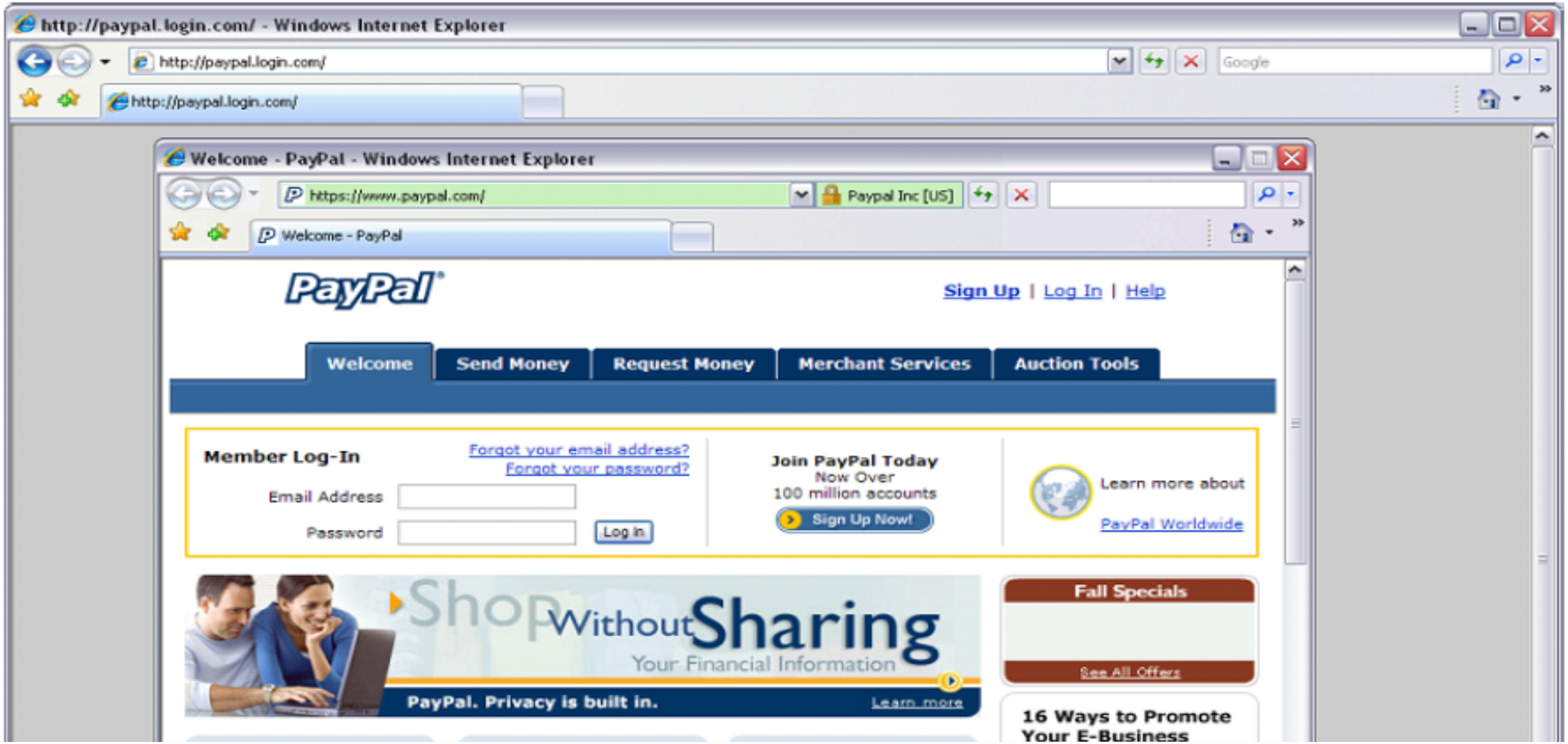
FIGURE 8.34 • Secure Sockets Layer (SSL)

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

What is SSL Certificate?

- 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”.

Designed for Banks and Large E-commerce sites



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?**

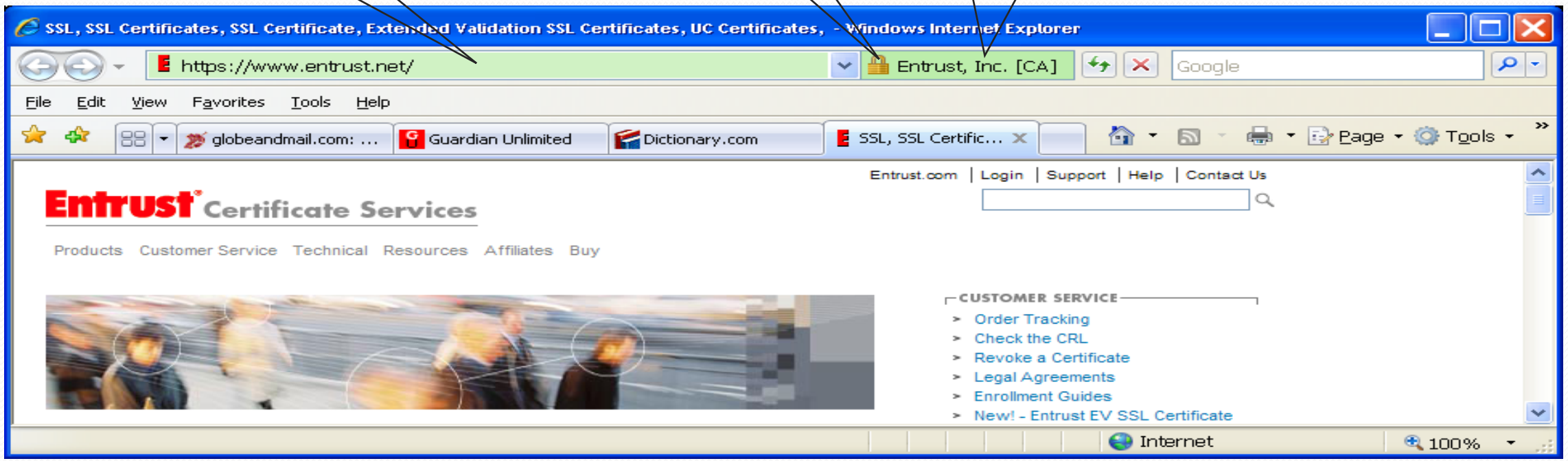
  A website using EV SSL Certificate will activate highly visible indicators directly on the browser address bar:
- **The green address bar, https:// and the padlock icon**
- **The name of the Organization that owns the website and the name of the Certification Authority that issued the EV SSL Certificate.**

Websites using EV SSL Certificates

Assumed name, registered name and country
alternating with
the issuer's name

Golden padlock

Green address bar



Remote Access Authentication

- Almost every business network today has (or will have) clients connecting to the network remotely, via dialup and/or **VPN connections.**
- 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.

Remote Access Authentication

- Remote access servers can be configured as dial-in servers or VPN servers.
- Dial-in servers use the Point-to-Point Protocol (PPP) or in the case of some older servers, the Serial Line Internet Protocol (SLIP) as the link layer protocol.
- VPN servers can use the Point-to-Point Tunneling Protocol (PPTP), Layer 2 Tunneling Protocol (L2TP), or IPSec tunnel mode to establish a secure "tunnel" over the Internet.
- Windows remote access servers support the following set of authentication methods:
  - Password Authentication Protocol (PAP)
  - Challenge Handshake Authentication Protocol (CHAP)
  - Microsoft's implementation of CHAP (MS-CHAP)
  - Updated version of MS-CHAP (MS-CHAP2)
  - Extensible Authentication Protocol/Transport Layer Security (EAP/TLS)

Remote Authentication Dial-In User Service (RADIUS)

- Remote Authentication Dial-In User Service (RADIUS) is a network protocol that **provides security to networks against unauthorized access.**
- RADIUS secures a network **by enabling centralized authentication** of dial-in users and authorizing their access to use a network service.
- It manages remote user authentication, authorization and accounting (AAA). So, RADIUS is often referred to as **RADIUS AAA.**
- RADIUS is used by many companies to enable roaming between ISPs, providing a single global set of credentials to be used on any public network.
- Further, the RADIUS server **keeps tracks of when a user session** begins and ends.

The RADIUS authentication mechanism works as follows:

1) Users **dial in and establish a PPP connection** with a network access server.
2) The user and the access server then **negotiate an authentication mechanism,** usually CHAP or EAP.
3) The user and the access server **exchange authentication information.**
4) The access server then packages the access information into an **"authentication request packet,"** along with information about the access server itself and the port being used.
5) **The packet is sent to the RADIUS** server over whatever connection is in use (LAN, WAN, switch, and so on).
6) When the RADIUS server receives the authentication request packet, it attempts to validate the user against the account information to which it has access. **The RADIUS server then returns either an "Authentication Acknowledgment" or an "Authentication Reject"** message to the access server.

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.

Policy-based encryption

- 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.
- **This functionality will give customers the ability to push encrypted messages to recipients with no dependencies on encryption technologies supported by the third party.**

Content Control

- By preventing access to unsafe or inappropriate material, an Internet content control solution **can help to strengthen an organization´s online security profile, reduce productivity loss and prevent bandwidth and HR issues** before they arise.
- **Content-control software**, commonly referred to as an **internet filter**, restricts or controls the content an Internet user is capable to access, especially when utilized to restrict material delivered over the Internet .
- Content-control software determines what content will be available or to be blocked.
- **Such restrictions can be applied at various levels:** a government can attempt to apply them nationwide (Internet censorship), or can be applied by an ISP to its clients, by an individual user to his or her own computer etc.

Content Control

- **Filters can be implemented in many different ways:** by software on a personal computer, via network infrastructure such as **proxy servers**, **DNS servers, or firewalls** that provide Internet access.
- Some techniques are:
  - Browser based filters
  - E-mail filters
  - Client-side filters
  - Content-limited (or filtered) ISPs
  - Network-based filtering
  - DNS-based filtering
  - Search-engine filters

E-Commerce

- 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.

Types of E-Commerce

- Business-to-consumer (B2C)
  - Connects individual consumers with sellers , cutting out the middleman
  - E.g. Amazon.com
- Business-to-business (B2B)
  - Supports business transactions on across private networks, the Internet, and the Web.
- Consumer-to-consumer (C2C)
  - Connects individual sellers with people shopping for used items
  - E.g. ebay.com
- C2B – Consumer to Business

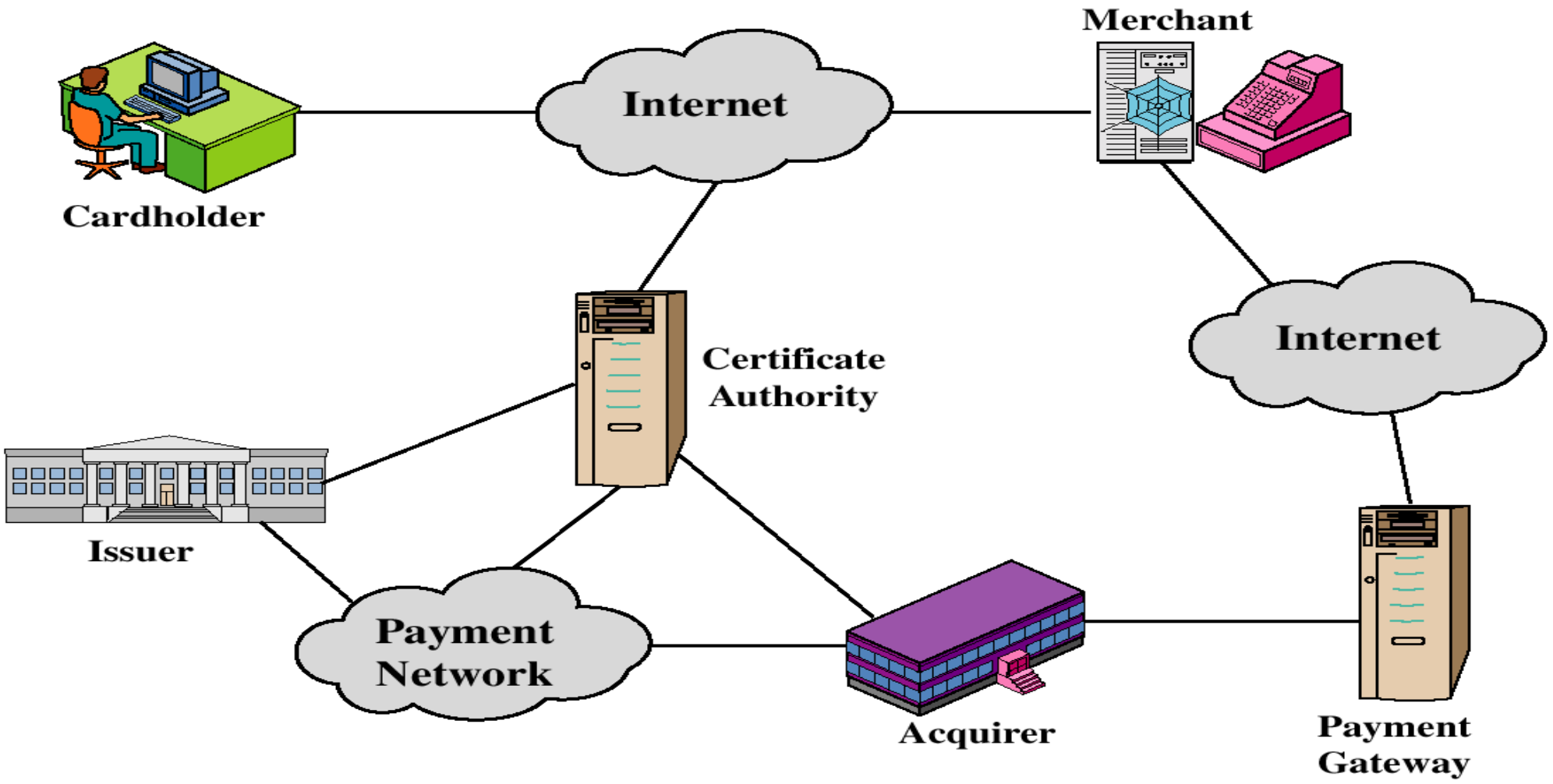
Secure Electronic Transactions (SET)

- Set of security protocols and formats.
- Provides a secure communication channel in a transaction.
- Protect credit card transaction on the Internet.
- Companies involved:
  - MasterCard, Visa, IBM, Microsoft, Netscape, RSA, Terisa and Verisign
- Not a payment system.
- Provides tust by the use of X.509v3 digital certificates.
- Ensures privacy.
- Provide confidentiality of payment and ordering information
- Ensure the integrity of all transmitted data
- Provide authentication that a cardholder is a legitimate user of a credit card account
- Provide authentication that a merchant can accept credit card transactions through its relationship with a financial institution

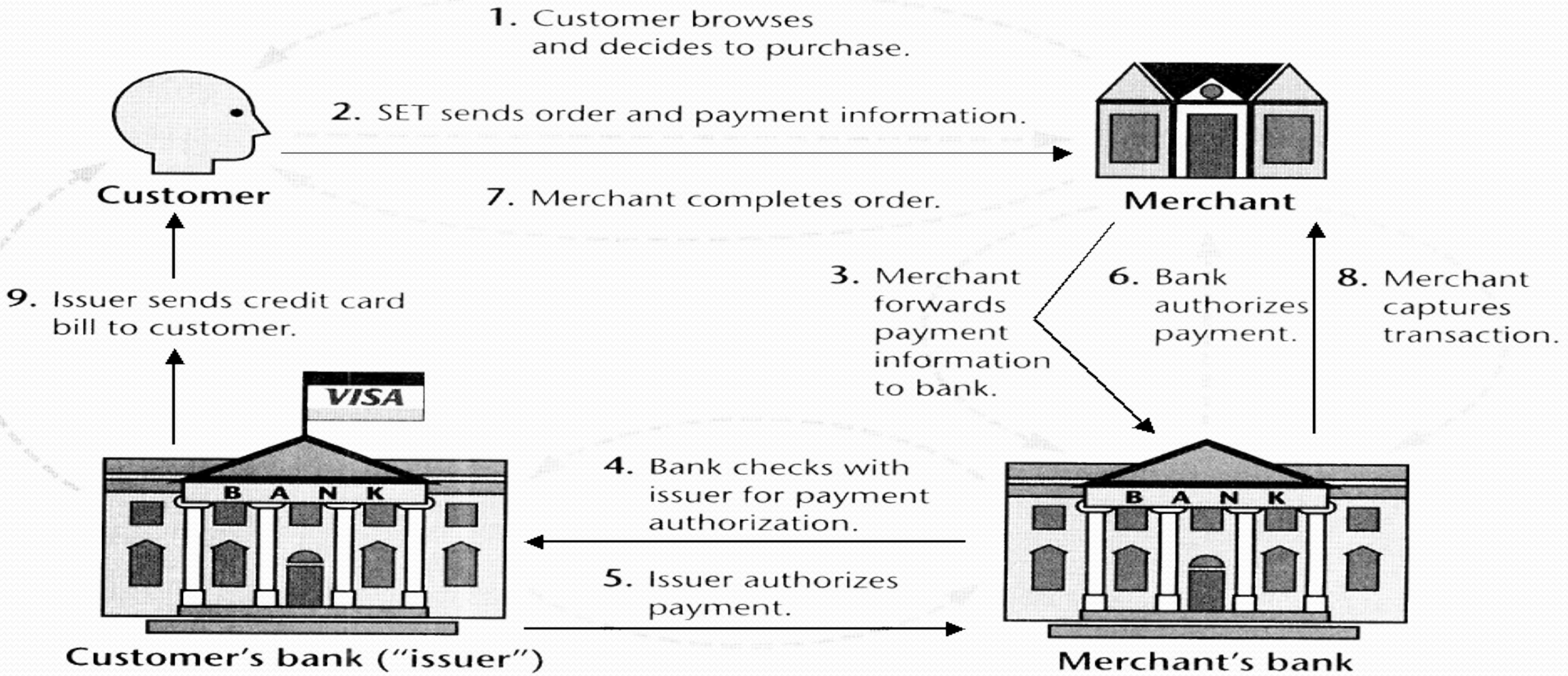
SET (cont..)

- Ensure the use of the best security practices and system design techniques to protect all legitimate parties in an electronic commerce transaction
- Create a protocol that neither depends on transport security mechanisms nor prevents their use
- Facilitate and encourage interoperability among software and network providers

SET Participants



SET Transactions



Assignment -1

- Write short notes on:

a) Significance of Biometric to control security threats
b) Role of encryption in IS security
c) Digital Signature and digital certificate

Email: shayakraj@ioe.edu.np

Deadline of submission: 2075-02-20

Thank you

Next Class:

Chapter-3 : Enterprise Management Systems