Introduction to Computer Security, Internet, E-commerce and E-governance with reference to Free Market Economy

Definition, Threats to security, Government requirements, Information Protection and Access Controls, Computer security efforts, Standards, Computer Security mandates and legislation, Privacy considerations, International security activity.

Conceptual Framework of E-commerce: governance, the role of Electronic Signatures in E-commerce with Reference to Free Market Economy in India.

Textbooks

1. Debby Russell and Sr. G.T Gangemi, "Computer Security Basics (Paperback)", 2ndEdition, O' Reilly Media, 2006. Computer Security Basics - Google Books
2. Cyber Laws and IT Protection, Harish Chander, PHI, 2012

Introduction to computer Security

computer security, the protection of computer systems and information from harm, theft, and unauthorized use. Computer hardware is typically protected by the same means used to protect other valuable or sensitive equipment.

The security precautions related to computer information and access address four major **threats**:

(1)theft of data, such as that of military secrets from government computers;

(2)vandalism, including the destruction of data by a computer virus;

(3)fraud, such as employees at a bank channeling funds into their own accounts; and

(4)invasion of privacy, such as the illegal accessing of protected personal financial or medical data from a large database.

Continues…

The laws make it a crime to reveal personal information gathered during business.

- Health Insurance Portability and Accountability Act (HIPAA)
- Family Educational Rights and Privacy Act (FERPA)

The organizations which provide assistance w.r.to attacks over internet:

- Defense Advanced Research Projects Agency (DARPA)
- Computer Emergency Response Team (CERT)

Information Sharing and Analysis Centers (ISACs) help in developing the best practices for protecting critical infrastructures and minimizing vulnerabilities.

Continues…

Computer crime is an act performed by a knowledgeable computer user, sometimes called a "hacker," that illegally browses or steals a company's or individual's private information. Sometimes, this person or group of individuals may be malicious and destroy or otherwise corrupt the computer or data files.

Examples:

- **Child pornography** - Making, distributing, storing, or viewing child pornography.
- **Click fraud** - Fraudulent clicks on Internet advertisements.
- **Copyright violation** - Stealing or using another person's Copyrighted material without permission.
- **Cracking**- Breaking or deciphering codes designed to protect data.

Continues…

Ref : What is Computer Crime? (computerhope.com)

Confidentiality, Integrity, Availability (CIA)

Computer and Network security is build on 3-pillars, C-I-A.

Confidentiality - preventing the disclosure of data to unauthorized parties.
Also keep the identity of authorized parties involved in sharing and holding data private and anonymous.

Often confidentiality is compromised by cracking poorly encrypted data, Man-in-the-middle (MITM) attacks, disclosing sensitive data.

Standard measures to establish confidentiality include:

1. Data encryption
2. Two-factor authentication
3. Biometric verification
4. Security tokens

Continues…

Integrity

Integrity refers to protecting information from being modified by unauthorized parties.

Standard measures to guarantee integrity include:

1. Cryptographic checksums
2. Using file permissions
3. Data backups

Availability

Availability is making sure that authorized parties are able to access the information when needed.

Standard measures to guarantee availability include:

1. Backing up data to external drives
2. Implementing firewalls
3. Having backup power supplies
4. Data redundancy

Continues…

Identification, Authentication, Authorization and Accountability

These are other terms but part of CIA model

Identification describes a method of ensuring that a user is the entity it claims to be. Identification can be provided with the use of a username or account number.

Authentication Prove you are **XYZ,** using multifactor authentication like password, biometric, passport, ID etc.

Authorization What are you allowed to access?

Accountability (also referred as Auditing)

Trace an action to a User's Identity

Prove Who/what a given action was perform by (non-repudiation)

Threats to Security

Vulnerability – weakness in a system

Threat – possible danger to the system

Countermeasures – techniques for protecting the system

Vulnerabilities

- Physical Vulnerabilities – intruder breaks into buildings & equipment/server room
- Natural Vulnerabilities – computers vulnerable to natural disasters (fire, flood, earthquakes, power loss) and environmental threats.(Dust, humidity, uneven temp.)
- Hardware and software Vulnerabilities
- Media Vulnerabilities – Damaged backup media
- Communication Vulnerabilities - interception
- Human Vulnerabilities – poorly trained administrator

Continues…

Threats

- Natural and physical threats – threats related to fire, flood, power failures and other disasters.

Can't prevent such disasters but can be detected quickly using fire alarms, sensors etc.

- Unintentional threats – ignorance creates dangers

More information is compromised, corrupted or lost through ignorance

- Intentional threats – outsiders and insiders

Countermeasures

- Computer security
- Communication security
- Physical security

Government requirements

The computer vendors who want to sell lot of work stations to govt., they are forced to build security into those products.

- Most govt. agencies specify security requirements along with the operational requirements.
- The seller need to use encryption to protect stored and transmitted data.
- Information protection : govt. agencies need to protect sensitive info. From theft, modification, data breaches and need to ensure integrity of the information.

Information Protection and Access Controls

Access control is a security technique that regulates who or what can view or use resources in a computing environment. It is a fundamental concept in security that minimizes risk to the business or organization.

There are two types of access control: physical and logical. Physical access control limits access to campuses, buildings, rooms and physical IT assets. Logical access control limits connections to computer networks, system files and data.

Physical access control can be limited by access card readers, auditing and reports to track employee access to restricted business locations and proprietary areas, such as data centers. Some of these systems incorporate access control panels to restrict entry to rooms and buildings, as well as alarms and lockdown capabilities, to prevent unauthorized access or operations.

Logical access control systems perform identification authentication and authorization of users and entities by evaluating required login credentials that can include passwords, personal identification numbers, biometric scans, security tokens or other authentication factors. Multifactor authentication (MFA), which requires two or more authentication factors, is often an important part of a layered defense to protect access control systems.

Ref: What is Access Control? (techtarget.com)

Access control methods:

Mandatory Access Control (MAC): • Only system owner manages access control. • End user has no control over any privileges.	**Based Access Control (RBAC):** • Provides access based on the position an individual has in an organization.
Discretionary Access Control (DAC): • Least restrictive model. • Allows an individual complete control over any objects they own.	**Rule Based Access Control (RBAC).** • Dynamically assign roles to users based on criteria defined by owner or system administrator.

Computer security efforts

In early 1950s, TEMPEST (the process of protecting sensitive equipment from emanating electromagnetic radiation (EMR) that may carry classified information)

- standards that strive to prevent outright data theft.
- 1960s – Department of Defense, National Institute of standers and technology or NIST, national security agency first initiated public awareness of security.
- 1967, DoD studied threats to computer systems and information
- Later Defense Advanced Research Projects Agency (DARPA) worked on identifying vulnerabilities and threats and introduced methods to safeguard systems and controlled access to defense computer systems, networks and information.
- 1970, Security controls for computer systems –a document is published, which is landmark in the history of computer security

Tiger Teams – In 1970s, first time emerged on computer scene.

These teams where govt. and industry sponsored teams of crackers.

They attempt to break down systems, security patches, flaws.

- Sponsored by DoD
- Penetration testing

Standards for secure Systems

National Bureau of standards (NBS) , also known as the National Institute of standards and Technology (NIST), responsible for the development of all kinds of standards.

- NBS sponsored conference on computer security in collaboration with ACM (Association of Computing Machinery).
- Required attention in three areas w.r.to:
- Policy : What security rules should be enforced for sensitive info?
- Mechanisms : What h/w and s/w mechanisms are needed to enforce the policy?
- Assurance : What need to be done for mechanisms to support the policy even when the system is subjected to threats?

National Computer Security Center (NCSC)

The Center was founded with the following goals:

- Encourage the widespread availability of trusted computer systems
- Evaluate the technical protection capabilities of industry- and government-developed systems
- Provide technical support of government and industry groups engaged in computer security research and development
- Develop technical criteria for the evaluation of computer systems
- Evaluate commercial systems
- Conduct and sponsor research in computer and network security technology
- Develop and provide access to verification and analysis tools used to develop and test secure computer systems
- Conduct training in areas of computer security
- Disseminate computer security information to other branches of the federal government and to industry

Computer Security mandates and legislation

Laws typical aim is to protect information.

-**protection of classified or sensitive information**

Legislation mandating computer security practices by federal agencies and con-tractors. The idea of this legislation is that organizations that process classified or sensitive unclassified government information must be careful to protect that information from unauthorized access.

-**computer crime**

Legislation defining computer crime as an offense and extending other regulations to cover thefts and other abuses carried out by computers and other new techniques. In addition to federal policies, virtually all U.S. states have enacted their own legislation prohibiting computer crime and abuse.

-**Privacy**

Legislation protecting the privacy of information maintained about individuals (e.g., health and financial records). Another consideration for computer privacy is the practice of merging records from multiple, seemingly benign databases into profiles that may reveal devastating amounts of information about an individual.

Privacy Considerations

The ability to collect and manage information doesn't necessarily confer the right to save, analyze, and publicize that information, but several recent attacks suggest that this is occurring.

In one high profile case, an airline was approached and asked to turn over the records of millions of passengers who had purchased tickets for trips on the airline.

Apparently the purpose was to combine the flight plans of customers with other data available commercially, such as reports from credit bureaus, and determine which fliers may fit the profile of a terrorist.

This is feasible only if you can rapidly combine information from several different databases, and that, in the view of many, represents a massive invasion of privacy.

International security activity

International security, also called **global security** is a term which refers to the measures taken by states and international organizations, such as the United Nations, European Union, and others, to ensure mutual survival and safety. These measures include military action and diplomatic agreements such as treaties and conventions. International and national security are invariably linked. International security is national security or state security in the global arena.

Chapter 2: Conceptual Framework of E-commerce: governance

➢ **Meaning of E-commerce**

Traditional method – contracts specifically written on paper documents.

The conduct of business and business transactions of any kind between the parties on the internet and cyberspace is called **e-commerce.**

While starting business on the internet or cyber space, the following points need to be followed:

- Market research
- Financial commitment – legal agreement
- Should be aware of problems in the business and type of transactions
- Should include certain terms & conditions in the contract which are profitable and favorable.
- New business can be started with single owner rather than partnership.

➢Growth and development of E-commerce

E-commerce have become popular especially in the corporate sectors due to scope of publicity.

--During COVID-19 and worldwide lockdown, e-commerce acted like a backbone for business and market industry.

-- not only purchase goods but also avail services.

--Jurisdiction for internet based disputes.

➢Definitions of E-commerce

-The World Trade Organization defined as “e-commerce is the production, distribution, marketing, sales or delivery of goods and services by electronic means”

-The consumer Protection Act, 2019 states, “ buying or selling of goods or services including digital products over digital or electronic network”

➢Various Modes of E-commerce

E-commerce operates through four modes:

- Advertising, sale, lease or license of tangible products

Ex: Books, machinery, buildings, land, vehicles

- Advertising, sale, lease or license of intangible products

Ex: IPR, copyrights, goodwill, patent, e-newspaper, online storage.

- Advertising, sale, lease or license of services

Ex: online ticket booking, online games, online banking

- Advertising, sale, lease or license of tangible products over the internet

➢**Mechanism involved in the operation of Internet**

All communicating devices are connected to the internet with there unique IP numbers.

Protocols like TCP/IP is used for data transmission.

Data is sent in the form of the packets, by using shortest path to destination.

For better security – packets are encrypted.

➢**Types of players in E-commerce**

- Network provider
- User
- Website
- Payment Providers
- Payment system provider
- Software Architects
- Advertiser
- Content Provider
- Back End systems

-- other than these search engines like google, yahoo etc.

- **Salient features of the new consumer protection Act, 2019: Law on E-Commerce and consumer protection**

Some changes are taken place after introduction of online or e-commerce in the consumer protection act, 1986.

Following are the features of Consumer Protection Act, 2019:

1. Def. of Consumer – person who " buys any goods" and " hires or avails of any service", but not a person who obtain goods for resale or commercial purpose.

2. Def. of e-commerce – in consumer protection act, 1986 was silent on online commercial transactions. IT Act, 2000 also not provided adequate framework.

But consumer protection act, 2019 defined e-commerce as " buying or selling of goods or services including digital products over a digital or electronic network"

3. Specification of 'Rights of Consumers' – The Act expressed rights of consumers under Section 2(9) of the Consumer Protection Act, 2019.

4. **Establishment of the Central Consumer Protection Authority (CCPA) :**

Sections 10-27 of CPA, 2019

5. **Key Concept of 'Product Liability' :** Under Section 2(34) of CPA, 2019 – responsibility of a product seller or manufacturer or service.

6. **Def. of 'Electronic Service Provider' :** Under Section 2(17) of CPA, 2019 – the person provides technologies to enable a product seller to engage in advertise/ sell goods/services to a consumer include online marketplace or online auction sites.

7. **Def. of 'Misleading Advertisement':** An advertisement which falsely describes the product or service.

8. **Establishment of Consumer Dispute Redressal Commission:** Sections 28 – 73 provides setting up of a Consumer Dispute Redressal Commission (CDRC).

9. Special Provisions on offences and penalties Under CPA 2019: Sections 88 – 93 regarding misleading advertisements, - fines with imprisonment.

10. Introduction of Mediation as an alternate Dispute resolution mechanism: : Under Section 2(25) of CPA 2019 defined termed mediation – the process by which a mediator mediates the consumer disputes.

Sections 74-81 – resolve the consumer dispute faster without approaching commissions.

- Web Development and Hosting Agreements
- Web Hosting
- The Problem of Internet Jurisdiction
- Illustrative Cases about cyberspace Jurisdiction

- **Types of websites**

Passive and interactive sites: These sites provide information in a read only format.

Interactive sites: These encourages the browser to enter information identifying the browser and provide back ground on the browser's interest or buying habits.

Chapter 3: The Role of Electronic Signatures in E-commerce with Reference to Free Market Economy in India

- Introduction
- Basic Laws of Digital and Electronic signature in India
- Authentication of digital Signatures and electronic records
- Authentication of electronic signatures and electronic records
- UNCITRAL(United Nations Commission on International Trade Law) : Model law on electronic commerce, 1996
- UNCITRAL: Draft rules of November, 1998
- Securing electronic transactions cryptography and securing electronic transactions
- The concept of Hash function
- Utility of Digital signature’s verification

- Certification, certifying authorities and the status of electronic signature under the Indian Law
- The appointment of controller and other officers and their functions
- Authentication and verification of electronic/digital signatures
- The cost and benefits of implementing electronic/digital signatures in E-commerce in India
- Security privacy of Electronic/Digital signatures
- Private key Escrow and key recovery systems
- Obligation of a certifying authority and certificate management
- Security threats to cyberspace and E-commerce
- International efforts to enact laws relating to electronic/digital signatures
- Efforts in the US
- Guidelines under the Singapore Electronic transaction Act, 1998
- Different approaches of digital signatures