Unit 8 Web Applications

Lesson Structure

8.0 Introduction

In this unit, you will learn about basics of the IP Address. A web browser is a software that interprets the coding language of the World Wide Web in graphic form. It also displays the translation rather than the coding. It allows users to 'browse or surf the web'. If you search the information through the browser it provides you the complete list of requested information. You will be able to navigate and switch between various linked pages. But you should be bypassing the surfing techniques. The role of keyword is very important in web surfing because keyword tags contains words and phrases the creator

of the page considers to be relevant to the document. The words are separated by commas or spaces or '+' sign.

In this unit, you will learn about web servers and the various services provided by them. Web services have the capacity to change the applications into web applications. You will learn about the two methods for writing web services. You will also learn about the composition of web servers. The web server composition can be defined with the help of various system components and alternatives, such as hardware alternatives, software alternatives and communication alternatives. The Domain Name System (DNS) is a client/ server identification application that uniquely identifies each individual host on the Internet. All the user names are methodized in a hierarchical fashion in DNS.

8.1 Unit Objectives

After going through this unit, you will be able to:

- Understand the significance of IP protocol and addresses
- Describe how messaging works in DNS
- Know the various domains in the DNS

8.2 Internet Security

Network security is a broad topic with a multi-layered approach. It can be addressed at the data link, network and the application layers. The issues concerned are packet intrusion and encryption, IP packets and routing tables with their update versions, and host-level bugs that occur at the data link, network and the application layers respectively.

TCP/IP protocols are used globally irrespective of the nature of the organizations, whether they are general category organizations or security-specific sensitive organizations. The news or information about hacking of websites or portals by undesired people is very common nowadays. This shows that the TCP/IP protocols are susceptible to interception. This generates a need to ensure all round security for the network in an organization. The tasks of the network administrator have to be widened to include the overall security of the network. He has to ensure that all parts of this network are adequately protected and adequate measures of security have been implemented within a TCP/IP network. He should be aware of an effective security policy. He should also be able to pinpoint the main areas of risk that the network may face. These main areas of risk vary from network to network depending upon the functioning of the organization. There are, therefore, various security-related aspects which have direct implications for the network administrator alongwith the means to monitor the implemented measures

of security effectively and to tackle the problem of breach of security if it happens.

Basic Requirements of Network Security

The main objective of the network is to share information amongst its users situated locally or remotely. Therefore, it is possible that undesired users can hack the network and prove to be harmful for the health of the network or the user. The network administrator must follow the following points to provide the network adequate security other than network-specific security as in the case of e-commerce, etc.

- Networks are designed to share information. Therefore, the network must be clearly configured to identify the shareable information and non-shareable information.
- The network should also clearly specify with whom the shareable information could be shared.
- An increase in the system security means a corresponding increase in the costs to the management. Therefore a compromising level between security and prices should be established as per the requirements of the network security system policy. This will largely depend upon the level of security needed for the network, the overall security requirements and the effective implementation of the chosen level of security.
- Division of the responsibilities concerning the network's security must be clearly defined between the users and the system administrator.
- The requirements for security must be detailed within a network security policy of the organization that indicates the valuable data and their associated cost to the business.
- After defining the detailed network security policy and clearly identifying his responsibilities in the organization, the system administrator should be made responsible for ensuring that the security policy is effectively applied to the company environment, including the existing networking infrastructure.

Levels of Security

The US Department of Defence has listed different steps in the evolution of security levels. The first step in this direction was the trusted computer system evaluation criteria in December 1985, popularly termed as the Orange Book. In continuation with this level, another security level known as the trusted network interpretation of the trusted computer system evaluation criteria or the Red Book was described in July 1987. These security levels contain the security-related problems in the component or the modular form.

Each level contains the specific security problem which is broken down into different divisions. Each of the divisions or classifications represents a security level defined in terms of the following general categories:

- User identification and authentication.
- The capability to monitor and audit system activity.
- Provision of discretionary access.
- Control of the reuse of resources.
- Identifying specific areas of possible attack.
- Provision of suitable counter measures.
- The level of system trusts, including systems architecture, design, implementation, transport, and trust of other hosts.

Data Security

Data security is concerned with the protection of data contained in a file or many files in a computer either as a standalone or on a network, from unauthorized interception.

In case of a postal system, a postcard as a carrier of information is open to all. It does not have any sort of security measures. An envelope is used to hide information from other people. An envelope acts as a means for security. Therefore, postcard and envelope have different purposes with respect to security. These two particular cases initiated similar actions to solve the security-related issues in case of data communication. E-mails are open to all as post cards. Following the envelope example in the postal system will enable users to secure at least some of their data.

The access protection provided by log on passwords is not a fool proof system and these may easily be bypassed. The bypassing can be done by booting from a diskette or connecting the stolen hard drive as a secondary one to another computer. In this manner, any vital data might easily be accessed. Consequently, encryption of the information seems to be the only effective way to protect data from being intercepted by unauthorized persons. The encryption must be developed to ensure reliable data security and that data is not decrypted without the right password or the right user. The main drawback of the password-based encryption includes the loss of password or registration of wrong passwords due to wrong spelling or some other human mistakes. In this case, it becomes impossible to restore the data. There are other rules to avoid in such situations.

The invalid access to the host can be prevented to a certain extent in the case of conventional host-to-terminal as the number of terminals connected is limited. The situation is entirely different in the case of Internet where access is allowed from any terminal connecting on a network. Therefore, this requires proper security measures. The following are the three types of security measures:

- Invalid access/Possibility of eavesdropping
- Firewall security
- Encryption (VPN Function)

8.2.1 Basic Techniques

Firewalls

The Internet provides a two-way flow of traffic that may be undesirable in many organizations where some information is needed exclusively for the organization or for the Intranet. The Intranet is a TCP/IP network that is modelled after the Internet that only works within the organization. In order to delineate information meant only for the benefit of the organization or its Intranet and the other open to all or meant for the Internet, some sort of security measures are needed to control the two-way flow of traffic. A measure known as firewall is used for this purpose.

A firewall is a combination of software and hardware components that controls the traffic between a secure network (usually an office LAN) and an insecure network (usually the Internet), using rules defined by the system administrator. The firewall sits at the gateway of a network or sits at a connection between the two networks, and the entire traffic between two or more networks has to traverse the firewall. The firewall stops or allows the traffic based on the security policy as defined in rules' table.

The secure trusted network is said to be 'inside' the firewall. The insecure untrusted network is said to be 'outside' the firewall. The firewall's architecture has to be such that it would permit a certain amount of traffic to get through, otherwise it would be more of a 'stonewall', preventing access to the Internet, or sending of e-mails or any other information from either side of the firewall, thus turning into a self-defeating exercise.

The fact that it allows some traffic through provides a channel that could potentially be exploited, and could carry viruses.

However, principally, the philosophy behind firewall is:

- It exists to block traffic.
- It exists to permit traffic.

In brief, the basic aim of firewall is to provide only one entrance and exit to the network. There are two firewalls. One blocks the undesirable traffic, while the other allows traffic.

8.2.2 Data Encryption

Encryption hides your data from curious eyes. This is a method of encoding data to prevent unauthorized persons from viewing or modifying it. The main features of data encryption are:

- Prevents unwanted access to documents and e-mail messages.
- Even the strongest levels of encryption are very difficult to break.

Processes and Types of Encryption

The process of data encryption consists of certain steps. The data passes through a mathematical formula called an algorithm, which converts it into encrypted data called ciphertext. These algorithms create a key and then encapsulate the message with this key.

There are two types of encryptions – asymmetric and symmetric.

Asymmetric Encryption

In public key (asymmetric) encryption, two mathematically-related keys are used – one to encrypt the message and the other to decrypt it. These two keys combine to form a key pair. Asymmetric encryption provides both data encryption and validation of the communicating parties' identities and is considered more secure than symmetric encryption, but is computationally slower.

A public key encryption scheme has following six major parts:

(i) Plaintext: This is the text message to which an algorithm is applied.

(ii) Encryption Algorithm: It performs mathematical operations to conduct substitutions and transformations to the plaintext.

(iii) Public and Private Keys: These are a pair of keys where one is used for encryption and the other for decryption.

(iv) Ciphertext: This is the encrypted or scrambled message produced by applying the algorithm to the plaintext message using keys.

(v) Decryption Algorithm: This algorithm generates the ciphertext and the matching key to produce the plaintext.

Encryption Process

The asymmetric data encryption process has the following steps:

- The process of encryption begins by converting the text to a pre-hash code. This code is generated using a mathematical formula.
- This pre-hash code is encrypted by the software using the sender's private key.
- The private key is generated using the algorithm used by the software.
- The encrypted pre-hash code and the message are encrypted again using the sender's private key.
- The next step is for the sender of the message to retrieve the public key of the person for whom this information is intended.
- The sender encrypts the secret key with the recipient's public key, so that only the recipient can decrypt it with his/her private key, thus concluding the encryption process.

Decryption Process

The asymmetric data decryption process has the following steps:

- The recipient uses his/her private key to decrypt the secret key.
- The recipient uses his/her private key along with the secret key to decipher the encrypted pre-hash code and the encrypted message.
- The recipient then retrieves the sender's public key. This public key is used to decrypt the pre-hash code and to verify the sender's identity.
- The recipient generates a post-hash code from the message. If the post-hash code equals the pre-hash code, then this verifies that the message has not been changed enroute.

Symmetric Encryption

Private key encryption (symmetric) – also known as conventional or single-key encryption – is founded on a secret key shared by two communicating parties. It requires all parties that are communicating to share a common key. The secret key is used by the sending party to convert simple text to encrypted text, i.e., text that is enciphered using the secret key as the security component of the mathematical process. The receiving party then proceeds to decipher the encrypted material, using the same secret key that it shares. Examples of symmetric encryption systems would include the RSA RC4 algorithm (that furnishes the basis for Microsoft Point-to-Point Encryption (MPPE), Data Encryption Standard (DES), International Data Encryption Algorithm (IDEA), and the procedure now put forward by the US Government called 'Skipjack' Encryption Technology already utilized in the clipper chip.

An encryption scheme has five major parts:

(i) Plaintext: This is the text message to which an algorithm is applied.

(ii) Encryption Algorithm: It performs mathematical operations to conduct substitutions and transformations to the plaintext.

(iii) Secret Key: This is the input for the algorithm as the key dictates the encrypted outcome.

(iv) Ciphertext: This is the encrypted or scrambled message produced by applying the algorithm to the plaintext message using the secret key.

(v) Decryption Algorithm: This is the encryption algorithm in reverse. It uses the ciphertext and the secret key to derive the plaintext message.

When using this form of encryption, it is essential that the sender and the receiver have a way to exchange secret keys in a secure manner. If

someone knows the secret key and can figure out the algorithm, communications will be insecure. There is also the need for a strong encryption algorithm. What this means is that if someone were to have a ciphertext and a corresponding plaintext message, they would be unable to determine the encryption algorithm. There are two methods of attacking conventional encryption – brute force and cryptanalysis. Brute force is just as it sounds; using a method (computer) to find all possible combinations and eventually determining the plaintext message. Cryptanalysis is a form of attack that strikes the characteristics of the algorithm to deduce a specific plaintext or the key used. One would then be able to figure out the plaintext for all past and future messages that continue to use this compromised setup.

8.2.3 Authentication

A user remotely located must be first authenticated before accessing the network or Intranet of an organization. The authentication procedures must be built into the firewall applied to the network or Intranet for security measures. The following are the procedures to validate remote login or access along with their comparisons and features.

1. **Using UNIX Password for Authentication:** The password without encryption is open to all over the network or the Internet. Hence, authentication practicing UNIX password may most likely lead to eavesdropping of the password over the network or the Internet because the password is not encrypted before being sent. This type of system is not suitable for authentication of remote login.
2. **Using IP Address for Authentication:** Packet-filtering types of firewalls commonly use IP addresses for authentication of data. They apply a set of already-defined procedures over each received packet before routing to the desired destination. Each packet received is examined for the pre-established rules to determine the access validity to the requested network or only for some available services on the network.

An authorized user, for example, may log into the network. However, he may be allowed to use only certain services or server on the destination network. This is achieved by filtering the packet for certain addresses or packet types.

The major disadvantage of this type of authentication procedure is that the IP address authenticated by firewall system or network to be accessed may fall into wrong hands. Consequently, undesirable users or hackers may hack the network by getting access through the authenticated IP address hacked as explained above.

Packet-filtering technique enables the network to determine the type, protocol, source and destination addresses for unauthorized access. This is a major advantage of this technique.

3. **Using One-Time Password for Authentication:** In the above two procedures, we have witnessed some loose ends which need to be looked into. In case of password authentication, the password remains unencrypted and therefore susceptible to be hacked. Access to a network by some undesirable person may be avoided if the password is validated only once to login to remote network. Different passwords are transferred over the network for each and every login. The authentication system involving this feature can assure the highest security of all types. It is evident that even if a hacker acquires the password, he cannot login to the network with that password.

8.2.4 Network and Web Security

Managing Windows security is required to manage the complete system for running the applications, downloading the update features for Windows, runtime programs, etc. For this, installing and downloading the updated antivirus, spyware protection, installing the firewall software, spamming and filtering the emails, accessing the damaged files, setting the permission level, removing network access for unauthorized users, setting the group policy for users and workgroups, securing virtual private network, configuring the wireless security features, creating back-up and restoring the essential files are essential. These tasks are essential to determine the Windows security. The Windows security policy is essential for programs and documents. It supports remote accessing of data, server security, e-mail accessing policy, anti-virus policy. It also permits the monitoring traffic too that is applied to handle the data transaction. The security setting for windows are basically managed by the network administrator because it is a part of the domain. Domain represents here a group of computers on a network. To help protect your computer, the administrator of this computer should do the following tasks:

- Install and use a firewall, such as Windows Firewall in Microsoft Windows XP or any other enhanced firewall.
- Set up Automatic Updates to download and install critical updates automatically. Install antivirus software keep it turns on and up to date.

The Windows can be secured by the implementation of following tasks:

Group Policy

Group Policy Objects (GPO) are linked to active directory containers. These containers are sites, domains, organizational units. GPOs cannot be linked directly to users, computers or security groups. GPOs can be linked to multiple sites, domains, or organizational units. In addition, a site, domain, or organizational unit can be linked to several GPOs. When you link with multiple GPOs to a single container, such as domain, site, OU, etc. you need

to specify the order in which the GPO are processed. The lowest link order GPO in the list has the highest precedence and overwrites the settings of all other GPOs. Group Policy is processed in this order:

Antivirus Software(s)

Now you know the concept of worms, spyware and viruses. You need to install and run the antivirus programs to clean the virus and provides the security for Windows. It helps in protecting Windows from crashing. The antivirus software available in the market to deal with virus-related issues are as follows:

- Symantec Antivirus that is used to check the security of foreign programs and applications.
- Windows 8/ Windows 10 AntivirusSpyware, AntivirusNorton Antivirus that is used to catch worms, rootkits, spywares, viruses, etc..
- Avast Antivirus.
- Kaspersky Antivirus that is used for HTTP traffic-checking and for providing a security wizard.

These antiviruses are useful for those types of viruses that are downloaded from the net or from email attachments. The most popular antivirus programs are Data Fellows F-Prot, EliaShim ViruSafe, ESaSS ThunderBYTE, IBM Antivirus, McAfee Scan, Microsoft Anti Virus, Symantec Norton Antivirus and S&S Dr Solomon's AVTK. The hard disks and drives must be scanned on a daily basis. Every week, hackers and malicious programmers release their virus programs across the Internet so it is better to keep the system updated with the latest antivirus software and programs. The updated user manual and help files must be provided to the users during the installation of expensive applications and the operating system. In fact, automatic updates to the list of antivirus and multithread detection are the standard features of an antivirus program.

8.3 Internet Services

The following are the various services provided by the Internet:

8.3.1 Blogging

Blog is short for Web log, a form of online journal. The best known services are offered by:

- WordPress
- Blogger
- Typepad
- Live Journal
- Squarespace

A blog can have a single author or several. Most blogs allow readers to post comments in response to an article or post. Bloglines is an RSS reader—a service that collects updates from your favourite blogs so that you can read them in one place. Microblogs is a cross between instant messaging and blogging. Twitter is a microblogging system that allows a user to send short, 140-character informational updates. Users can also follow the updates of selected friends.

Blogs are online journals that have come to be the most popular form of social media. Entries appear in reverse chronological order, that is, the most recent appears first. Microblogging can be best described as a combination of social networking and small-scale blogging. It is different from traditional blogging in that its content is smaller in size. Content or updates in small, limited amounts are distributed online and through the mobile phone network. The users exchange small bytes of content, images or video links, which are often referred to as microposts. The topics may vary from mundane to intellectual or spiritual. The most popular microblogging medium is Twitter.

The term 'Web log' or 'blog', was coined by Jorn Barger in 1997. It is simply a Web page comprising brief entries or content in the form of opinions, information, personal diary entries, or links, known as posts. These posts are organized in a chronological manner with the most recent coming first, just like in an online journal. Most blogs permit visitors to add a comment below an entry. Blogs are unique and different from other Websites due to several characteristics:

- **Tone:** Blogs are written in a personal, conversational style. They are written by identified authors or groups of authors.
- **Topic:** Blogs actually define what they write. They can be specific or very wide in scope. They could talk specifically about a certain book or reflect on life itself.
- **Links:** It is very easy to insert links and trackbacks to other Websites in blogs. These links are inserted in reference to an article or post or lead to additional information on the subject being written about.
- **Comments:** Each blog post has a section on comments, which acts as a message board for that article. On popular blogs, depending on the size of the audience, there could be prolonged debates in these sections.
- **Subscription:** RSS technology makes it easy to subscribe to blogs. The free blogger service offered by Google makes it extremely easy to set up blogs. Others like WordPress and Typepad offer more features. Some offer these features for a fee.

Types of Blogs

Bloggers are of different genders and come from different backgrounds, age groups and ethnicity. They cannot be generalized. Blogs can be personal or political.

Personal blogs are written by people who are in the habit of writing personal diaries. Sometimes, such personal blogs become very popular. In fact the very popular ones are usually anonymous. There is a recent trend of writing blogs about politics. These **political blogs** voice their opinions in response to media bias. They comment on the news, analysing misrepresented issues or misreporting by by mainstream media.

In the US, presidential candidates are known to employ bloggers who advise on the ways to reach out to political bloggers and their readers. In India too, political bloggers have begun playing a significant role in the political scenario, and some politicians are using them to making their presence felt in the mainstream media.

Business blogs, maintained by professionals and businesses allow companies to communicate in an informal sort of way unlike traditional in newsletters, brochures and press releases. These lend a human face and voice to the organization. For individuals in business, a blog can become an effective way of building a network of like-minded individuals and raising their own profiles. Some blogs operate as proper media businesses carrying advertisements and employing fulltime bloggers. They are the ones who benefit from new blogging technologies and opportunities with which communities can be built. Such blogs cover news and opinions in the technology and media industries. Such blogs are referred to as 'Almost media' blogs.

Most national and international newspapers including BBC have blogs for some of their reporters and editors. These are **mainstream media blogs**. These provide insights into the news-gathering and reporting process and also reveal the personal views of journalist which would otherwise never have been revealed. While several journalist blogs are hosted on newspaper sites themselves, several are independent, personal blogs focussed on specific professional interests.

8.3.2 Social Networking

Social media has not been properly defined. It cannot be called media in the true sense because social media Websites like Facebook, Twitter and others are merely platforms for interaction and collaboration. They are not really media. In fact, the traditional media like print and broadcast provide platforms for delivery of content and also advertisements. Social media is a place for collaboration and interaction and not advertisements and content. Social media is defined by some as a media for social interaction, which uses highly

accessible and scalable communication methods. It uses mobile as well as Web-based technologies to transform communication into interactive dialogue.

Generally, social media comprises the applications used by people and communities to exchange and collectively generate information. Specifically, social media has all the real time communication tools for sharing. The main characteristics are as follows:

Participation: It allows people to contribute and give feedback. The difference between audience and media is very thin.

- **Collaboration:** The audience is encouraged to interact and contribute. The applications make it possible for the audience to comment, share information and also give feedback. Opinion polls are encouraged. Nothing hampers accessibility or usage of content.
- **Conversation:** Traditional media focusses on transmission or distribution of content to the user. Social media, on the other hand, encourages twoway conversation. Not only can communities be created quickly, it is possible to share content effectively. Web-based communities are formed around common interests or goals. Social media also supports the basis for collaboration among the already present communities.
- **Connectivity:** Almost all social media thrive on connectivity. They help connect people and information in one place. They make use of external hyperlinks to other Websites, resources and people. Although social media can be defined in many different ways, one thing is very clear. It will continue to evolve and its use will expand in the coming days. It will soon integrate itself more into our personal lives and also in a commercial way.

CompuServe was the first major commercial Internet service provider for the public in the United States. It used a technology, which was then known as dialup. It dominated through the 1980s and remained a major player till the mid- 1990s. The first e-mail was delivered in 1971. However, the history of social media can be traced back to the late 1970s when computer enthusiasts Ward Christensen and Randy Suess invented the Bulletin Board System (BBS). Usenet was an early bulletin board that connected Duke University and the University of North Carolina. In 1992, Tripod was founded as an online community for college students. Beverly Hills Internet (BHI) began Geocities in 1994, which allowed people to create their own content. GeoCities crossed one million members in 1997 but was soon shut down in 2009 when it had around 38 million users. By 1997, the Internet had crossed one million sites. Blogging, alongwith online chat began for the first time. SixDegrees.com helped users to create profiles and list friends. AOL (America On-Line) Instant Messenger opened the Internet Relay Chat (IRC) system.

Next came the online Content Management System for Teachers and Students called Blackboard. Friends Reunited, was founded in 1999 in UK to trace old school friends. It is regarded as the first online social network, which gained importance. In 2001, the world's largest wiki known as the Wikipedia, an online encyclopedia was started and Apple launched iPods. In 2002, Friendster, a social networking site, was opened to the general public in the US. It became hugely popular and grew to 3 million users in just three months.

The clone of Friendster known as MySpace was launched in 2003 while Linden Lab created the Second Life, the next generation virtual world. LinkedIn was the next which started as a work-related social networking site for professionals.

The revolutionary social networking site, **Facebook**, was launched in 2004 for students at Harvard College. **Podcasting** was started on the Web and **Flickr** was founded as a site, which allowed people to upload pictures. **Bebo** (Blog Early, Blog Often) was started as another social networking Website while **YouTube** began storing and retrieving videos. By 2006, **Twitte**r opened as a microblogging site, allowing members to send and receive 140-character messages named tweets. **Geocities** and **Blogger** started in the late 1990s and continued to progress with **Friendster** and **MySpace** in the new millennium to the new social media giants like **Facebook**, **Twitter**,**Google+** and **Pinterest**.

8.3.3 E-Commerce

Electronic commerce or e-commerce is a business activity that occurs over telecommunication networks. E-commerce is a process of buying and selling products, services and information over computer networks. Electronic commerce has begun to address the needs of consumers, organizations, and vendors resulting in cost effectiveness and improved quality of goods and services. Another outcome of e-commerce is the increased pace of service delivery. E-commerce is a term that also relates to the application of computer networks to search and retrieve information over the Internet for decision-making. Electronic commerce makes use of various technologies, such as electronics, commerce, the Internet marketing, Supply Chain Management (SCM), Electronic Data Interchange (EDI), inventory management systems, automated data collection systems and online transaction processing. Modern electronic commerce will deal with the World Wide Web (WWW) at one point or the other in the life-cycle of every transaction. Apart from the World Wide Web, e-commerce may also incorporate a larger arena of technologies like social media, mobile devices, e-mail and telephones as well.

E-commerce is related to buying as well as selling of information, products including services over computer networks. This activity occurs via

a variety of networks that make up the Information superhighway (I-Way). A principal element of e-commerce is the processing of information and it is usually considered from the sales perspective of e-business. E-commerce also comprises the exchange of data to promote the payment and financing perspectives of business transactions.

The different levels of commerce, other than production, distribution, and the delivery of goods, are forms of information gathering, processing and manipulation. Distribution of information occurs over computer networks that are perfectly befitted to handle this operation.

Transactions between a company and its consumers happen over public networks for various purposes such as home banking and home shopping. Such critical operations use encryption for security and, credit, electronic cash, or debit tokens for payment.

Some of the e-commerce transactions include:

- Trade transactions.
- Payment transactions.
- Buying and selling transactions.
- Data transfer.

Using e-commerce, transactions can be done very effectively and quickly as there is no human intervention involved in carrying out these transactions.

8.3.4 E-Learning

E-learning (or eLearning) is the use of electronic educational technology in learning and teaching. Information and Communication Technology (ICT) in education, EdTech, learning technology, multimedia learning, Technology-Enhanced Learning (TEL), Computer-Based Instruction (CBI), Computer Managed Instruction, Computer-Based Training (CBT), Computer-Assisted Instruction or Computer-Aided Instruction (CAI), Internet-Based Training (IBT), flexible learning, Web-Based Training (WBT), online education, virtual education, Virtual Learning Environments (VLE) (which are also called learning platforms), m-learning, and digital education. In usage, all of these terms appear in articles and reviews; the term “e-learning” is used frequently, but is variously and imprecisely defined and applied.

These alternative terms are all linguistically more restrictive than ‘educational technology’ in that they refer to the use of modern tools, such as computers, digital technology, electronic media, networked digital devices and associated software and courseware with learning scenarios, worksheets and interactive exercises that facilitate learning. However, these alternative names individually emphasize a particular digitization approach, component or delivery method. Accordingly, each conflates to the broad domain of educational technology. For example, m-learning emphasizes mobility, but is otherwise indistinguishable in principle from educational technology.

The origin or etymology of e-learning is contested, with the e- part not necessarily meaning electronic as per e-mail or e-commerce. Coined between 1997 and 1999, e-learning became first attached to either a distance learning service or it was used for the first time at the CBT systems seminar.[6] Since then the term has been used extensively to describe the use of online, personalised, interactive or virtual education.

Bernard Luskin, an educational technology pioneer, advocated that the "e" of e-learning should be interpreted to mean "exciting, energetic, enthusiastic, emotional, extended, excellent, and educational" in addition to "electronic." Eric Parks suggested that the "e" should refer to "everything, everyone, engaging, easy". These broad interpretations focus on new applications and developments, as well as learning theory and media psychology.

Moore *et al.* found "significant variation in the understanding and usage of terms used in this field" and pointed to "implications for the referencing, sharing and collaboration of results." In usage, e-learning is an extremely significant (but incomplete) subset of educational technology.

8.3.5 Digital Signature and Smart Card

Digital signatures are not the literal digital images of a typical handwritten signature. Digital signatures are a form of encryption that provide authentication. They are gaining much popularity and have been touted as a way to move into a completely paperless environment.

Digital signatures are not the typical digitized image of a handwritten signature put on an electronic document. It is a method of authenticating information electronically by using encryption. Therefore, we know that the information will have to be authentic and secure if the decryption of the information works properly with the sender's public key. If the decryption works properly, we have some integrity protection as well and also know that the information did not change during transmission. With a digital signature, we want to take this protection one step further and protect the information from modification after it has been received and decrypted.

Figure 8.45 shows how this may be done. First, information is put through a message digest or hash function. The hash function creates a checksum of the information. This checksum is then encrypted by the user's private key. The encrypted checksum and the information are then sent to the receiver of the information. When the receiver gets the information, she can also put it through the same hash function. She decrypts the checksum that came with the message and compares the two checksums. If they match, the information has not changed. By keeping the original encrypted checksum with the information, the information can always be checked for modifications.

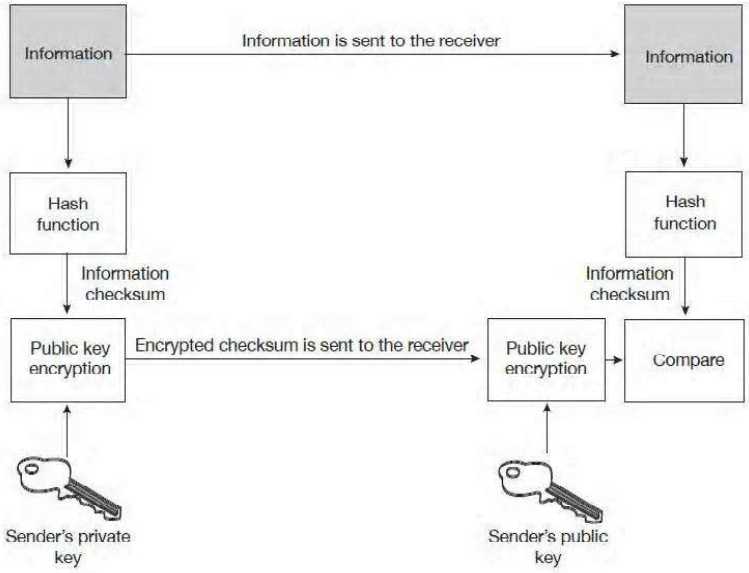

Fig. 8.45 *Secure Hash Functions*

The security and usefulness of a digital signature depends upon two critical elements:

- Protection of the user's private key
- A secure hash function

A user must protect his private key. If the private key is lost/stolen, then he cannot be sure that only he is using it. If someone else is also using his private key, there is no guarantee that only the correct user could have signed the information in Question. Secure hash functions are necessary for digital signatures. A hash function can be called secure if:

- The function is one-way. In other words, the function creates a checksum from the information but you cannot create the information from the checksum.
- It is very difficult to construct two pieces of information that provide the same checksum when run through the function.

The second condition is not as easy to satisfy. The checksums should also be smaller than the information so as to make it easier to sign, store, and transmit. If this is the case, then it must also be true that a large number of different pieces of information will correspond with the same checksum. What makes the functions secure is the manner in which all the bits in the original information correspond with all the bits in the checksum. Thus, if a single bit in the information is changed, a large number of bits in the checksum will automatically change. Secure hash functions should create a checksum of at least 128 bits.

The two most common secure hash functions are:

- MD5, which produces a 128-bit checksum
- SHA, which produces a 160-bit checksum

There are many other hash functions but most of them have been proven insecure. MD5 has been identified as having weaknesses that may allow a computational attack. This attack may allow a second piece of information to be created that will result in the same checksum. SHA was developed by the United States government and is currently believed to be secure. Most security software offers both MD5 and SHA as available options.

Smart Card

A smart card, chip card or Integrated Circuit Card (ICC) is any pocket-sized card with embedded integrated circuits. Smart cards are made of plastic, generally polyvinyl chloride, but sometimes polyethylene terephthalate based polyesters, acrylonitrile butadiene styrene or polycarbonate. Smart cards can provide identification, authentication, data storage and application processing

Thus a smart card is a plastic card with a microprocessor and memory embedded in it. These cards are available in various sizes and are of different types. They can be as big as a credit card or as small as SIM cards. Some cards have only non-programmable memory in them. These cards are read-only and the information on them cannot be changed or manipulated. The smart cards with a microprocessor in them have various functionalities. Smart cards are defined based on, (*i*) How the card data is read and written; and (*ii*) The type of chip implanted within the card and its capabilities. Mostly all chip cards are built from layers of differing materials, or substrates, that when brought together properly gives the card a specific life and functionality. The card layers are printed first and then laminated in a large press. Smart-cards can authenticate identity. Usually, they employ a Public Key Infrastructure (PKI). The card stores an encrypteddigital certificate issued from the PKI provider along with other relevant information.

Classification of Smart Cards

The smart cards are classified as follows:

On the basis of the capabilities they are classified as:

- **Microprocessor Based Cards:** These have greater memory storage as compared to the cards without a microprocessor. The security of data on the microprocessor cards is greater than any other storage device because it has the microprocessor embedded in the plastic card along with the memory.
- **Memory Based Cards:** These are used for applications in which the function of the card is fixed. These cards need a card reader to manipulate the data on the card. These cards communicate to the reader using some synchronous proto cols .Memory based smart cards have no processing power and cannot manage the data stored in them. These cards are widely used as prepaid phone cards.

On the basis of the mechanism they are classified as:

- **Contact Cards:** As the name suggests, they come in contact with the reader.

  These are the size of a credit card. A metallic chip is embedded inside the plastic card with a microprocessor and a memory or only with a memory. They are widely used in network security, access control, e-commerce, electronic cash and as health cards.
- **Contactless Cards:** The contactless cards do not directly come in contact with the card. These cards have an antenna built in the card. The antenna of the contactless cards is used to communicate to the card reader for reading and writing data on the card. The working of these cards is based on Radio Frequency Identification (RFID) technology. These cards are used as parking cards, student identification and electronics passports.
- **Combination Cards:** These are a combination of the contact and contact less smart cards. These cards can be read and written with contact or without contact with the reader. The antenna of the card is used or the contact pads are used to manipulate data. These are used as vending passes, meal passes, access control and network security.
- **Proximity Cards:** The proximity cards are contactless cards and they have an antenna embedded in the card. However, the proximity cards are read only card sand the information on these cards cannot be manipulated. The proximity cards also use the RFID technology. The applications of these cards include access control, identification and security.
- **Hybrid Cards:** These have more than two technologies embedded inside a single card. These cards use any two of the above mentioned types in a single chip. Some applications of smart card require more than two technologies like

The proximity card and the contact card integrated in a single chip.

8.4 Summary

- The IP protocol operates as the third level of the in the OSI reference model. The DNS is a client/server identification application that identifies each individual host on the Internet with a unique user friendly name. All the user names are methodized in a hierarchical fashion in the DNS.
- Electronic commerce or e-commerce is a business activity that occurs over telecommunication networks. E-commerce is a process of buying and selling products, services and information over computer networks
- E-learning (or eLearning) is the use of electronic educational technology in learning and teaching.

A smart card, chip card or Integrated Circuit Card (ICC) is any pocket-sized card with embedded integrated circuits.

8.5 Key Terms

- **Home page:** The first file or Uniform Resource Locator (URL) that automatically loads when a web browser starts or when the browser's 'Home' button is pressed.
- **Bookmark:** A saved link to a web page. If a user visits a particular website or home page and want to be able to quickly get back to it later, you can create a bookmark for it.
- **Web server:** The computer program or virtual machine which serves web pages utilizing the Hypertext Transfer Protocol (HTTP) across the World Wide Web (WWW).
- **IP protocol:** A connectionless type service which operates at the third layer of OSI reference model.
- **Domain name system (DNS):** A TCP/IP application service that converts user-friendly names to IP addresses.
- **DNS server:** A computer that holds information about name space.

8.6 Questions for Exercise

Short-Answer Questions

1. What is the importance of address bar in web browser?
2. What are web services? Name the elements for its platform.
3. What is an IP address?
4. What is domain name system?
5. What is DNS port? How is it classified?

Long-Answer Questions

1. Describe the tools used for various web services.
2. How are web services managed? Describe with the help of an example.
3. Why is IP address configured? What is IPv4 addressing and how is it classified?
4. What is the significance of DNS ports? Discuss its various types.

8.7 Further Reading

ITL Education Solutions Limited. *Introduction to Computer Science*, 2nd edition. United Kingdom: Pearson.

Jaiswal, A. *Fundamentals of Computer and Information Technology*. New Delhi: Dream tech Press.

●●●