Date
Page

Anish Sachdeva
DTU/2K16/MC/13

Computer Network
(MC-308)

Assignment - III

Q1) How does encryption/decryption protect storage or transport of information?

Ans 1) Transport Encryption

The transport layer involves the transport layer security (TLS) certificates, and identity verification. Both the TLS and SSL are cryptographic protocols that provide communications and security over a network.

A properly designed transport protocol can ensure that data, key handshaking, and data integrity verification are encrypted using secure transport protocols such as TLS and SSL. The most common encryption methods we are using in computer networks are mainly based on 3 algorithms: SSL, TLS, HTTPS.

There are many threats in transporting data over a network like an authorized access, availability, spoofing attack, selfish threat, malicious code, Denial of service (DOS), Transmission threats, Routing attacks, Cross site scripting attacks (CSRF) cross site referential forgery attack.

So, by adding encryption, decryption in our network layer, we can ensure that even if someone were to gain access of the data packets we are sending they won't be able to analyze them or comprehend them, as only the receiver (designated receiver) will be able to decrypt the message and understand it.

Storage

When we are storing data either in servers or even of hardware that is directly connected to the BUS of the machine via the PCIE or NVME slot, the data can be first encrypted and then stored so as to make sure that even if the unauthorized parties were to gain access, they won't be able to use the data in any meaningful manner.

Q2) Compress the given data string using LZ coding technique

WEDWEWEEWEBWET

Symbol	Compressed code
W	1
E	2
D	3
WE	4
WEE	5
WEB	6
WET	7

String

WEDIE4E4B4T

Q3) Explain the importance of DCT and quantization for image compression.

Quantization involved in image processing, is a lossy compression technique achieved by compressing a range of values to a single quantum value.

When the number of discrete symbols in a given stream is reduced, the stream becomes more compressible. For example reducing the number of colors required to represent a digital image makes it possible to reduce its file size.

Specific applications include the DCT (Discrete Cosine Transform) in JPEG and DWT in JPEG 2000.

DCT (Discrete Cosine Transform)

The discrete cosine transform (DCT) helps separate the image into parts (or spectral sub-bands) of differing importance (with respect to the image's visual quality).

The DCT is similar to the discrete Fourier Transform (DFT).

It transforms the image from the spatial domain to the frequency domain.

$$DCT[f(x,y)] = F(u,v)$$

$$F(u,v) = \left(\frac{2}{N}\right)^{1/2}\left(\frac{2}{M}\right)^{1/2}\sum_{i=0}^{N-1}\sum_{j=0}^{M-1}\Lambda(u)\Lambda(v)\cos\left[\frac{\pi u(2i+1)}{2N}\right]f(i,j)$$

Q) What are the rules of User Agent and MTA in Electronic mail?

Ans) Mail User Agent (MUA)

A mail user agent (MUA), also referred to as an email client, is a computer application that allows you to send and retrieve email.

A MUA is what you interact with, as opposed to an email server, which transports mail. MUA's can be software applications such as Outlook Express and Lotus notes, or they can be webmail services such as those provided by Yahoo!, Microsoft Outlook and Gmail.

MUA's are component with the Simple Mail Transfer Protocol (SMTP) system responsible for creating email messages for transfer to Mail Transfer Agent (MTA).

Mail Transfer Agent (MTA)

A mail transfer agent (MTA), also referred to as message transfer agent, mail server, or mail exchanger (MX) is a computer program or software agent that sends and receives email messages from one computer to another computer.

Q5] Write a short note on

i] Virtual Terminal

In open systems, a virtual terminal is an application that:

a) Allows host terminals on a multi-user network to interact with other hosts regardless of terminal type and characteristics.

b) Allows remote log-on to local area network managed for the purpose of management.

c) Allows users to access information from another host processor for transaction processing.

d) Serves as a backup facility.

PUTTY is a example of virtual terminal.

ii] Public and Private Networks

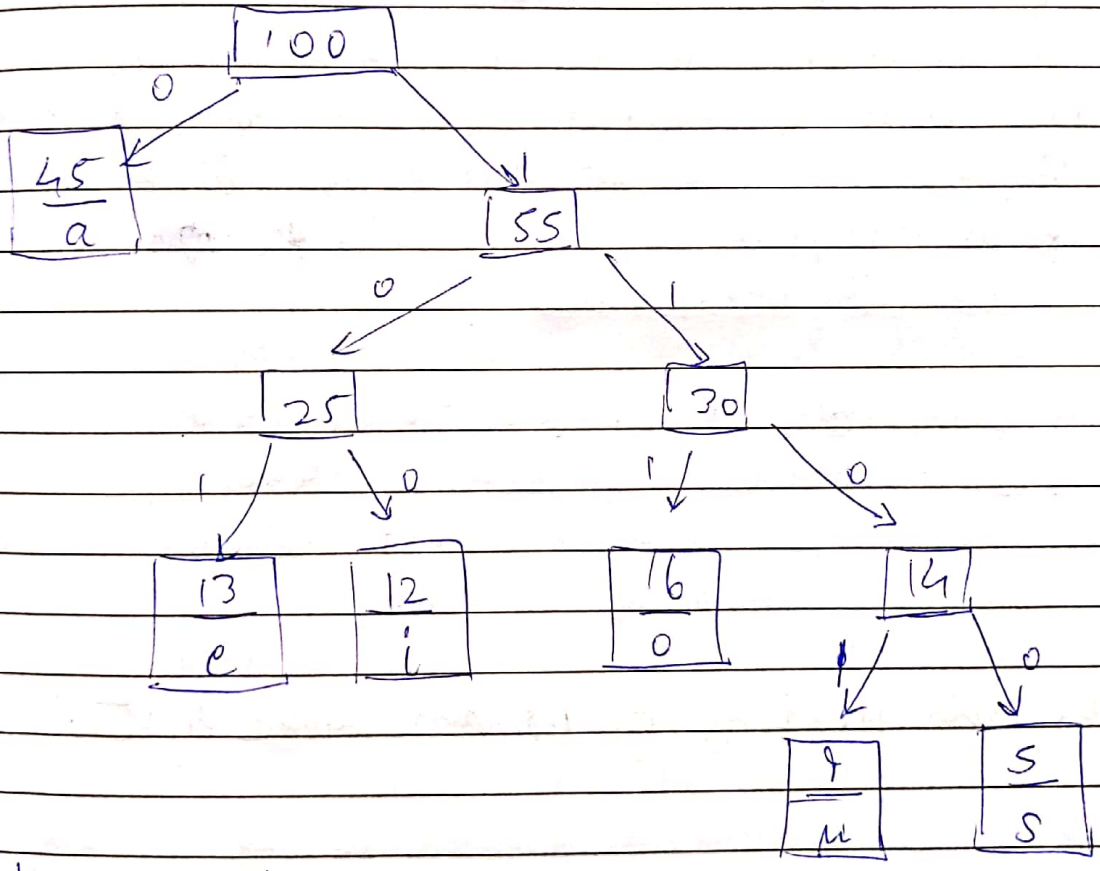
A public network is a network to which anyone can connect. The best, and perhaps only pure, example of such a network is the internet. A private network is any network to which access is restricted. A corporate network or a network in school are examples of private networks.

The main difference between public and private networks, apart from the fact that access to a private

network is tightly controlled and access to a public network is not, is that the addressing of devices on public network must be done carefully whereas the addressing on a private network has a little more latitude.

(b) Perform Huffman Coding on the following set of characters.

Character	a	e	i	o	u	s
Frequency	45	13	12	16	9	5



Huffman Code

Character	Code
a	0
e	101
i	100
o	111
u	1101
s	1100

Q7) State the drawbacks of Lossy compression techniques.

Ans 7) i) Loss of quality - In lossy compression, we lose information that was contained in our image / text / other data and this leads to a degradation in resolution.

A loss in quality can also affect our consumption of media, such as added noise in audio due to loss in quality.

ii) Loss of integrity - A loss in integrity can lead to corruption of files and even a failure to load them. eg. a loss of integrity in a pdf file or a text file can corrupt it and render it unusable. eg. a corruption or loss of integrity of audio file can lead it unplayable.

iii) Computationally Intensive - To compress a file using a lossy compression technique while also retaining all important features requires additional computational power.

Q8) Explain working of Domain name system.

The process of DNS resolution involves converting a hostname (such as www.example.com) into a computer-friendly IP address (such as 192.168.1.1). An IP address is given to each device on the internet, and that address is necessary to find the appropriate internet device like a street address is used to find a particular home.

When a user wants to load a webpage a translation must occur between what a user types into the web browser (example.com) and the machine friendly address necessary to locate the example.com webpage.

There are 4 DNS servers involved in loading a webpage

i) DNS resolver: The resolver can be thought of as a librarian who is asked to go find a particular book somewhere in a library. The DNS resolver is a server designed to receive queries from client machines through applications such as web browsers. Typically the resolver is then responsible for making additional requests

ii) Root Nameserver - The root server is the first step in translating human readable host names to IP addresses. It can be thought of like an index to a library that points to different racks of books.

iii) TLD nameserver - The top level domain server (TLD) can be thought of as a specific rack of books in the library. This nameserver is the next step in the search for a specific IP address, and it hosts the last portion of a hostname. (in example.com TLD is com)

iv) Authoritative nameserver - This final nameserver can be thought of as a dictionary on a rack of books, in which a specific name can be found to its definition. The authoritative nameserver is the last

step in the nameserver query. If the authoritative name server has access to the requested record, it will return the IP address for the requested hostname back to the DNS resolver that made the initial request.

Q7) Explain the kernel activity attribute of an file?

Kernel entered attribute is a way to boost performance of an image file signature validation. It is expensive operation to verify an image's signature. Therefore, storing information about whether a binary, which has previously been validated, has been changed or not would reduce the number of instances where an image would have to undergo a full signature check.

Q8) Why is translation required in the presentation layer for data transmission?

The translation services provided by the presentation layer is important for end systems and end-system applications that use different representations for data. For example text can be represented by a number of different codes (eg. ASCII EBCDIC). If the two sides of a communication use a different encoding, a translation is necessary to avoid corruption of data.

Similarly different hardware architectures use varying representations for numbers (eg. big-end

little-endian) and translation is necessary to ensure correct interpretation by the application.

Note that translation services can also be implemented for more complex data structures (eg. strings, XML content)