CNS - Assignment - 3

1DB18IS098
Vivek V. Hal

① Explain HTTP streaming & UDP streaming in detail:

→ HTTP streaming:

- The video is stored in an HTTP server as an ordinary file with a specific URL
- Here is how it works

① When a user wants to see the video, the client.

② Then, the server responds with the video file, within an HTTP response message.

③ On client side, the bytes are collected in a client application buffer.

④ Once no of bytes in this buffer exceeds a specific threshold, the client begins playback.

Advantages:

① Not costly & complex. ② No firewall problem

③ Refetching video.

UDP streaming

- The server transmits video at a rate that matches the client's video consumption rate.
- The server transmits the video-chunks over UDP at a steady rate
- UDP does not employ a congestion-control mechanism.
- Therefore, the server can push packets into the network at the video consumption rate.
- Typically UDP streaming uses a small client-side buffer.
- Using RTP, the server encapsulate the video chunks within transport packets

- The client & server also maintain a control - connection over which the client sends commands.
- The client & server also maintain a control - connection over which the client sends commands.
- The RTSP is a popular open protocal for a control connection.

Disadvantages:
1) Unreliability 2) costly & complex 3) Firewall Problem.

(5) Explain (or) Mention the protocals for Real - Time Conversation Application Explain RTP.

→ Protocols:
- Real- time applications are very popular for eg:
  ex: VOIP & video conferencing.
- Two standards bodies are working for real - time applications.
  1) IETF & 2) ITU
- Both standards (IETF & ITU) are enjoying widespread implementation in industry products

RTP:
- It can be used for transporting common formats such as
  → MP3 for sound and
  → MPEG for video
- It can also be used for transporting proprietary sound & video format
- Today, RTP enjoys widespread implementation in many products & research prototypes
- It is also complementary to other important real - time interactive protocols such as SIP.

(6) Explain the classification of Network Attacks

Ans: * Active attacks: attempts to alter system resources.

1) Masquerade:

It attack takes place when one entity pretends to be different entity. A masquerade attack involves one of the other form of active attcks

③ Modification of messages:

It means that some portion of a message is delayed or recorded to produces an unauthorised effect.

④ Repudiation:

This attack is done by either sender (or) receiver. The sender (or) receiver can be denised later that he/she has send (or) receive a message.

⑤ Replay: It involves the passive capture of a message & its subsequent the transmission to produce an authorized effect.

⑥ Denial of services:

It prevents normal use of communication facilities. This attack many have a specific target. Another form of service denial is the disruption of a entire network wither by disabling the network or by overloading it by menages so as to degrade performance.

Passive attacks:

It attemps to learn or make use of information from the system but does not affect system resources

① The release of message content:

Telephonic consersation, an electronics mail message. (or) a transferred file many contain sensitive (or) confidential information.

② Traffic analysis:

Suppose that use had a way of masking of info; so that the attacker even if captured the message could not extract any info from the message.

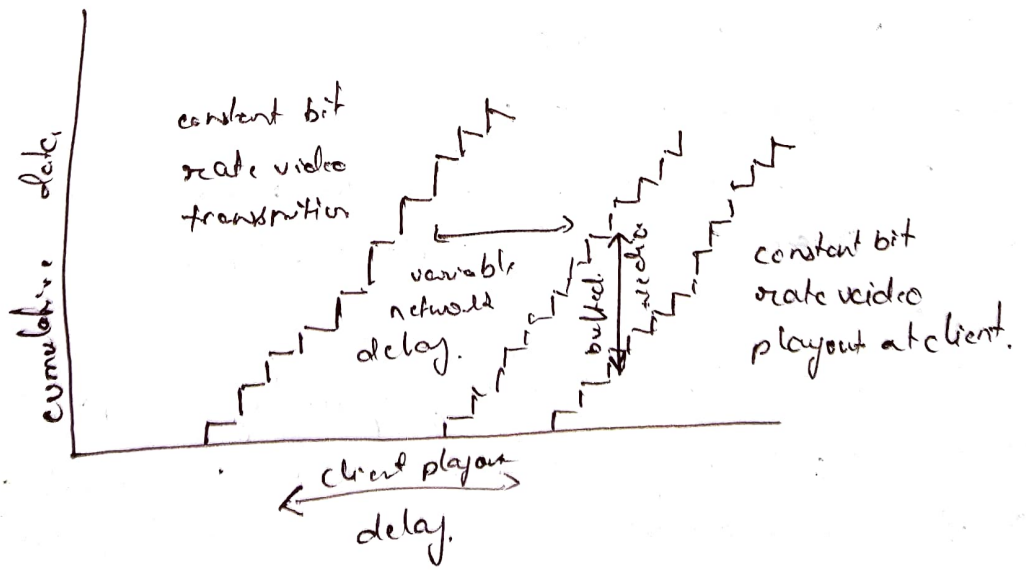
④ What are the examples for Public-key Cryptography? Explain Diffie-Hellman key-exchange protocol.

→ Examples of public-key cryptography

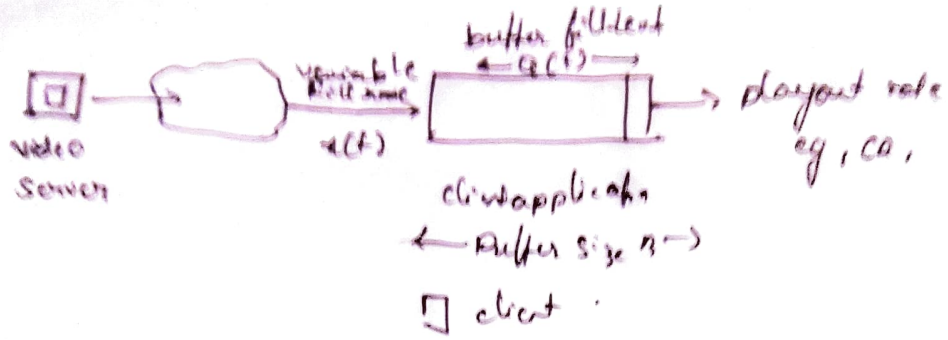
* Diffie-Hellman key-Exchange protocal
* DSS (Digital Signature standard)
* Elgamal
* pailler cryptosystem.
* RSA encryption algorithm.
* Cramer-shoup cryptosystem

Diffie-Hellman key exchanging cryptographic keys over a public channel & was one of the first public-key protocols are conceived by Ralph merkle and named after whitefield Diffie & merkle and ~~named after~~ martin Hellman. DH is one of the earliest practical examples of public key exchange implemented within the field of cryptography published in 1976 by Diffie and Hellman, this is the earliest publicly known work that proposed the idea of a private key & a corresponding public key.

⑤ With graph, explain client playout delay in video streaming.



- client-side buffering & playout delay: compensate for network-added delay, delay jitter



① Initial fill of buffer until playout begins at t_p

② playout begins at t_p.

③ Buffer fill level variable over time as fill rate $x(t)$ varies and playout rate(x), playout rate (r):

* $\bar{x} < r$: buffer eventually empties:
* $\bar{x} > r$: buffer will not empty, provided initial play-out delay is large enough to absorb variability in $x(t)$. Initial play out delay tradeoff: buffer starvation less likely with larger delay, but larger delay until user begins watching.