15-441 Question Set #4

Due: Thursday, May 3rd, 2007 at 23:59:59

April 26, 2007

1 Quality of Service Examples

In the Quality of Service discussions there were 3 different models for applications' bandwidth needs. Provide 2 examples of applications conforming to each model and briefly explain (1 sentence) why they fit the model.

Extra Credit: Give an example of an application that clearly doesn't fit any of the models.

2 Quality of Service Reservations

In RSVP why are bandwidth reservations granted on the way back from the destination to the requester rather than on the way from the requester to the destination?

3 Mobile Latency

(a) Suppose you and your partner transfer a large file between your adjacent laptops in the cluster on CMU's network. How many trips across the internet will each packet and it's corresponding ACKs take?

(b) Now suppose you both go to an onsite interview at your favorite company and the company kindly allows your laptops on the corporate network and, even better, lets your keep your CMU ip addresses using Mobile IP. Suppose you and your partner, once again, transfer a large file between your adjacent laptops in a conference room. How many trips across the internet will each packet and it's corresponding ACKs take?

4 Public vs Private Key

With the advent of public key encryption it might seem that private key encryption should be obsolete as we can have private, authenticated conversations by signing messages with our private key and encrypting them with our correspondent's public key. Frequently, however, this technology is used as a way of exchanging private keys and then a conversation continues using the private keys. Why do we do this? Give two or three plausible reasons.

5 Evading Security

A replay attack is an attack on a server where we first observe a legitimate client authenticate with the server and then replay some of the messages we observed to gain control of the server ourselves.

Alice and Bob have designed the following protocol for authenticating with their mp3 server:

K_{USER} is a private key shared by USER and the mp3 server

client to server: $\{\text{USER}, \text{NONCE}1\}$
server to client: $\{\{\text{NONCE}1\}_{K_{\text{USER}}}, \text{NONCE}2\}$
client to server: $\{\text{SONGNAME}1, \{\text{NONCE}2\}_{K_{\text{USER}}}\}$
server to client: $\{\text{SONG}1\}$
client to server: $\{\text{SONGNAME}2, \{\text{NONCE}2\}_{K_{\text{USER}}}\}$
server to client: $\{\text{SONG}2\}$
client to server: $\{\text{SONGNAME}3, \{\text{NONCE}2\}_{K_{\text{USER}}}\}$
server to client: $\{\text{SONG}3\}$
etc.

(a) How can we use a replay attack to gain access to their music library?

(b) How can we adjust the algorithm to prevent this attack?