

6.263 Problem Set 9

MIT, Fall 2005

Issued: Tuesday, Nov 29

Due: Tuesday, Dec 6

Problem 9.1: Authenticate or Serve?!

Company BAR runs a server that receives jobs over the Internet and executes them. Each job takes $y = 0.01$ seconds to execute. Each job request fits in a single UDP packet. Users interested in executing a job on the server can buy an electronic stamp from BAR using some out-of-band mechanism (whose details are irrelevant to this problem). A user includes the stamp in the same packet as the job request. The server can check that the stamp in the packet is valid, and drop packets with invalid stamps without executing them. Such a check takes x seconds of the server time.

FOO is a competitor of BAR. It wants to degrade BAR's service by mounting a denial of service attack on BAR's server. It sends the server illegitimate jobs that carry invalid stamps. Assume that the arrival rate of legitimate jobs is 100 job/s and the arrival rate of illegitimate jobs is also 100 job/s.

The server has a small queue to contain waiting request messages. If a request arrives when the queue is full, the request is discarded; you can assume that legitimate and illegitimate requests are discarded with equal probability due to queue overflows. Assume that there are always requests waiting in the queue. For each request it takes from the queue, the server decides whether to validate the stamp before executing the job. If the server decides not to validate the stamp, it executes the job immediately. If the server validates the job and the job turns out to be valid the server executes it immediately, otherwise the server discards the request.

Define the goodput of the server as the number of legitimate jobs it serves per second. The server would like to maximize goodput.

1. If the server never checks the validity of the stamps, what will its goodput be?
2. Assume that $x = y = 0.01$ seconds. How often should the server validate stamps if it wants to maximize its goodput? Should it validate every job? every other job? never

validate?

3. If the server validates the stamp of every job before executing it, what will its average goodput be as a function of x ?
4. Consider the following two policies: “always validate” and “never validate”. Which one achieves better goodput when $x = 0.008$? How about $x = 0.001$? What is the value of x at which the server should switch policy?

Problem 9.2 Ben wants to start its own ISP. He obtains a class A sized address space (2^{24} addresses). Before he even installs any machines he notices that his network is receiving traffic. In particular, it is receiving 600 SYN/ACK packets from `www.mit.edu` every minute. Assume that all packets are delivered, all solicit a response, and any attackers using spoofed addresses generate them at random.

1. Describe the attack that is going on.
2. What is the current rate of attack