CptS 464/564
Lecture 15

4th March 2003

Summary

- Finishing chapter 3
- Exam Review
  - Exam from last time the course was taught
  - Your questions
- Reference for secret sharing: A. Shamir. *How to share a secret,* Communications of the ACM, 22 (1979), pp. 612-613

The key observation: a polynomial of degree k is determined by $k+1$ points. To share a secret with n people so that any k of them can gain no information about the secret by conspiring, but any $k+1$ of them can recover the secret entirely, I choose a secret polynomial, P, of degree k so that

$$P(0) = theSecret$$

I hand out "shares" of the secret to as many people as I'd like by giving each one a different point:

$$(i, P(i))$$

for i#0. To recover the secret, any $k+1$ of the points can be interpolated to determine P, which can then be evaluated at 0 (i.e. $P(0)$) to determine the secret.

Example:

My secret is 1437. I want to share it so that any two people can determine the secret, but no individual has any information about it. I choose a degree 1 polynomial, i.e. a linear equation

$$P(x) = -997x + 1437 = ax + b$$

and I give my friends points such as (1,440), (3,-1554), (-9,10410). Then any two of them can determine the equation of a line between their two points, for example, the first and third by solving a set of linear equations:

$$a + b = 440$$

$$-9a + b = 10410$$

$$-10a = 9970$$

$$a = -997$$

$$b = 1437$$

I will *not* ask you about secret sharing on the exam.

RPC (3.6)

Read section 3.6, but we will not cover it in class. Most of the material should be familiar based on earlier discussions about CORBA, but there are a few architectural issues of interest that are addressed here.

Group Communications (3.7) and Distributed Shared Memory (3.8)

We are skipping these sections.

Message Buses (3.9)

The idea of a message bus is that producers/senders and consumers/receivers are decoupled in time and space: messages may be sent at one time and delivered later; also senders and receivers need to know less about one another's identities. (Notice that group communications/multicast mechanism provide some aspect of this latter property).

One use of the message bus idea is in building *publish-subscribe* systems. Publishers (producers/senders) send messages to the bus. Subscribers indicate to the bus their interest in a certain kind of message. The bus delivers the requested messages to subscribers. Publishers and subscribers need not know one another's identities.

Volatile vs. persistent buses: are messages delivered to subscribers that weren't around to receive them when sent? (Temporal decoupling). Yes – persistent bus; no – volatile bus.

Netnews newsgroup as an example of a persistent message bus: messages posted to the newsgroup, not individual subscribers; subscriber doesn't have to be available at the time a message is posted.