Protection (We will not attempt to test every technique known to man — we will come closely along one complete path)

2 Aspects

a. Specification of who may get at a piece of information

b. Enforcement of the specification.

a. (Page 2 of 653 s notes)

Segment (by def) is smallest unit of information separately protected by system.

b. Enforcement (p. 4-8 of lecture)

n.b.: Area of weakness: don't easily protect small information items. (Monitoring is moderately powerful)

E.G., a dossier with a 10 character protected entry.)

But fundamental problem is the negative aspect

1. Specs say "this cannot be permitted" rather than "this must be"
2. It helps merely in natural computation

Certification

Toughest problem of all:

Do all of my mechanisms work the way they are supposed to?

* Negative Specs
* Out of main stream. Dilemma: lots of complicated programs.
  inevitable bugs; potential hardware failures
  no methodical scheme for proof.

Techniques: Make the programs few + simple (Partition them)
Audit them read them over
Concurrency checks
Put in attempts to break down the barriers
at random intervals.
Leave audit trails to help determine
unknown extent of a failure.
Higher level languages (but entrusts the computer too)

Certification is easier if

a. User executes interpretively only
b. User can only type commands.
(Exhaustive testing many times the odds for)

~~c. Hardware does not have pipelining, etc.~~

Hardware features to help configuration

0. No. pipelines
1. Single, standard addressing scheme
2. Asynchronous organization
3. Program readable configuration
4. Program readable clocks