SECURITY

There are two sorts of security, one of which depends critically on the other. The dependent sort is concerned with what goes on while the system is being used, with subjects doing things to objects in the ordinary way. If this is to work at all, though, there is one vital preliminary : we must be able to identify the subjects. In some cases, such as subjects which are part of the operating system, we can do so straightforwardly, but this is not the usual case. Most subjects are not of this sort; instead, they either are, or derive their privileges from, people who come and go.

As we saw in the chapter *LOOKING AFTER PEOPLE*, an operating system in a shared environment must identify people as they log in so that it can give them access to their property in the system. *This is the only identification process*; if during this step you can give information which the system associates with A.B. Smith, then it will give you access to A.B. Smith's property, whoever you really are. All the rest of the security system depends on this step – so it's odd that it's commonly guarded by one of the weakest of the protection mechanisms !

This observation illustrates a general principle : security depends on security. You can't invent security out of nothing – so if your computer hardware doesn't have some built-in security, you can't construct it in the system. In its most primitive form, the hardware security might be a reliable lock on your computer room door, but we usually think in terms which are a little more subtle. The combination of supervisor call and memory protection, both implemented in hardware, is a good start; we met it earlier, in *ONWARDS AND UPWARDS – OPERATING SYSTEMS.*