Software locks to protect computers, microprocessors, and other appliances.

These appliances pose novel problems of physical security against theft.

On the other hand, microprocessor chips are approaching universal use, notably in personal computers. This is a vindication of these machines and appliances.

The concept is to design the processor so that it can be "locked" by the entry of a user-designated password and correspondingly "unlocked". With volatile memory devices, the lock will guard the data with some form of auxiliary memory, e.g., a battery. If the key on the chip is the mechanical setting of a group of switches related to the key on a user's home or office algorithm (The broadcast requirement is a form of biostatistics, allowing some property to be placed "even if the truck blows the sky"), keys would be recorded as data in the normal operation of the device.

As more valuable machines become ever more portable, their security will be correspondingly harder to manage. The advent of small chips that the device is useless if stolen (without the key) should help deter the theft.
If these lock systems with key or magnetic card entry are already in wide use.

This concept is then extended to the microprocessor.

What in that expression is already practical or is non-potential should be investigated.

Many devices may be left controllable, remaining in that condition until power is disconnected.

Only when the device is turned off and the key removed will it be rendered. This approach can then be used to protect a wide range of domestic appliances (e.g., kitchen hand sets, TV, stereo, VCR, radio) from intentional and well as theft mechanisms. Control mechanisms of outlets could also be protected, but new mechanical security designs would be needed against overides by any amount of the control box.

This extension may also help in national security - technical / self-control.
They suggested to Dr. Higfield. He thought it might be reversible. Did it come from care food?