

Module Security Device

The present invention relates to memory modules and in particular to Single In-line Memory Modules (SIMMs) which are used in many common personal computers to extend the dynamic memory of the computer.

5 There has been a remarkable increase in the number of incidents of theft of Single In-line Memory Modules (SIMMs) from computers. SIMMs are an attractive commodity to steal for several reasons:

- they are small and light, which means that there is no difficulty in transporting them;
- 10 - they are easy to remove from a computer system;
- they are interchangeable and largely transparent to the user, so there is no great compatibility problem;
- they are valuable, SIMMs may sell for \$75 each;
- there is a large demand for SIMMs on a world-wide scale;
- 15 - they are hidden from view in operation so stolen SIMMs are very difficult to trace;
- modern software requires a large amount of memory to run so they are becoming more desirable;
- SIMMs are very difficult to secure (physically) from theft;
- many modern offices have a large number of computers, each containing some
- 20 SIMMs which means that there are areas with a large concentration of SIMMs.

Due to the small size and the immediate interchangeability of these devices they are not easy to protect from theft. The SIMMs could be removed from each computer every night and stored in a safe but this is not feasible in a large office because of the trouble involved in removing and reinserting these devices each day.

25 Conventional SIMMs contain a number of memory circuits, frequently DRAM (Dynamic Random Access Memory) circuits, on a small printed circuit board (pcb). On power-up of a computer, the processor within that computer tests whether any SIMMs are present in the appropriate connector slot of the computer. SIMMs do not usually contain any memory management logic or controllers as these would be superfluous. Thus, apart

30 from putting some physical (visible or invisible) mark or tag on each SIMM there would seem to be no way of identifying it. The use of a mark or a tag for security purposes has

a number of disadvantages. It would not stop the use of stolen SIMMs since the mark or tag must be seen to enable identification and detection of the SIMM as stolen. It would not inform the unwary user of the SIMM that the SIMM was in fact stolen. It would be better if there was some method by which any computer could detect that the particular SIMM connected was in fact stolen and then disable operation of the SIMM.

The present invention provides a memory module containing a plurality of memory circuits, a non-volatile memory which stores a code, control means to intercept access to the module on power-up of the computer, such that the correct code needs to be entered to enable the initialisation of the memory module.

The present invention is most suited to memory modules which utilise partial memory circuits because they already have a controller on the module to redirect accesses to faulty locations. If this controller was by-passed then the module would not work. If the invention was used on a standard memory module then the additional controlling means could be by-passed because the additional controlling means are not needed for normal operation of the module. Thus the security measure could easily be avoided on normal memory modules.

The present invention provides a memory module containing a plurality of memory circuits, a non-volatile memory which stores a predetermined code, counting means to count up (down) to (from) a predetermined value on power-up of the module, and control means to disable the module if the predetermined code is not received by the module before the predetermined count is reached.

For a better understanding of the present invention, and to show how it may be carried into effect reference will now be made, by way of example, to the accompanying drawings in which:

Figure 1 shows both sides of a memory module (in this example a SIMM).

Referring to the drawing, Figure 1A shows the front side of the module 1 populated with DRAM circuits 2 and Figure 1B shows the rear of the module which contains a control circuit 3 and a non-volatile memory 4.

It is not necessary to have the control circuit and non-volatile memory on the opposite side of a SIMM to the memory circuits, the control circuit and non-volatile memory could be on the same side of the module as the memory circuits or the system

could be arranged in any other convenient way.

Using a code to disable operation of a SIMM is not trivial. This is because there is a problem in interrupting the host computer which holds the SIMM during its initialisation cycle. The host computer must be allowed to perform the initialisation function on power-up. However, once the memory is initialised it would not be easy to
5 disable it. The present invention overcomes this problem by using a counter which increments (or decrements) on power-up of the module. If the module has not received a certain code or sequence of codes before the counter reaches its predetermined value then the control mechanism on the module disables the module, for example by disabling the
10 data buffer, thus causing an error in the computer.

The counter used may count clock cycles, the number of refresh cycles, the number of read or write cycles or some other operation, for example the number of times that the Column Address Strobe (CAS) goes active (or inactive).

The code or sequence of codes is stored in the non-volatile memory on the module.
15 At the user end of the computer the code or sequence of codes will be entered by the BIOS (Basic Input/Output System) or from software, for example from the initialisation files of the computer. The code or sequence of codes may even have to be entered manually by the user. The code or sequence of codes would be entered in a similar way to a password. The code may even be linked to the keystroke speed, e.g. the "time warped" interval between
20 characters of the user's password.

In some embodiments the non-volatile memory and the control mechanism will be in the same device (an Application Specific Integrated Circuit).

The output of the memory circuits could be disabled by disabling the output enable of these memory circuits or of the memory device.

25 The advantage of the present invention is that the control mechanism waits for the memory module to be initialised before it requires a security code to enable or disable the module.

The code would preferably be entered manually each time the computer was booted-up, although it could be entered using one of the initialisation files (e.g. the autoexec.bat file in a personal computer), but this has the disadvantage that the files can be duplicated
30 and examined to retrieve the code.

An alternative, to avoid this problem is to add the code to a FLASH boot EPROM or encode the file using a password. For example, on installation of the Memory Module a setup or installation program prompts the user for a password, which the installation software encodes along with the key needed to enable the memory security device. A
5 program is then added to the config.sys, autoexec.bat or other initialising batch program to prompt the user for the password, which is then used to decrypt the key file and write this to the controller on the memory module. Failure to provide the correct password would result in the counter timing out and the memory of the computer becoming inoperable.

It will be appreciated that various modifications may be made to the above
10 described embodiment within the scope of the present invention.

Claims

1. A memory module containing a plurality of memory circuits and a non-volatile memory to store a predetermined code **characterised in that** it includes counting means to count to a predetermined value on power-up of the module and control means to disable the module if the predetermined code is not received by the module before the predetermined count is reached.
2. A memory module according to claim 1 **characterised in that** the counter means counts the number of read or write cycles.
3. A memory module according to claim 1 **characterised in that** the counter means counts the number of clock cycles.
4. A memory module according to any preceding claim **characterised in that** the predetermined code is a sequence of codes.
5. A memory module according to any preceding claim **characterised in that** the predetermined code is entered manually.
6. A memory module according to any preceding claim **characterised in that** the control means disables the module by setting the output disable inactive.
7. A memory module according to any preceding claim **characterised in that** the memory module is a Single In-line Memory Module.
8. A computer system including a memory module according to any one of the preceding claims.