Copy protection schema in Emulator I

Important note

Emulator and Emulator I are trademarks of E-Mu Systems.
The information in this document is not based on any official specification of E-Mu Systems and has not been confirmed or approved by this company.
The information in this document is the result of reverse engineering activities on the Emulator I hardware and BootRom images.
The author(s) of the document can not be held responsible for any use of this information or any damage caused by using the information in this document.
The specifications in this document have not been tested thoroughly, and any usage of them are the full and sole responsibility of the user himself/herself.

Log of Changes

Date	Version	Author(s)	Description
11 Nov 2010	0.9	///Esynthesist	Initial version. Based on the contents of some different Emulator I boot rom images (version 820816) and the hardware wiring between the 2708 Eprom and the Zilog Z80 CPU on the Emulator I CPU board.
12 Nov 2010	1.0	///Esynthesist	Corrections made in Introduction section and in section about protection key addresses in boot rom

Introduction

The E-Mu Emulator I uses a copy protection method for accessing floppy disks containing special system software such as the User Formatting disk and the Multi Sampling disk.

Originally all Emulator disks were copy protected, but owners who had more than one Emulator I complained about this, so E-Mu decreased dramatically the impact of this copy protection schema in subsequent operating system versions quite soon after the initial release of the Emulator I.

These protected disks uniquely belonged to the Emulator on which they were created or for which they were created in the factory. This results in not being able to use some floppy disks from Emulator A on another Emulator B.

It is reported that if an Emulator still refuses to load system software from a certain disk, it’s just a matter of write-enabling the disk so that the Emulator can write its protection key to that disk.

So fortunately this copy protection schema is not that important anymore. But the mechanism is still there to some extent… so it was interesting to reverse engineer it.

The protection key in the boot rom

The copy protection is based on a **key** which corresponds to **the serial number of the boot eprom**. Note that this is not the same as the serial number of the Emulator I itself !

The key consists of 2 bytes which are stored in the boot rom. As a consequence, each boot rom is different and has been burned by E-Mu uniquely for a specific Emulator I.
When comparing the boot rom images from two different eproms of the same OS version (e.g. version 820816), 2 to 4 bytes will be different.

- If the eprom is a 2708 1K IC, only two bytes will be different
- If the eprom is a 2716 2K IC, four bytes will be different, but the 2 additional bytes are just a copy of the two other ones.

If you want to burn a replacement boot eprom for your Emulator-I, based on an image of another Emulator-I (e.g. downloaded from the internet), you can simply replace these bytes by the correct ones for your Emulator-I. This can easily be done in a hex editor on a computer.

The protection key bytes can be found on following locations in the boot rom:

- Address 208h (= 520 decimal)
- Address 237h (= 567 decimal)

In a newer 2716 eprom, two additional bytes also contain the same key, because the 2716 eprom contains the 1K boot image exactly twice (so the data from 000h → 3FFh can be found again in area 400h → 7FFh):

- Address 608h (= 1544 decimal)
- Address 637h (= 1591 decimal)

How to determine the value of the protection key based on the boot rom serial number ?

E-Mu was quite inventive in making it hard to “hack” their machine… They didn’t match the numbering of the address and data lines of the eprom with the corresponding lines on the Z80 CPU. The lines (and hence also the bits) are shuffled, so they must be reshuffled again before being able to see data or addresses that actually make sense…

For determining the protection key, the assignment of the data lines between the eprom and Z80 is important. It can be derived from the CPU board that the pins are connected as follows:

2708 eprom Data lines		Z80 CPU Data lines	
Pin	**Databit**	**Databit**	**Pin**
9	0	6	10
10	1	2	12
11	2	0	14
13	3	1	15
14	4	7	13
15	5	5	9
16	6	3	8
17	7	4	7

Based on this table, the serial number mentioned on the label of the boot rom can be translated to the value of the protection key. Here’s an example:

Boot rom labeled “600X.PROM(C) 820816#0197”

The serial number is 0197. This is a **hexadecimal number** and it is the representation of the protection key in the Z80 processor. It consists of:

- Byte 0 = 97h → its converted value can be found on address 237h (and 637h) in the boot rom
- Byte 1 = 01h → its converted value can be found on address 208h (and 608h) in the boot rom

Based on the pin assignment table above, let’s do the conversion now:

Byte 0 = 97h becomes 9Eh in boot rom location(s) 237h (and 637h), as follows:

Databits of Z80 Byte 0 = 97h							
7	**6**	**5**	**4**	**3**	**2**	**1**	**0**
1	0	0	1	0	1	1	1
1	0	0	1	1	1	1	0
7	**6**	**5**	**4**	**3**	**2**	**1**	**0**
Databits of EPROM Byte 237h = 9Eh							

Byte 1 = 01h: becomes 04h in boot rom location(s) 208h (and 608h), as follows:

Databits of Z80 Byte 0 = 01h							
7	6	5	4	3	2	1	0
0	0	0	0	0	0	0	1
0	0	0	0	0	1	0	0
7	6	5	4	3	2	1	0
Databits of EPROM Byte 208h = 04h							

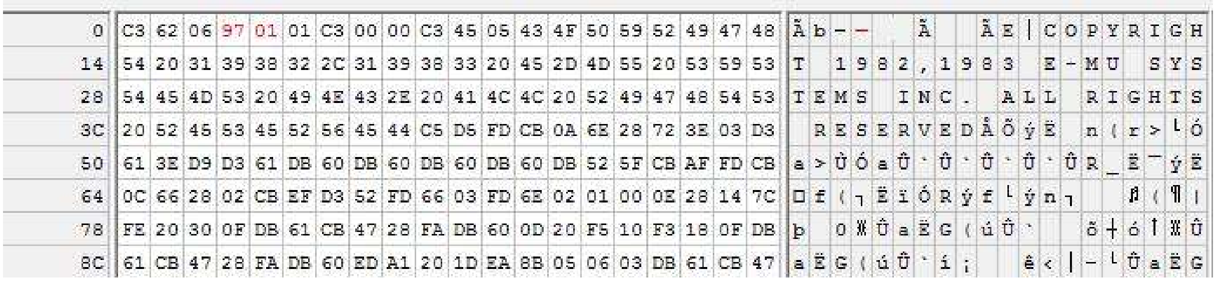
Conclusion: rom serial number #0197 (hex) corresponds to protection key #049E (hex) in the boot rom.

Serial number on system software disks

The copy protection mechanism validates the boot rom protection key against the serial number written to the system software floppy disks of the Emulator I.

The **boot rom serial number** (not protection key !) can be found on the floppy disk in track 00 on position 03h and 04h (counting starts at 00h).
Byte 0 can be found on location 03h, Byte 1 can be found on location 04h.

You can see a dump of part the data of track 00 of a system disk belonging to our boot rom serial number #0197 Emulator here:



```
 0  C3 62 06 97 01 01 C3 00 00 C3 45 05 43 4F 50 59 52 49 47 48  Ãb--  Ã  ÃE|COPYRIGH
14  54 20 31 39 38 32 2C 31 39 38 33 20 45 2D 4D 55 20 53 59 53  T 1982,1983 E-MU SYS
28  54 45 4D 53 20 49 4E 43 2E 20 41 4C 4C 20 52 49 47 48 54 53  TEMS INC. ALL RIGHTS
3C  20 52 45 53 45 52 56 45 44 C5 D5 FD CB 0A 6E 28 72 3E 03 D3   RESERVEDÅÕýË n(r>└Ó
50  61 3E D9 D3 61 DB 60 DB 60 DB 60 DB 60 DB 52 5F CB AF FD CB  a>ÙÓaÛ`Û`Û`Û`ÛR_Ë¯ýË
64  0C 66 28 02 CB EF D3 52 FD 66 03 FD 6E 02 01 00 0E 28 14 7C  □f(┐ËïÓRýf└ýn┐  ♫(¶|
78  FE 20 30 0F DB 61 CB 47 28 FA DB 60 0D 20 F5 10 F3 18 0F DB  þ 0☼ÛaËG(úÛ`  õ┼ó↑☼Û
8C  61 CB 47 28 FA DB 60 ED A1 20 1D EA 8B 05 06 03 DB 61 CB 47  aËG(úÛ`í¡  ê<|-└ÛaËG
```