August 23, 1982

TO: Dave Chandler

FROM: Jerry Comisar
          Jason Soo

SUBJECT: USE OF AN ID ROM TO PROTECT DECADE DISKETTES

In designing a disk operating system (DOS) for the Decade expansion module,
we have an opportunity to enhance the security of the system against
software piracy. The idea is to write a secret number in nonvolatile
memory within each expansion module. A newly purchased diskette would
come with a "Zero" serial number buried in each record header. The
DOS would look for the diskette serial number.   If it were "Zero"
the unique serial number for that machine would be written into
each record header; if it were neither "Zero" nor its own serial
number the diskette would be erased. Thereafter the DOS would always
look for the proper serial number. Thus the user could make
as many backup diskettes as he needed, but they could only be used
on his machine.

The idea of an ID ROM has been proposed before as a security measure.*
In our case, we can build the protection right into the basic
system architecture. In particular we suggest:

1) DOS read-write logic be put in ROM to avoid re-booting.

2) DOS utilities be performed only in the supervisor mode, while game
    software only be executed in user mode. Hence the user is
    shut out of the operating system.

3) All supervisor calls be vectored out of a hardware protected
    RAM page. This can be accomplished by nand-ing together the
    address lines A8-A19, the address strobe AS, and the CPU
    supervisor pin FC2, via the decoding logic inside the expansion
    box, to generate a BERR exception. This denies the user the
    ability to re-write any system vectors.

*See Chris Morgan, "How Can We Stop Software Piracy," BYTE, May 1981,
 Page 6.

The ID number ROM would not need to be given a unique part number. In fact, the unique serial number could be blown in during the last stages of board manufacture, even during automatic test or burn-in. If a non-volatile memory device is included in the system for high score record keeping, it could also share the ID function; however, to protect security we would need to restrict all writing to that device to protected supervisor calls.

This protection mechanism would not be a restraint against non-Mattel software, since DOS could look for the Mattel copyright notice before enforcing protection.

No security measure, including this one, can prevent the sophisticated pirate from doing a nibble copy of any protected diskette. However, by clever DOS design one can deny the pirate the use of a Mattel machine to perform his dastardly deeds. Furthermore, one can complicate things enough to frustrate the use of a personal computer and common copy utilities such as ZAP.*

*See Don Worth and Pieter Lechner, "Beneath Apple DOS", Quality Software, 1981.

JC/bb

cc: D. Hostetler
     L. Pumphrey