Permanence and Security of Data using WORM technology

Robert Milton Underwood, Jr.

Permanence and Security of Data using WORM technology

In an increasingly competitive business world, where the prudent utilization of advances in technology can give a competitive edge, more companies are becoming concerned with permanent data storage and data security issues. Some companies have chosen the write-once-read-many (WORM) technology as the ideal storage solution (Peebles, 1998). A WORM memory device allows an author to store prepared files once into memory so that others may read, but not alter, those files (Jensen, 2000).

There are two basic types of disks, magnetic disks and optical disks. On magnetic disks, data is encoded as microscopic magnetized needles on the disk's surface and the data can be added and erased many times. Several forms of magnetic disks are floppy disks, hard disks, and removable cartridges.

Optical disks record data by burning microscopic holes in the surface of the disk with a laser. The process involves placing a thin aluminum film between two glass or plastic platters (Silberschatz & Galvin, 1999). The laser light perforates the aluminum by burning small holes. The holes in the aluminum cannot be reversed, and each part of the disk can only be written onto one time. To read the disk, another laser beam shines on the disk and detects the holes by changes in the reflection pattern. A WORM disk is one of the three basic forms of optical disks[1] (ZDNet, 2000). A special WORM disk drive is needed to write data onto a WORM disk.

WORM technology can be used with optical CD-type disks as well as with tapes. In 1998, a company called Storage Technology Corporation (StorageTek) announced beta testing of its WORM products, which used tape technology. The tape technology provides that the tape be housed in a notched casing that does not allow the data to be overwritten. These products were

[1] The other two basic forms of optical disks are CD-ROM disks and erasable optical (EO) disks.

targeted to information technology (IT) customers who require large volumes of secure, inerasable data. To provide logical security, StorageTek micro code is incorporated into the tape drive electronics, and bit settings on the tape itself also prevent overwrites (Pendery, 1998). An additional security bit is set each time data is written to tape by the IT customer, who is only able to write additional data onto blank areas at the end of the tape's last data file.

The WORM technology in tape format saves users money when compared to optical disk technology. StorageTek's tape storage costs only about one cent per megabyte, compared with eleven cents per megabyte for 12-inch[2] WORM optical disks, and 9 cents per megabyte for 5.25-inch optical disks (Kovar, 1998). However, despite the cost savings of WORM tape technology, for data that must be kept for many years, possibly for many decades, WORM technology with optical disks is considered more durable than with magnetic tapes.

Security is not the only reason that WORM technology is needed. Generally speaking, as computer technology progresses at an increasingly rapid pace, hard drive storage capacity is also increased. Only a few years ago, a hard drive on a personal computer with 300 megabytes (MB) of hard drive space was considered substantial. Now, a hard drive with ten times that capacity may not be enough for some users. As hard drive storage capacity increases, the user seem to *need* more capacity. However, hard drive storage may not be convenient and practical for users who wish to store, and later retrieve, important data. WORM disks and tapes allow users to store huge volumes of data without having to deplete hard disk storage. The capacity of WORM disks is very important for users. WORM drives with the 12-inch optical platter format can easily hold over 6 gigabytes (GB) of data (Starrett, 1997).

[2] According to Glatzer (2000), there are only two major companies in the drive business at this time: Plasmon, who manufactures 12-inch disks, and Sony, who manufactures 5.25 inch disks.

Application programs have become larger as they have advanced throughout the years. According to Starrett (1997), the text of a 3,000-word magazine article takes up about 21 kilobytes (KB) as ASCII characters. But in Microsoft Word 6.0 for Windows, which embeds formatting commands and other invisible characters, the same 3,000-word article would take up 37 KB of space. If high-quality graphics or high-resolution photos are added to the article, its size can grow immensely, possibly too large to fit on one 1.44 MB 3-inch by 5-inch floppy disk.

External storage media have become useful for mobility. It is usually not convenient to take a hard drive to numerous physical locations, but it is easy to take a floppy disk, an Iomega® disk, or a WORM disk. What distinguishes WORM technology from other portable storage media is that the information cannot be overwritten, thereby providing certainty that important data will not be lost.

WORM drives for recording have never really become popular with the small PC user. Perhaps the main reason is cost, at up to $2,300 or so per drive. For some applications, especially those that have legal or regulatory requirements for data permanence, WORM systems are considered indispensable by users for whom data permanence and security are paramount, and for whom price is not an issue.

There are many potential users who would and do benefit from the security and data permanence that WORM technology provides. The United States Securities and Exchange Commission (SEC) has strict regulations for record keeping and archiving, requiring that such be “nonerasable and nonrewritable” (Kovar, 1998). Prior to the availability of WORM technology, only microfiche and paper records were used at the SEC.

There are many practical uses of WORM technology in sundry industries where security is paramount. For instance, bank personnel can use the technology to take pictures of bank

customers, to be stored on a WORM disk. Then, on subsequent visits to the bank, customers can transact without having to be asked for photo identification each time. Once the account number is entered, the teller's terminal will render an image of the customer along with other account information.

Another possible use of WORM technology for purposes of security is at prisons and jails. While officials at these institutions have long kept photos of inmates on file, they may also find it prudent to take pictures of visitors of inmates. This process would allow officials to keep records of the specific visitors that inmates have, and can ensure that the individual leaving the institution is actually the visitor and *not* the inmate.

Those in the fields of science can find WORM technology very helpful, especially in instances where permanence of data is of paramount importance. Meteorologists, oceanographers, and astronomers need to be able to store huge volumes of historical data for future reference.

Huge volumes of law books can be written on disks using WORM technology. With this convenience, attorneys and legal assistants can work far away from the office and still have historical records and case studies close at hand.

The airline industry can benefit from having access to data that is permanently recorded and easily accessible. Detailed data about aircraft crash histories, subsequent follow-ups, and conclusions can be stored on WORM disks so that data can be easily accessed and studied to prevent future crashes.

Another instance of a use of WORM technology where permanence, rather than security, is important, is with the print media. Newspapers and magazine articles can be archived with

WORM technology. This may make it easier for individuals to get historical reports than by going to a local library to sift through microfiche sheets or reels of microfiche tapes.

A use of WORM technology where both permanence and security of data is important is with shipping and/or delivery industry. Some transport and package delivery companies are now taking and keeping signature-images as proof that the recipient accepted the delivery (Glatzer, 2000). The signatures are captured on hand-held devices and downloaded into servers that store the images on WORM media. This practice can ensure that the recipient was the intended recipient, and can prove that the delivery was indeed received.

The data on WORM disks can only be as permanent and secure as the user-protection systems will allow. Silberschatz and Galvin (1999) wrote that data can be destroyed on a WORM disk by burning holes everywhere on the disk. Protective measures must be taken so that the WORM disk-writing drives are not abused. Even if the WORM disk itself is sound from damage or data destruction, it is possible to download files on WORM disks into hard drives and make revisions that can then be recorded on a new disk (Jensen, 2000). Managers of companies that use WORM technology should be conscientious of the systems they set in place to protect the disks themselves and the data the disks contain.

Potential users of WORM technology will probably increase in the future, and more competitors may enter the WORM drive industry. As with most advances in computer-related technology, costs typically lower and stabilize after their initial introduction into the market. Although costs may be higher for creating WORM disks or WORM tapes than with the magnetic recording of data in the nonsecure and nonpermanent read-write format, cost is not necessarily a concern for certain users. For any company that wants a system to either (a) ensure the security

of its data, or (b) ensure the permanence of its data, or both, WORM technology should be considered.

References

Glatzer, H. (2000, March). WORM Enables Some Unusual Apps. Computer Technology Review. [on-line].

Jensen, B. (2000). Technology glossary. [on-line].

Kovar, J. (1998, July 20). Storage Tek bets on WORM—Technology will replace optical discs in some arenas. Computer Reseller News. [on-line].

Peebles, M. (1998, December). Safeguarding data with WORM: Technologies, processes, legalities, and standards. Computer Technology Review. [on-line].

Pendery, D. (1998, July 20). Storage Tek breaks out unerasable tape technology. Infoworld. [on-line].

Silbershatz, A. & Galvin, P. (1999). Operating systems concepts (5th Ed.) (pp. 456-457). New York: John Wiley & Sons.

Starrett, R. (1997, October). In search of secondary storage: from MO to WORM to CD, the fastest and vastest in the field. Emedia Professional. [on-line].

ZDNet, & internet.com Corporation. (2000). [on-line].