The Techniques and Challenges of Immutable Storage with Applications in Multimedia*

Ragib Hasan[†‡] Joseph Tucek[†‡] Paul Stanton[†‡] William Yurcik[†]
Larry Brumbaugh[†] Jeff Rosendale[†] Roelof Boonstra[†]

[†] National Center for Supercomputing Applications (NCSA)
[‡]Department of Computer Science
University of Illinois at Urbana Champaign

ABSTRACT

Security of storage and archival systems has become increasingly important in recent years. Due to the increased vulnerability of the existing systems and the need to comply with government regulations, different methods have been explored to create a secure storage system. One of the primary problems to ensuring the integrity of storage systems is to make sure a file cannot be changed without proper authorization. Immutable storage is storage whose content cannot be changed once it has been written. For example, it is apparent that critical system files and other important documents should never be changed and thus stored as immutable. In multimedia systems, immutability provides proper archival of indices as well as content. In this paper, a survey of existing techniques for immutability in file systems is presented.

Keywords: immutability, secure storage, archival system, WORM.

1. INTRODUCTION

Immutability refers to the property, which, once applied or given to an object, prohibits any subsequent changes to that object. In terms of file systems, immutability refers to preventing any changes or modifications to the contents of the file [1]. The primary goal of achieving immutable storage is to attain the capability of assigning the immutable or unchangeable attributes to specified file objects.

Multimedia is one of the prime application areas for immutable storage and archival. In most cases, multimedia objects, once created, are not changed or altered afterwards. In particular, multimedia can be considered to be a good target for immutable storage systems because multimedia objects are frequently created, distributed, and in most cases are not supposed to change other than through appending. Hence, incorporating the immutable attribute to multimedia objects would enable unaltered storage for critical information.

In view of copyright and intellectual property legislation, it has become necessary to verify and ensure the authenticity of many multimedia objects. Immutable storage systems provide this important protection to documents and objects that render them impossible to change or modify, thereby ensuring their integrity.

In the recent years, the proliferation of the Internet has opened new opportunities in multimedia content distribution and storage. At the same time, this has given rise to increased levels of unauthorized intrusions and attacks into computer systems. In most cases, intruders gained root level access to systems making the storage prone to modification and malicious tampering. The impact on multimedia is the illegal serving of copyrighted content from compromised machines referred to as 'zombies'.

* This work is supported by a grant from the Office of Naval Research (ONR) under the auspices of the Technology, Research, Education and Commercialization Center (TRECC) "Storage Security" Project 2004-2005.
Author emails are *{rhasan, tucek, pstanto, byurcik, ljbrumb, jeffr, roelof}@ncsa.uiuc.edu*

Along with immutability, tamper-resistance is another vital aspect of data protection and authenticity. In [2], Haubert et al present a comparison between tamper-resistant storage and immutable storage. Tamper-resistance and immutability are two closely related but independent techniques in providing data security. Unlike immutable storage which prevents any changes to data once it has been written, tamper-resistant storage does not provide complete protection against modification. Rather, it provides verification about the integrity of data through hashes or cryptographic signatures. Tamper-resistance also involves detection of any modifications to data. To summarize, immutability prevents changes while tamper-resistance makes sure that any changes would not go unnoticed.

The necessity of immutable storage is also reinforced by Federal and State regulations regarding storage security. In particular, the following legislations [3] imply the need for a secure technology for preventing data theft and loss due to intrusions. Table 1 contains an overview of the most important Federal and State regulations that affect storage security:

Health Insurance Portability and Accountability Act of 1996 (HIPAA) [4]	Mandates confidentiality, integrity and availability of patient and other medical records and requires healthcare providers to secure the stored records.
SEC 17A-3 and 17A-4 [5]	Requires financial entities to retain client correspondence and all electronic records preserving integrity for auditing.
Gramm-Leach-Bliley Act	Requires financial entities to disclose policies for protecting confidential customer information and ensure security and confidentiality while preventing unauthorized access.
Sarbanes-Oxley Act [6]	Ensures accuracy and reliability of corporate disclosures by requiring corporate officers to validate integrity and accuracy of financial records.
California State Law SB 1386	Requires all state agencies and businesses that store client information to promptly disclose security breaches.

Table 1. Federal and State Legislation Affecting Storage Security

Immutable storage can have a crucial role with archived data. There is a significant difference between backing-up data and archiving data. Archived data is not used for traditional back-up purposes or disaster recovery. Rather, it is data that is to be kept for a long period of time and remain in a specific state during that time. It is sometimes referred to as fixed-content data. Formerly corporations determined how long to keep archived data, but now regulatory compliance requirements, as shown in Table 1, dictate the retention periods for various types of data. They also specify the manner in which the archived data is to be maintained and accessed. For example, SEC Rule 17A-4 [5] specifies the very stringent requirements for archived Email and instant messages for SEC members. Active deletion can take place after seven years. One archived copy needs to be kept offsite, in addition to a local copy. The data needs to be stored on non-rewritable, non-reusable media. Writes need to be verified. In addition, archived data has a recovery time objective associated with it. This is the time period in which specific data can be retrieved. This period usually requires that an index structure be employed to locate specific data, because a sequential search will take too long. Finally, SEC 17A-4 requires an audit of all activity in the message store.

There has been a shift in the broadcast industry to use computer-based video recording and editing equipment because of the cost effective solutions and the manageability of large quantity of data. There is a multitude of processes from the recording to broadcasting of multimedia and video data. The first process that was affected by the move to the digital world was seen in digital video editing in the 1980s. Now, all major studios use digital editing suites. An abacus letter generator used to cost $89000 in the 1980s. Now it is possible to apply hundreds of effects for only the price of a commodity PC and some software. U-matic is rarely used and most studios are moving away from expensive Betacam systems. The move from analog to digital broadcast video is about to expand into the consumer arena. The demand for digital cameras for use in broadcast environments has expedited the development of these cameras to the point that both Panasonic and JVC came out with a HDTV camera for under $3000. Even though general consumers are not concerned with copyrights, it is a clear example of the increase in demand for secure disk space.

Consumer requirements for high quality television have generated the demand for HDTV. Beyond the requirements for more and larger data formats, in the near future the requirements for fast on-demand and secure copyrighted materials will exponentially increase by the move from push to pull technologies in the television arena to provide interactive on-demand programming. Both push and pull digital technologies will replace many of the current analog television broadcasts because of the extended reach and markets that these technologies will and already do provide. With solutions for scalability like MPEG-4, live and on-demand transmissions can now be received worldwide on TV, computer, notebook, PDA and cell phone. The scope will increase even more when high speed broadband becomes available via 802.16 implementations.

The growth of digital data all around the world is going to continue to increase and with this also requirements for secure and on-demand data storage will grow in parallel. In this paper, the different methods of incorporating an immutable storage and archival system and its corresponding applications in the multimedia domain are explored. The rest of the paper is organized as follows: the motivation for immutable storage in the context of security is discussed in Section 2. In Section 3, a brief review of WORM research is presented. Section 4 provides a survey of the existing immutable storage techniques. In Section 5, the challenges in implementing immutable storage are explored. Section 6 compares existing immutable systems based on their characteristics. Next, the implications and application of immutable storage to multimedia applications is discussed in Section 7. Finally, Section 8 concludes.

2. MOTIVATION FOR IMMUTABLE STORAGE IN SYSTEM SECURITY

Security of computer systems has always been a major issue. With the proliferation of the Internet, the additional connectivity has given rise to an increase in intrusions into systems. Unfortunately, the standard security policies and mechanisms provided by mainstream operating systems fail to prevent most of these intrusions. In [7], Loscocco et al discuss the mistaken assumption that adequate security can be provided in applications when existing operating system mechanisms are inherently flawed. In many cases, even the most secure operating system can be broken into, and intruders can render irreparable damages to the data. As described in Section 1, many types of records used in business, health care, law etc are required to be unchangeable; therefore, protection from possible tampering or deletion of such records needs to be ensured. In the recent years, electronic records are deemed suitable in legal proceedings [8], and hence need to be stored in a way that ensures their authenticity.

System penetration, in turn, gives rise to the problem of data security. The number of Internet security incidents is approximately increasing more than 100% per year [9]. Also, in a series of penetration tests, it was found that 88% of attempted penetrations were successful and, 96% were undetected and 95% of detected penetrations were not handled at all [9]. In [10], Blakley describes the inapplicability of the traditional security models in post-Internet computing. This concern is also expressed in [11]. The recent spring 2004 break-ins into highly secure computing facilities at NCSA, San Diego Supercomputer Center, Stanford University as well as other institutions of the TeraGrid highlight this threat [12]. It is especially alarming that the intrusions occurred in high performance systems where the intruders could have destroyed years of research data.

What makes matters worse is the fact that intruders have become smarter and commonly cover their tracks by deleting system logs [13] and installing sophisticated ‘rootkits’[14] which hide files, processes and connections. Even in highly secure systems, the access control policies can be bypassed when the intruders assume the identity of the system administrator [15]. Recovery from such intrusions is expensive, time consuming, and in most cases, may lead to dire consequences like the loss or modification of vital data.

However, integrity of data is not the only concern. System intrusion is facilitated in most cases through the use of widely available exploits. Intruders gaining access to a system modify the system files and install their own, compromised binaries [14]. It is very difficult to detect systems compromised in this manner, as the very tools for intrusion detection are modified. If the intruder can masquerade as the system administrator, most software techniques aimed at protecting data and critical system files can be bypassed.

Immutable storage provides a solution to the problem, both for critical system files, and for data that does not change. Intrusions may still occur, but in a system where the system binaries are protected in immutable storage, the damage would be less and the efforts to restore the system would be easier for administrators.

3. LITERATURE REVIEW

Most of the research on immutable storage systems is designed using hardware-based techniques. These are discussed in Section 4. In this section, the important research projects on immutable storage are reviewed.

Most of the earlier immutable storage systems involved the use of optical storage. However, these were more focused on backup than on implementing a general purpose immutable storage for system files and data. The File Motel [16] uses a WORM device for storage of backup copies, but is very slow. It maintains a database on magnetic disk to index the files in the WORM device. Optical File Cabinet [17] implements a block oriented storage using optical disks. Using a logical address space which is smaller than the WORM device capacity, it maps logical block numbers to unused physical WORM addresses when a block is written. Russo et al describes an operating system independent WORM archival system in [18]. Based on optical disks, this WORM has been used to archive data received from the Hubble Space Telescope. Quinlan [19] describes a general purpose file system using a WORM optical disk accessed through a magnetic disk cache. Use of the cache provides faster access and write performance.

Plan 9 from Bell Labs [20] uses an optical WORM based backup storage. It includes a magnetic disk based cache mechanism that enables faster file access while accumulating changes to be subsequently written to the jukebox. Later versions of Plan 9 use Venti - a network storage system that applies a unique hash of block contents to identify blocks, and hence implements the WORM storage in magnetic disks [21]. It provides a simple protocol for client applications to read and write blocks of archival data. Read-Only Secure File System (SFSRO) [22] uses the same approach for block identification. However, the emphasis in SFSRO is on security and scalability. It ensures authenticity of data using digital signatures. In contrast, the Stanford Archival Vault [23] uses content based hash on digital objects for implementation of immutable storage. Any modification to a stored object is treated as corruption, and the object is automatically replaced with an unmodified replica. It allows changes only in form of version chains with each version of an object pointing to the previous version. Aprvrille et al describe a timestamp based virtual WORM system in [24]. The system is based on chained hashing, secure time stamping and digital signatures. The advantage of this approach is the additional capability of detecting tampering of data. Distributed Information Storage Protocol (DISP) [25], based on the INDIA protocol [26] from Ellard et al uses a secure distributed client/server based protocol to manage storage of immutable data objects. Use of unique write handles or certificates allow writing only new objects while maintaining the integrity of older objects.

Self-securing Storage [15] from Carnegie Mellon University addresses the problem of system intrusion in detail and uses versioning and an immutable storage mechanism for storing system logs. Self-securing storage devices audit all requests internally. Old versions of data are retained for a window of time, irrespective of operating system commands. The Elephant file system [27] has detailed support for versioning and has a user-definable policy for keeping file versions across changes. Rather than modifying data, it creates a new version while keeping the old version unchanged. In contrast, Fast and Secure Magnetic WORM [13] implements immutable storage on magnetic disks by means of modified block device drivers and disk firmware. The system is built using cheap commodity magnetic disks with special device drivers or firmware that allow only read and append access to data.

4. SURVEY OF EXISTING TECHNIQUES

As storage system security concerns increased, researchers developed a number of approaches towards solving this problem. [13] presents a classification of Write-Once-Read-Many times or WORM technologies. [28] also presents a taxonomy of current WORM technology. According to [28], WORM devices can be classified into 3 main categories:

- Physical WORM technology or P-WORM
- Embedded WORM technology or E-WORM
- Software WORM technology or S-WORM

Each of these three categories are now discussed including their advantages and disadvantages.

4.1 Physical Immutable Technology

Also known as P-WORM, the physical storage technologies include media that is by nature immutable and unchangeable. The advantage of this type of WORM devices results from this physical immutability which renders them impregnable against malicious changes. Two different technologies – optical and magneto-optical –are widely used and available from different vendors in this field.

4.1.1 Optical WORM

The most popular type of physical WORM is the optical WORM. Examples include CD-R and DVD-R. Before the advent of these P-WORM technologies, [21] discusses the use of Optical jukeboxes in building read-only or append only storage and archival systems. These optical jukeboxes combine several optical drives with multiple WORM disks.

Optical WORM device capacity has increased ever since their introduction in the mid eighties. From several hundred megabytes, optical WORM capacity has progressed to gigabyte amounts in recent years. With DVD-R media, the capacity of 5.25" optical disk storage has increased to more than 17 GB. [29] discusses Ultra Density Optical (UDO) disks with capacities of more than 30 GB. Research is already underway at HP and Plasmon to develop UDO disks with capacities greater than 120 GB by 2007.

With Optical WORM disks, the access times are much better and faster as accesses can be random and non-sequential, unlike tape storage. However, data transfer rates are somewhat slower when compared to tape.

4.1.2 Magneto-Optical WORM

Magneto optical disk storage operates on the principal of changes to the magnetic properties of certain media at particular temperatures. Heating of the surface is controlled optically using a laser. The media can only be written when heated to a particular temperature range. Magneto-Optical media has the advantage over Optical WORM because it tolerates mechanical damages to the media far better than optical disks. Reading occurs at speeds of magnetic disks. Currently available Magneto-optical disks have capacities up to 9 GB.

4.1.3 Advantages and Disadvantages of P-WORM

The greatest advantage of P-WORM technology is its widespread adoption by different vendors. CD-R and DVD-R are almost ubiquitously available. Similarly, magneto-optical disks are available from different vendors. The mass marketing, research and development into P-WORM have also lowered its price, compared to other WORM technologies.

The major problem with Optical P-WORM devices is that write operations are extremely slow when compared to their magnetic counterparts. In addition, the capacity of each physical media is relatively small. For example, a CD-R usually can contain about 700 MB of data. A DVD-R has much higher capacity (>15 GB) but that is still lower than the requirements of many of the recent data intensive high resolution multimedia applications. Optical jukeboxes [21] have implemented multiple media based optical platters. Finally, management of a large number of media disks proves to be a big problem.

4.2. Embedded WORM Technology

In embedded WORM or E-WORM, device driver and firmware work together to implement an immutable storage system. This approach is very popular and many large storage vendors have come up with proprietary storage solutions incorporating E-WORM. Some of these are magnetic tape based while others use magnetic disk.

Magnetic tape WORM involves a combination of tape storage and firmware based protection techniques. Commonly used tape is not usually write-protected, so this requires specialized tape drives with embedded write protection mechanism. Individual tapes can be identified as read-only or read/write. Magnetic disk WORM is a relatively new technology that uses the disk firmware to add protection mechanism to magnetic disks. Tape libraries are somewhat similar in nature to the optical juke boxes. In the same way as optical jukeboxes access multiple optical WORM media,

tape libraries combine multiple WORM tapes to provide a larger storage system. The EMC product Centera [30] and the Network Appliance product NetStore/Snaplock [31] are two examples of embedded WORM technology based on hybrid firmware/software approach.

4.2.1 Advantages and Disadvantages of E-WORM

E-WORM devices have larger storage space available per tape or magnetic disk. Also, faster write operations are performed than with optical media. Considering the capacity, the cost is comparatively small. A major disadvantage of E-WORM is that magnetic media is prone to problems related to physical damage. WORM tapes are not recognized or usable with non-WORM devices. Also, magnetic tape WORMs allow only sequential read/writes but not any random access to the contents. Finally, intruders with physical access to magnetic WORM tape can damage the tape and destroy the contents

4.3 Software WORM Technology

In software WORM or S-WORM, the operating system provides protection using mechanisms like capability-based schemes or modified file systems. Beyond the basic file access permissions, Unix™ provides a mechanism for indicating system files and directories immutable. System utilities like *chattr* and *lsattr* [32] can be used to set the immutability flag and render a file impossible to modify even with root access. However, this approach can be circumvented when an intruder gains root access and removes the immutability flag, making changes or deletion possible. Also, after gaining root privileges, an intruder can modify the kernel behavior to bypass checks for the immutable bit, rendering this method unusable in practice.

Linux Intrusion Detection System (LIDS) [33] provides immutability by modification of inodes and is based on the Virtual File System (VFS). LIDS is a Linux kernel patch that allow many of the all-powerful root privileges to be revoked. Therefore, an intruder who has gained root privileges cannot perform many activities used for exploiting the machine. To restrict the root user to change the immutability bit, LIDS can disable the capability CAP_LINUX_IMMUTABLE. This capability allows modification of the immutable and append file attributes. LIDS also can prevent rootkits that use Linux Kernel Modules (LKM), by allowing only loading of LKMs until the kernel is sealed by LIDS[33]. In addition to these, LIDS can enforce access control list or ACLs on file system objects. By enforcing the DENY, the existence of an object would be denied. By using READ, the object would be available read only and cannot be modified. A problem with using LIDS is that, all the above features are implemented using the Linux VFS. An intruder can still modify or delete a file by using the raw disk interface, circumventing the ACLs enforced by LIDS. To solve this, LIDS can be used to disable the capability CAP_SYS_RAWIO. This would prevent any raw access to storage devices.

4.3.1 Advantages and Disadvantages of S-WORM

A major advantage of software-based WORM technology is that it is simple to implement and integrate with existing operating systems. A disadvantage of S-WORM solutions is that they all depend on the file system code to incorporate security. Anyone with root privileges could bypass the file system and access the physical media. Also, intruders who gains root access to a system have almost complete control over memory and can bypass any software based immutability mechanism.

5. CHALLENGES AND DIFFICULTIES IN IMMUTABLE STORAGE

Developing immutable storage has been one of the prime objectives of the storage research community in recent years. However, efforts towards building ubiquitous immutable WORM storage system are hindered due to the various difficulties inherent in contemporary approaches to solving this problem. In this section, some of the basic problems of immutable storage are discussed.

5.1 Storage Capacity

Capacity of immutable storage depends on the technology involved to implement the storage system. Magnetic tape storage traditionally has the highest capacity. Optical storage devices do not have as much capacity. With the introduction of large data centers, the amount of data that needs to be stored in an immutable manner has also increased

exponentially. [34] shows that in 1986, NCSA mass storage facility required only 36 gigabytes of storage, whereas it uses several petabytes at present. The amount of storage at NCSA increased almost 88% between 1997 and 2001.

5.2 Data Throughput

Data throughput is a major concern with real time applications. Both read throughput and write throughput need to be considered. In the context of immutable storage, write throughput refers to the speed of writing to the media. Optical media is inherently slower than magnetic media when write throughput is considered. Magnetic media provides faster speeds. Other factors which effect write throughput is the complexity of implementing immutability. In software WORM, there is an additional layer of computation required to enforce immutability, which may be a bottleneck. In case of read throughput, magnetic media obviously outperform optical media. A significant disadvantage of magnetic tape is that it only allows sequential processing.

5.3 Management Overhead

In any data storage facility, the management overhead soon overshadows everything else. With current data centers storing petabytes of information, management overhead is certainly an important issue. In [35], Uttamchandani et al discuss the impact and extent of this growing management problem, and state that as system capacity increases, the load on administrators increase rapidly. This increase in management overhead leads to longer backup windows and complex security scripts to be specified by administrators. When performing immutable storage or backup with removable media, the difficulty in integrity verification, storage and archival of the media often overwhelms other critical activities. The ideal immutable storage needs to have very low overhead in managing the storage process.

5.4 Security

Most software based techniques are inherently insecure in the sense that when operating systems get compromised, it is extremely difficult to ensure security of storage systems. Use of firmware based techniques provide additional security, but complicates system design. Removable media like CD-R, DVD-R and tape have the vulnerability of being stolen or damaged by intruders gaining access to a storage facility. The ideal secure immutable storage would have to be impregnable, not prone to system intrusion, and have protection against physical theft. Cryptography can enable security of data even in case of theft of physical storage devices.

One common method of attack against computer systems is to install applications with hidden “trojan” functionality (such as traffic sniffing or password capture). If standard applications could be made immutable, then such trojan attacks would not be possible. However, at present, such trojan attacks are widespread with detection relying solely on host intrusion detection systems that themselves are vulnerable since they are dependent on the integrity of the host operating system. Immutable storage independent of the operating system provides another level of defense which would be invaluable in thwarting or delaying malicious intrusions.

5.5 Cost

It is inevitable with the rise in the total amount of data to be stored and protected that cost is a major factor. From experience at NCSA [34], it can be seen that the volume of data that needs to be stored in an immutable manner increase almost exponentially. Hence, the storage solution needs to be cost effective to bring down the total cost of operation. Traditionally, magnetic tape has always been the cheapest media. However, with the increase in storage density in magnetic disks, disk based storage is also rapidly gaining acceptance as a cheap mode of immutable storage. Also, tape libraries and the robotic manipulators used with them are very costly, with prices easily reaching into millions of dollars [34]

6. COMPARISON OF TECHNIQUES

In this section, the different techniques for implementation of immutable storage are compared. Table 2 contains a qualitative comparison of the different types of WORM technologies currently available. For comparison, five major properties were chosen and evaluated for each technique using a five point scale (very low=1, low=2, medium=3, high=4, very high=5). Figure 1 shows a comparison of the different immutable storage techniques which was derived from assigning each property numeric values and summing these values for an aggregate score.

WORM / Properties	CD-R, DVD-R	Optical Jukebox	Magnetic Tape	Magnetic Disk (NAS, SAN)	Unix FS Tools	OS Based Techniques
Cost/MB	High	Very High	Very Low	Medium	Medium	Medium
Capacity	Low	Medium	Very High	High	High	High
Speed	Low	Low	Very Low	High	High	High
Security	High	High	Medium/Low	Medium	Very Low	Low
Management Overhead	High	Medium	High/Medium	Low	Low	Low

Table 2. Comparison of different WORM technologies.

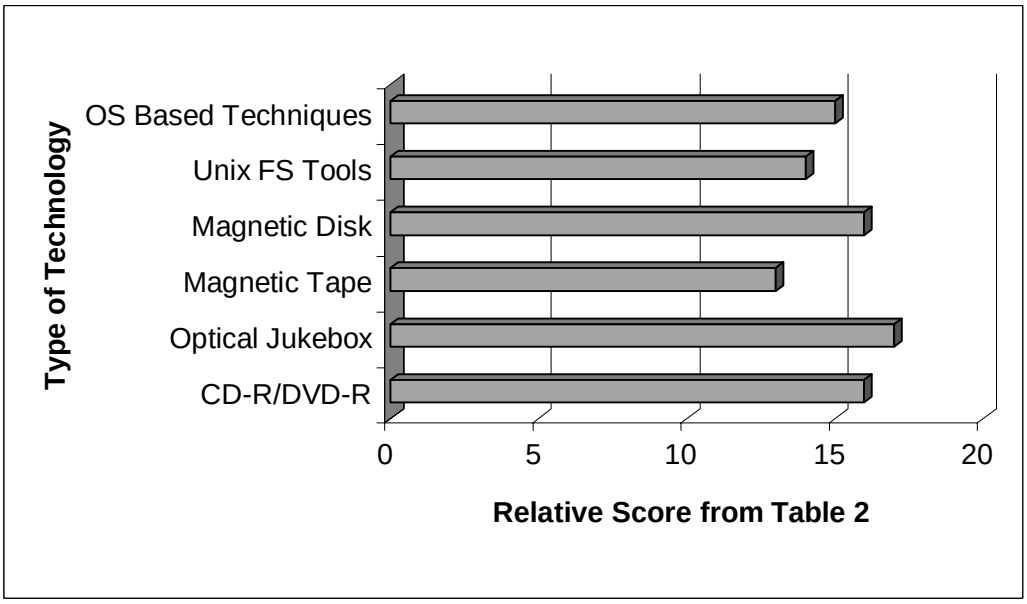

Figure 1. Relative comparison between immutable storage technologies.

From Table 2, it can be seen that the two most secure techniques, CD/DVD-R and Optical Jukebox, are both P-WORM techniques. Physical immutability provides total protection against remote modification, and excellent protection against disgruntled employees. However, both techniques are expensive, slow, provide low capacity and are difficult to manage.

Magnetic tape is the cheapest of all of the technologies. It also offers the highest potential capacities. However, the linear access properties of magnetic tape combined with relatively low transfer speeds result in the worst speed. The security and management properties of magnetic tape can vary. Given physical access to the media, it is possible to modify without much difficulty [13]. If protection from hostile employees is needed, magnetic tape is weak. Remote attacks on the media are still fairly difficult. Additionally, in small quantities, it can be difficult to manage magnetic

tape. For the largest of deployments, tape silos similar to optical jukeboxes exist which can ease management. However, these are very expensive.

The three high-speed techniques are all ultimately based on spinning magnetic disk. All three have low management overhead and can scale to large capacities for reasonable cost. They differ, however, in their security. The Unix FS tools offer only minimal security—it is common for today's root kits to include tools to bypass *chattr* protections. Other OS-based techniques are better only in that tools to bypass them are not common—this reflects their low deployment rate. Their base security is no better. The embedded magnetic disk systems [30] offer better protection. Generally such systems use RAID to prevent data loss from hardware failures, and the embedded nature of the devices prevent trivial modifications. However, the ultimate security of such devices is dependant on the quality of the firmware code and is therefore not as high as a physically immutable solution. In summary of the comparison considering cost, capacity, speed, security, and management overhead factors, the optical jukebox is the best overall immutable storage solution at present (not by much) and each of the immutable storage techniques have advantages and disadvantages that may make a particular technique better suited for different specific situations.

7. ISSUES RELATED TO MULTIMEDIA

Driven by a continuous demand for ever-higher quality and an accelerated rate of production, the need for multimedia storage has grown dramatically. As demand for quantity has grown, new regulations, new threats, and new formats like 720p and 1080i for HDTV transmissions and MPEG-2 encoding have increased the qualitative requirements for multimedia storage. Combined, these new requirements are difficult to meet.

- Higher Frame Resolution – more data per frame
- Higher Frame Rate – more data per time unit
- More Programming – more simultaneous streams
- On-demand Video – simultaneous pull requests for video
- Growing Digital Consumer Market – More demand, more data flow

The total effect of these movements is not the sum but the multiplication of the above factors. Therefore the demand of secure multimedia storage will grow in large demand as well.

7.1 Performance Issues

The performance requirements of multimedia have been thoroughly studied. Everything that can be said about non-immutable storage applies to immutable storage as well. For consumer video, the increased prevalence of video on-demand, streaming video, and high bit-rate formats increases the performance requirements beyond what they were in the past. Medical data has been moving to higher resolutions, with high quality requirements precluding the use of lossy compression. Security cameras involve many continuous feeds, which must be kept for significant time periods. Additionally, these cameras are moving towards higher quality and more useful S-VHS resolution formats. Soon, low-cost 3CCD 1080i equipment will be available for security applications, driving bandwidth and space requirements to very high levels. However, the cheapest and most secure immutable technologies are unable to meet these performance demands, while the best performing technologies may be cost-prohibitive at the required sizes.

7.2 Security Issues

The need to protect multimedia data from destruction comes from the growing value of the data itself. Digital security footage is of little use if it can be deleted. Hackers have attacked analog cable and satellite systems before. New digital video deployments are even more vulnerable to remote attack.

It is important to consider that a worst-case Internet virus or worm, which destroys data, has not appeared yet. [36] theorizes that code with a malicious payload such as destroying data on remote and local disk or destroying the Boot ROM on different vendor systems could cause $50 billion in damages. While data may or may not be protected by backup or versioning, such an attack would make a PC unusable without opening the case to reflash the BIOS, or replacing the motherboard entirely. This type of attack would be mitigated or stopped if critical operating system files were immutable.

7.3 Special Challenges of HIPAA

HIPAA poses special challenges for multimedia storage. Digital medical imaging is becoming more common, driven by the increased availability of digital technology. Higher resolution devices create images which are consuming more and more storage. Beyond new technology, digital imaging is driven by HIPAA itself. HIPAA requires better access methods than the older physical file folder techniques of the past. Digital storage is all but mandated.

Tamper-resistance techniques can be much simpler than immutability techniques. For a security system, preventing the change of data may be sufficient. Outright destroying the data may draw more attention then leaving it alone. However, HIPAA cannot be satisfied by tamper-resistance. The requirements are that medical data cannot be lost, something tamper-resistance alone cannot provide. More than any other type of data, the integrity and immutability of medical imaging are essential as data loss is totally unacceptable.

8. CONCLUSION

Building secure immutable storage and archival systems is emerging as a critical requirement of next generation multimedia and content management/storage systems. Immutability ensures the integrity of data and thwarts intruders' attempts to manipulate the data. Some of the early approaches towards meeting the growing demand for storage security with respect to persistent data archival have been discussed. With stringent government regulations requiring strong protection from unauthorized modification to or loss of data, the need for secure storage is growing. At the same time, performance and storage needs, especially for image and video data, are also growing rapidly. In the near future, immutable storage systems will become an integral part of multimedia content management and storage systems.

REFERENCES

1. *Computer Storage, Wikipedia*, http://en.wikipedia.org/wiki/Computer_storage.

2. E. Haubert, J. Tucek, L. Brumbaugh, and W. Yurcik, "Tamper-Resistant Storage Techniques for Multimedia Systems," *IS&T/SPIE International Symposium Electronic Imaging / Storage and Retrieval Methods and Applications for Multimedia (EI121)*, San Jose CA USA, January 2005.

3. J. Gruener and M. Kovar, "Abridged Report: The Emerging Storage Security Challenge," *The Yankee Group Report*, September 2003.

4. *Health Insurance Portability and Accountability Act of 1996* http://www.cms.hhs.gov/hipaa.

5. *General Rules and Regulations promulgated under the Securities Exchange Act of 1934*

6. Sarbanes-Oxley Act. *One Hundred Seventh Congress of the United States of America at the second session.* 2002. http://news.findlaw.com/hdocs/docs/gwbush/sarbanesoxley072302.pdf.

7. P. A. Loscoco, S. D. Smalley, P. A. Muckelbauer, R. C. Taylor, S. J. Turner and J. F. Farrell. "The Inevitability of Failure: The Flawed Assumption of Security in Modern Computing Environments," In *Proceedings of the 21st National Information Systems Security Conference*, pp. 303-314, Crystal City, VA, October 1998.

8. *Electronic Signatures in Global and National Commerce Act, Public Law*, pp. 106-229, U.S.A. June 2000.

9. D. Cooper and C. Pfleeger, "Security and Privacy tc," *IEEE Computer*, pp. 118-119, March 1996.

10. B. Blakley. "The Emperor's Old Armor," In *Proceedings of the 1996 Workshop on New Security Paradigms*, pp. 2-16, Lake Arrowhead, CA, 1996.

11. D. B. Baker, "Fortresses Built Upon Sand," In *Proceedings of the 1996 Workshop on New Security Paradigms*, pp. 148-153, Lake Arrowhead, CA, September 1996.
12. A. Desjanun, "Hacker Teams Breach Powerful Research Networks," *USA Today*, April 14, 2004. http://www.usatoday.com/tech/news/computersecurity/2004-04-14-synchronized-hacking_x.htm

13. Y. Wang and Y. Zheng. "Fast and Secure Magnetic WORM Storage Systems," In *Proceedings of the 2nd USENIX Conference on File and Storage Technologies*, San Francisco, CA, 2003.

14. S. Manap, "Rootkit: Attacker Undercover Tools," http://www.niser.org.my/resources/rootkit.pdf.

15. J. D. Strunk, G. R. Goodson, M. L. Scheinholtz, C. A. N. Soules and G. R. Ganger, "Self-Securing Storage: Protecting Data in Compromised Systems," In *Proceedings of the 4th Symposium on Operating Systems Design and Implementation*, San Diego, CA, October 2000.

16. A. Hume, "The File Motel – An Incremental Backup System for Unix," *Summer USENIX Conference Proceedings*, pp. 61-70, 1988.

17. T. Laksodi, B Eifrig and J. Gait, "A UNIX File System for a Write-Once Optical Disk," *Summer USENIX Conference Proceedings*, pp. 51-60, 1988.

18. G. Russo, S. Russo, and B. Pirenne. "An Operating System Independent WORM Archival System," *Software – Practice and Experience*, **Vol. 25(5)**, pp. 521-531, May 1995.

19. S. Quinlan. "A Cached WORM File System," *Software—Practice & Experience*, **Vol. 21, Issue 12,** pp. 1289-1299, 1991.

20. R. Pike, D. Presotto, S. Dorward, R. Flandrena, K. Thompson, H. Trickey and P. Winterbottom, "Plan 9 from Bell Labs," *Computing Systems*, **Vol. 8, 3**, pp. 221-254, Summer 1995.

21. S. Quinlan and S. Dorward. "Venti: a New Approach to Archival Storage," In *Proceedings of the USENIX Conference on File and Storage Technologies*, San Francisco, CA, 2002.

22. K. Fu, F. Kaashoek and D. Mazières, "Fast and Secure Distributed Read-only File System," In *Proceedings of the 4th Symposium on Operating Systems Design and Implementation*, San Diego, CA, October 2000.

23. A. Crespo and H. Garcia-Molina, "Archival Storage for Digital Libraries," In *Proceedings of the Third ACM International Conference on Digital Libraries*, 1998.

24. A. Apvrille and J. Hughes, "A Time Stamped Virtual WORM System," *Sécurité des Communications sur Internet (SECI02)*, Tunis, Tunisia, September 2002.

25. D. Ellard and J. Megquier, "DISP: Practical, Efficient, Secure and Fault Tolerant Data Storage for Distributed Systems," *Harvard Computer Science Technical Report TR-17-03*, December 2003.

26. D. Ellard, J. Megquier, L. Park and N. Yuan, "The INDIA Protocol – Project Report", *Harvard Computer Science Technical Report TR-25-97*, December 1997.

27. D. S. Santry, M. J. Feeley, N. C. Hutchinson, A. C. Veitch, R. W. Carton and J. Ofir, "Deciding When to Forget in the Elephant File System," In *Proceedings of the 17th ACM Symposium on Operating Systems Principles (SOSP)*, pp. 110-123, 1999.

28. R.Williams, "P-WORM, E-WORM, S-WORM is a Sausage a Wienie?" Chicago, 1997.

29. G. Quickel, “Infinistore Virtual Disk – Optical WORM killer?” *Global Information Distribution White Paper*, 2002.

30. EMC Centera Product Description Guide, http://www.emc.com/pdf/products/centera/centera_guide.pdf.

31. C. Lueth, “WORM Storage on Magnetic Disks using Snaplock Compliance™ and Snaplock Enterprise™,” *Network Appliance Technical Report TR3263*, August 2003.

32. Unix Man Pages, http://www.rt.com/man.chattr.1.html.

33. Linux Intrusion Detection System, www.lids.org.

34. M. Butler, “Storage Issues at NCSA: How to Get File Systems Going Wide and Fast Within and Out of Large Scale Linux Cluster Systems,” *10th Goddard Conference on Mass Storage Systems and Technologies*, 2002.

35. S. Uttamchandani, K. Voruganti, S. Srinivasan, J. Palmer and D. Pease, “Polus: Growing Storage QoS Management Beyond a “Four Year Old Kid”,” In *Proceedings of the 3rd USENIX Conference on File and Storage Technologies (FAST '04)*, 2004.

36. N. Weaver and V. Paxson, “A Worst Case Worm,” In *Proceedings of the 3rd Workshop on Economics and Information Security (WEIS)*, 2004.