Towards Tamper-evident Storage on Patterned Media

Pieter H. Hartel Leon Abelmann Mohammed G. Khatib
Fac. of Electrical Engineering, Mathematics and Computer Science,
Univ. of Twente, P.O. Box 217, 7500 AE Enschede, The Netherlands,
email {p.h.hartel, l.abelmann, m.g.khatib}@utwente.nl

Abstract

We propose a tamper-evident storage system based on probe storage with a patterned magnetic medium. This medium supports normal read/write operations by out-of-plane magnetisation of individual magnetic dots. We report on measurements showing that in principle the medium also supports a separate class of write-once operation that destroys the out-of-plane magnetisation property of the dots irreversibly by precise local heating. We discuss the main issues of designing a tamper-evident storage device and file system using the properties of the medium.

1 Introduction

Tampering with data is a problem because it affects many businesses and organisations [11]. The culprits include everyone from the casual hacker who tries to obliterate the trace of his actions, to the CEO and his accountant who destroy vital evidence [10]; and the stakes are high [20]. As a result, laws such as the US Sarbanes-Oxley Act of 2002 (SOX) [37] and the EU data retention directive [49] have been introduced to create a legal framework in which to deal with tampering.

To deal with tampering on a technical level a large variety of disk, tape, and optical Write Once Read Many (WORM) technologies have been developed that are designed [15] to resist or at least to help detect tampering. Unfortunately, tamper resistance is a hard problem [3] that none of the existing storage technologies actually provide. For example, there is nothing to stop a dedicated attacker from tampering with a Read-only Memory (ROM) [4]. On the other hand it is difficult to cover the traces of tampering with a ROM. Mass storage such as disk, tape and optical disk is probably just as easy to tamper with as ROM, so we believe that we should put our efforts in improving the tamper evidence of mass storage.

It is always difficult to find the right balance between security and usability, and tamper evidence of mass storage is no exception to this rule. To guide the discussion we analyse how mass storage is used. Probably most applications use a data base, which requires efficient random reads and writes. Tampering with data is easy, as any record can simply be rewritten. Therefore most data bases support a snapshot operation that freezes the contents of the data base, for instance for auditing purposes, recovery, etc. If the snapshot is written to a disk, the attacker will find it as easy to tamper with the snapshot as it is easy to tamper with the live database. If on the other hand the snapshot is written to an optical WORM device, tampering would be more difficult to hide. Unfortunately the WORM device also has an impact on the way the snapshot can be read, as the performance characteristics of hard disk and optical disk are different. An ideal solution would combine the performance of the hard disk with the tamper evidence of the optical disk. In other words we require not a WORM device but a Selectively Eventually Read-only (SERO) device, i.e., a device that begins life as a Write Many Read Many (WMRM) device, selected parts of which are subjected to Write Once (WO) operations, and which ends life as a Read-only (RO) device.

The construction of a SERO device is still a long way away, but in this paper we would like to lay the physical foundation for the medium used in such a device, also giving the design considerations for a device and a file system that would support SERO storage. Our proposal combines an idea of Molnar et al. [31] for *tamper-evident storage* with our own work on *patterned media*. We introduce each of these two elements below.

Molnar et al. [31] describe how standard Programmable Read-Only Memory (PROM) can be used to build *tamper-evident storage*. The basic idea is to store each bit of information in a cell occupying two bits using Manchester encoding: the logical bit 1 is encoded as the cell 10 and the logical bit 0 is encoded as the cell 01. The value 11 indicates a cell that has not yet been used

(all cells in a PROM are initialized to 11). The value 00 indicates a cell that has been tampered with for the following reason. The physical properties of a PROM make it *impossible* to change a 0 back into a 1 (except by exposing the entire memory module to ultra violet light, which would reset all cells to 11). Therefore, the only way to tamper with information (which is encoded as 01 or 10) is to clear a bit. This immediately results in an invalid cell 00, which provides the evidence of tampering.

A *patterned medium* [52] consists of a regular arrangement of magnetic dots separated by sub-micron distances that can be magnetised in two directions along a fixed magnetic axis. A magnetic dot can be read and written magnetically any number of times. However, by precise local heating of a dot, the orientation of the magnetic axis of the dot can be changed irreversibly. The idea is to use this feature to create a storage device that begins life as a WMRM device, reading and writing dots magnetically. After heating, a dot can no longer be read or written magnetically, but the fact that a dot has been heated can be detected. From then on the heated parts of the medium operate as a tamper-evident RO device, while the rest of the medium continues to operate as a WMRM device. The ability to heat parts of the medium incrementally provides flexibility that cannot be matched by current WORM technology. (The operation we call "heating" is usually called "freezing" in the literature, but given the physical realisation of the operation we decided to stay with the term heating.)

In the rest of the paper, we discuss the issues that must be addressed for the combination of tamper-evident storage and patterned media to result in a SERO device with the following properties. Firstly, like a hard disk, the device is expected to offer random WMRM access to a large number of blocks with a total capacity of the order of 1 Terabit [39]. Secondly, the device is expected to be capable of a WO operation of a block by heating the magnetic dots of the block. After the WO operation the block is RO. We will also refer to the WO operation of a block as *heating a block*. Finally, heating a block is expected to be relatively slow. Therefore, the device is expected to be able to heat a contiguous sequence of blocks, henceforth referred to as *heating a line*, by (a) calculating a secure hash of the line, and (b) applying a WO operation on the first block of the line to record the hash.

Our proposal does not use cryptographic keys. We provide only data integrity (using secure hashing and hardware support) but no confidentiality or authenticity. Our proposal is thus complementary to the vast amount of work on using symmetric and public key cryptography to provide storage with confidentiality and authenticity, and our work could be combined with many of the existing approaches.

Contribution The contributions of the paper are (1) to evaluate the feasibility of heating dots, and (2) to discuss whether a tamper-evident probe storage device and file system on a patterned medium are feasible. The paper touches upon all the relevant aspects from regulatory issues studied by lawyers down to material science studied by physicists.

Related work is discussed in the next section. Then we speculate on the feasibility of a device (Section 3), and a file system (Section 4) for SERO storage. A security analysis of the hypothetical SERO file system and device is presented in Section 5. We describe concrete examples of an actuator (Section 6), and a medium (Section 7) that could be used to build a SERO device. Section 8 discusses open issues. The last section concludes and suggests further work.

2 Related work

We discuss related work in a top down fashion, starting with the regulatory issues all the way down to material science.

Regulatory issues The world of data storage goes through a period of turmoil. Taylor [49] describes how the EU data retention directive will increase the difficulty of companies and organisations to comply with the already burdensome laws and regulations. Hasan et al. [17] describe the struggles and demise of Storage Service Providers, largely due to regulations such as SOX, while the business case for outsourcing data storage is as strong as ever due to the rising Total Cost of Ownership (TCO). Hasan and Yurcik [16] discuss the effects of disclosure legislation on companies, which stipulates that storage security breaches must be reported, in some cases even in public, on TV and in newspapers. The effect on the reputation of businesses affected can be devastating. Tamper-evident storage is needed to help address the problems.

Tamper evidence There are three basic approaches to providing tamper evidence. The first and most commonly practiced approach relies on hardware support; for example using Write Once Read Many (WORM) technology [5]. The main disadvantage is that WORM technology tends to be inflexible; data can only be written once, while most applications (chiefly data bases) write and rewrite data often until the moment has arrived to take a snapshot for auditing and compliance purposes. The second approach to providing tamper evidence relies on a trusted third party (TTP) to provide notary services [6], secure time stamps [26], etc. It is not always

practical to rely on a TTP; for example in mobile applications the TTP may not always be reachable. The third approach either (a) distributes the data over many servers, only some of which are assumed to be malicious or faulty [2], or (b) uses many clients to control the server. A good example of the latter is SUNDR [24], in which each client keeps a record of his last transaction with the SUNDR server. This allows the client to check whether his previous transaction has somehow been "forgotten" by the server. This works fine as long as all clients regularly check their last transaction, but the mechanism is ineffective if this is not the case; for example if most clients make only one transaction. SUNDR is geared towards detecting tampering during data sharing; in our work we do rely on others to detect tampering but rely on hardware support.

All the approaches mentioned rely on something external to system that is intended to deliver the secure store (i.e., separate hardware, separate servers and/or separate clients). Our approach relies on hardware support, while improving the flexibility beyond what a typical WORM system can offer.

WORM technologies Write-protect rings have been used for 50 years on magnetic tapes to prevent accidental overwriting of valuable data. There are many variations on this idea to protect disks, tapes and optical media.

Physical WORM technologies using optical media and tape are widely used. Optical WORM technologies offer a high level of integrity but the cost of ownership is higher than that of disk-based technologies. For example CDROMs are cumbersome to manage (because they have a small capacity, which leads to large collections of CDs), and professional optical storage systems are expensive (because they often contain mechanical robots). Tape based technologies are generally inexpensive but offer integrity at the medium level only. For example a tape cartridge in the Linear Tape-Open 3 (LTO-3) industry standard has a small semiconductor memory in which a read-only flag can be set [21], such that a compliant tape drive will refuse to write on such a cartridge. The tape itself can still be written using a tape drive that has been tampered with, or after tampering with the cartridge.

Software based WORM technologies are based on the idea that the disk driver or the firmware of the disk can be modified to block future writes to selected areas of the disk. The integrity offered by this approach is relatively weak, as software modifications can generally be undone. There are many Virtual Tape Library products in the market that depend on software based WORM technologies [55].

An IBM patent [56] proposes to connect the write signal of a disk head via a blowable fuse such that once the fuse is blown, an entire disk platter becomes immutable. This offers a high level of relatively coarse grained integrity. As in the case of the LTO-3 tape standard, the platter is still writeable but it would be more difficult to repair the fuse in the head than it is to tamper with an LTO-3 tape drive.

Probe storage During the last ten years, several recording systems based on probe microscopy technology have been proposed. Leading research by IBM [39] is followed by other companies such as HP [34], Samsung [30], Seagate [23], LG [22] and a number of universities such as Carnegie Mellon, DSI Singapore, Exeter, Tohoku, Twente, and Yonsei. Probe storage is also being combined with disk storage [18].

Materials aspects To understand the details of the modification of magnetic materials, background information is given in section 6. For the following it is sufficient to understand that the individual elements in the patterned medium, the dots, have an easy direction of magnetisation perpendicular to the film surface, rather than in-plane. This is achieved by using a stack of ultrathin films (tens of layers, each thinner than 1 nm) of interleaved magnetic and non-magnetic material. The many interfaces between the magnetic and non-magnetic films force the magnetisation perpendicular to those interfaces, and therefore to the film.

The modification of the magnetic properties of a multilayered patterned medium is relatively easy. The first experiments were performed with Ga ions from a Focussed Ion Beam [50], using modest irradiation doses. The magnetic properties of the material are modified by displacement of the interface atoms, and inclusion of Ga. By using lighter ions, such as He^+, the incorporation of ions can be avoided, and only interface mixing results [41]. As a result, the easy axis of magnetisation rotates from perpendicular to in-plane. By using shadow masks to shield from the impingement of ions, these irradiation techniques can be used to pattern multilayered films into areas with perpendicular and in-plane magnetisation. These types of patterned medium have the advantage that the surface remains flat.

In this work we suggest to use temperature-assisted interface mixing to destroy magnetic dots selectively. On the effect of heat treatment of multilayer materials, much less is known, primarily because it is considered a detrimental effect that cannot be used for patterning. Encouraging experiments show however that at relatively low temperatures of about 300 °C, interface mixing occurs between Co (magnetic) and Pt (non-magnetic) [46]. Heat treatment can however also have beneficial effects on the interfaces. In Co/Cu systems for instance, the interfaces are found to enhance at temperatures of 300 °C [7]. Most

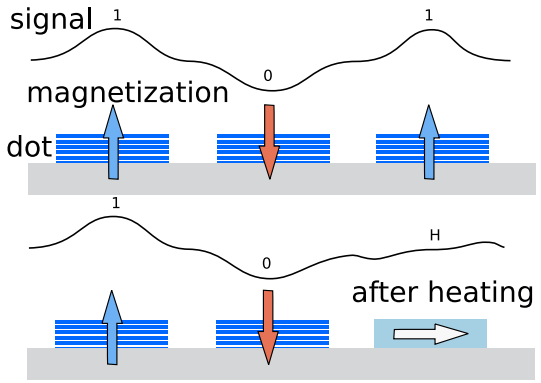

Figure 1: Above: dots are magnetised upwards or downwards; Below: destroyed dots have a perpendicular or in-plane easy axis.

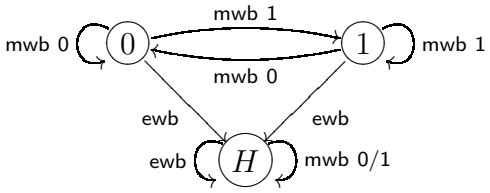

Figure 2: The state transitions of one bit. H indicates a heated bit, and $0/1$ indicates a bit that has not been heated.

likely this has to do with the solubility of both materials. Therefore the material combination has to be chosen with care. Even so, it is possible to damage the films at higher temperatures. In the same Co/Cu system, at 700 °C grains start to grow and the Co layers start to coalesce, thus destroying the interface completely. From these experiments we can conclude therefore that thermal destruction of the magnetic properties by interface mixing is in principle possible, provided that the right material combination is chosen.

This concludes the survey of related work on all relevant aspects of tamper-evident data storage.

3 Device

We argue that tamper evidence storage requirements can be served flexibly by six high level sector operations, which are built out of four low level bit operations. We describe the bit operations first, followed by the sector operations.

Magnetic bit operations We require magnetic read and write operations for bits and a second set of electrical read and write operations for bits. We discuss the magnetic read and write operations first. In the normal mode of operation we have a medium with a regular matrix of magnetic single domain dots with a preferred axis of magnetisation perpendicular to the medium. This is illustrated in the top half of Figure 1, which shows the substrate and three layered dots. The first and last are magnetised in the upwards direction, the middle in the downwards direction.

The magnetic write bit operation mwb sets the direction of the magnetisation (up is 1, down is 0) and the corresponding magnetic read bit operation mrb senses the direction of the magnetisation. The signal measured by the read heads is shown schematically, indicating a positive peak for the first and the last dot, and a negative peak for the middle dot. The top half of Figure 2 illustrates the transitions from 0 to 1 and vice versa, as effectuated by the magnetic write operations on the state of an individual bit.

Electrical bit operations The second set of read and write operations on bits has an electrical basis. The electrical write bit operation ewb heats an individual dot by means of an electric current flowing from the probe tip via the dot to the medium. This heating causes the multilayer structure of a dot to be destroyed and as a result the easy axis of magnetisation rotates into the medium. The data stored by magnetic write operations is lost. Now, we have a third way of representing data, indicated by the letter H (for heated), and effectuated by the ewb operation. (We will also indicate un-heated bits by the letter U). The bottom half of Figure 1 shows that the layered structure of the last dot is permanently destroyed. The peak in the magnetic read signal for the last bit has disappeared. The electrical write bit operation ewb is an irreversible process, which can only change a 0/1 bit into a H, as shown by the one-way transitions from the states 0 and 1 in the top half of Figure 2 to the state H. (See Section 7 for detail on the physics.)

Strictly speaking there is no electrical read bit operation erb; instead erb is built out of magnetic read and write operations. The operation erb detects the presence or absence of an out-of-plane dot by performing an atomic sequence of mrb and mwb operations as follows:

1. mrb to read the original bit;
2. mwb to write the inverse of the original bit;
3. mrb of the inverse to verify that the inverse can indeed be read back;
4. mwb to write the original again;
5. mrb to verify that the original can indeed be read back.

Block	Bit number					Purpose
	0	1	…	4094	4095	
0	HU/UH		…	HU/UH		hash+meta.
1	0/1	0/1	…	0/1	0/1	512B data
2	0/1	0/1	…	0/1	0/1	512B data
			⋮			
$2^N - 1$	0/1	0/1	…	0/1	0/1	512B data

Figure 3: Sample medium layout of a heated line of 512 bytes=4096 bits each. 0/1 represents a magnetically written bit, HU represents an electrically written, Manchester encoded logical 0 and UH represents a logical 1.

If any of the two verification steps fail we assume that the dot has lost its out-of-plane property and let the electrical read operation erb return H, else erb returns U (the two inversions ensure that the original magnetic data is restored for dots that have not been heated).

The erb operation is at least 5 times slower than mrb, and ewb is also slower than mwb because of the local heating process. Therefore, as stated before, the idea is to use the erb and ewb operations sparingly.

As illustrated in Figure 2 (bottom right), applying a single mrb operation to an electrically written bit would yield a more or less random result. To avoid this, the device must follow the proper protocol which means that magnetically written data must only be read magnetically and that electrically written data must only be read electrically. A simple way to achieve this is by reserving specific physical areas for electrical data while using other areas for magnetic data. As we shall see below, this rigid segregation of electrical and magnetic data puts severe constraints on the design of the device and the file system. An alternative would be to read the in-plane magnetic signal directly, however, this requires carefully constructed elliptic dots to ensure that the direction of the in-plane magnetization is known (See Section 7).

Sector operations Following Pozidis et al. [39] we assume that a sector has a standard size of 512 bytes and about 15% sector overhead for the sector header, error correction, and cyclic redundancy check. This allows us to build a magnetic read sector operation mrs and a magnetic write sector operation mws using the magnetic read and write operations for bits described above, and taking error correction appropriate to the medium, the tips, etc. into account. Henceforth we will talk about a block as the smallest unit of storage, and for simplicity we assume that a block is a single sector. Similarly we can build an electrical read sector operation ers and an electrical write sector operation ews using the electrical read and write operations for bits described above.

Heat a line Assume that at a certain moment some existing data must be heated, after which the data cannot be destroyed without leaving a trace. Our heat operation works on a *line*, which is a sequence of 2^N contiguous blocks aligned on a 2^N boundary. When given a line, the heat operation performs the following atomic sequence of steps:

1. Read blocks $1 \ldots 2^N - 1$ representing the line to be protected using $2^N - 1$ calls to mrs;
2. Calculate a secure hash (e.g., SHA-256) of the blocks and their addresses just read;
3. Write the 512-bit Manchester encoding of the 256-bit hash in block 0 using the electrical write operation ews, this leaves 4096-512=3584 bits of space for meta data, signatures, etc.;
4. Check that the hash can be read back using ers, or else fail.

All lines can be heated individually, thus providing significant flexibility over WORM-based approaches. Blocks $1 \ldots 2^N - 1$ of a heated line can still be read magnetically, hence efficiently, and as often as needed. Figure 3 illustrates the result of the heat operation. The last $2^N - 1$ blocks are written magnetically, shown as zeros and ones. Block 0 is written electrically in a Manchester encoding, where each logical bit of the hash occupies two physical bits on the medium. The Manchester encoding ensures that a heated bit (i.e., an H) has at most one heated neighbour. Since each electrical write may be expected to have a detrimental effect on the neighbouring bits, spreading out heated bits is good for reliability.

The heat operation, when applied to a line that has already been heated either has no effect and is therefore harmless (if the data in block 0 is invariant) or it will turn Manchester encoded bits into HH, thus providing evidence of tampering.

Verify a heated line The verify operation computes the hash of a line and compares the computed hash to the electrically written hash. A mismatch represents evidence of tampering.

Addressing Modern disks offer a uniform method of accessing blocks by logical block address, rather than by physical block addresses (which may vary wildly between devices), and automatic bad block handling by the device offers the file system the abstraction of a reliable device. However, to be tamper-evident we must know exactly where to look for evidence of tampering. This means that a SERO device and the SERO file system should use physical block addresses (PBA) rather than

logical block addresses (LBA) so that we know exactly at which PBA to look for heated hashes. Bad block handling is a challenge, because a heated block should not be misinterpreted as a bad block. If the disk exposes its physical layout to the file system, the file system should be able to recognize when data is in the right place.

4 File system

Having described a SERO device that can make a line RO by heating the line, we discuss the main questions that the designer of a file system must address to serve such a device. The main question that we wish to pose is *what properties a high performance, tamper-evident file system should have so that it can serve a SERO device*. We will explore the performance issues first, followed by the tamper evidence issues.

4.1 SERO file system performance

Standard hard disk WMRM storage offers high data rates and low access times, whereas WORM storage typically has higher access times (especially when tape or disk robots are involved), and lower data rates than WMRM. A SERO mass storage device combines the two classes of use in one device, which poses a challenge to the device and the file system not to degrade the performance of WMRM operations due to the presence of RO lines. The two types of storage are normally served by different file systems, whereas a SERO device could probably be served better by a single file system.

As a SERO device ages, slowly but surely parts of the storage become RO, such that the WMRM area not only shrinks but it might also become fragmented. Considering that it does not make sense to move a RO line (because this would not leave behind usable space), the file system has an important task in avoiding fragmentation of heated lines.

Interestingly, part of the answer to the question we posed at the beginning of this section is provided by Rosenblum and Ousterhout, who observe that when the read cache is large enough, disk I/O is dominated by writes. Therefore, the disk has the best chance of keeping up with the CPU if writes are clustered [42]. Many file systems have since been proposed that cluster writes. From a write performance point of view it makes no difference whether the blocks in a cluster are related, for instance when the blocks are part of the same file or when the blocks are unrelated. However, from the SERO point of view it does make a difference whether blocks are related, because it does not make sense to heat a line of unrelated blocks. In the end, it depends on the application whether or not clusters of related blocks are likely to occur. For instance, taking a data base snapshot would probably result in a cluster of related blocks.

So why does clustering help our SERO device? Clustering makes it possible to take a contiguous sequence of related blocks, to hash the data stored in those blocks, and to use the WO operation to store the hash of the sequence. The advantages of clustering are twofold. Firstly, the larger the cluster, the lower the overhead of the hash can be. Secondly, the WO operation is expected to be considerably slower than the WM operation, and clustering allows the WO operation to be used sparingly.

We will now have a closer look at the original log-structured file system [42]. LFS treats the space on the disk as a collection of contiguous segments, each of which consists of a contiguous sequence of blocks. This collection of segments is called the log. New data is written sequentially to the log and the log is filled incrementally.

An LFS has to manage data blocks and free blocks on the storage device, while keeping the performance of the disk as high as possible. To achieve this performance goal, it (1) accumulates small writes and commits them to the disk in a single operation, and (2) gathers related but scattered blocks, removing dirty blocks by running the garbage collector.

The presence of heated lines complicates the tasks of the LFS. This is because once a line has been heated it cannot be copied by the garbage collector, since a heated line leaves no reusable space behind. Copying a heated line just decreases the free space that can be potentially used for new data. Therefore, like clustering of related blocks, heated lines should also be clustered.

Based on the behaviour of the application, it should be possible to predict which lines will be heated at the same time. Therefore, during garbage collection, the file system may cluster lines into segments, that are likely to be heated at the same time. As a result of such a clustering policy, the file system creates a bimodal distribution of heated segments; that is we have only mostly heated segments and mostly unheated segments. As a result, (1) the performance of reading/writing blocks should not be affected much, since heated lines and WMRM live data blocks are kept separate, (2) space decreases only if new data is written and not when lines are heated, since lines are heated in the right place, avoiding the need to copy them, and (3) the garbage collector skips over heated segments, avoiding reading and writing them repeatedly, thus saving on disk bandwidth. Summarizing, the bimodality should help to keep the performance high in the presence of heated lines.

Other file systems do not use a log, but pack data into clusters. For example, the Berkeley Fast File Systems (FFS) [44] uses clusters to pack small files with their metadata, or to pack related blocks of large files into the

same cluster. The discussion above on bimodality holds for these file systems as well; FFS-like clustering policies should maintain mostly heated clusters and mostly unheated clusters.

4.2 SERO file system tamper evidence

The second part of the answer to the question we posed at the beginning of this section is provided by a number of proposals that hash disk blocks to provide tamper evidence.

So why does hashing help to protect the integrity of the data? Basically because it is easy to compute a hash from a group of disk blocks, while it is hard to find another set of disk blocks with the specific hash. We discuss two file systems for archival storage that use hashes extensively. The first builds an index structure from the leaves up, and the second builds the index from the root down.

Venti [40] uses a secure hash as the address of a node, where a node consists of a block of data or hashes. Venti builds a hierarchy of nodes from the leaves upwards by storing the hashes of the children of a node in the parent. The hash of the root node represents the entire hierarchy. As long as the hash of the root is stored securely, tampering can be detected. To check a node we use the hash of the node as its address, then re-compute the hash of the node, and finally compare the computed hash to the address. A computed hash that does not match the address of the node presents evidence of tampering.

A SERO device would be appropriate to keep the hash of a node secure. For simplicity, assume that the granularity of a node in the Venti hierarchy is a line. Then heating the line that represents a node is sufficient to calculate and store the hash of the line RO. The most relevant node to be heated is the root node, because this protects the entire hierarchy.

Venti lays different hierarchies on the data blocks to be able to record different snapshots of the file system (for example one for every working day). The same idea can also be used to construct hierarchies for different subsets of the data, such as the data accessible to different users, of different projects, etc. This would offer fine grained protection. However, the more nodes are heated, the more WMRM space on the medium is reduced to RO space, thus resulting in a reduction in usability.

A fossilised index [57] builds a tree from the root downwards. To insert a new node in the tree we start at the root, visiting all nodes down to a leaf until a free slot is found in which the hash of the new node can be inserted. The hash of the node completely determines which slot in an existing node must be used, and what path to traverse. The tamper evidence guarantee of the fossilised index relies on the assumption that once all the slots of a node have been filled, the storage device ensures that the node becomes RO, for example by copying it to a WORM device.

A SERO device would provide appropriate support for a fossilised index as it makes copying the completed node to the WORM unnecessary. Again, assuming that a node fits in a line, a completely filled node is simply heated.

5 Security analysis

Triggered by large corporate scandals in the recent past, Hsu and Ong [19] propose the following threat model for secure storage. Assume that a powerful attacker (i.e., a disgruntled employee, or a dishonest CEO) regrets the existence of a certain stored record, and that he wishes history to be rewritten by tampering with the storage system so that it "forgets" the record. The attacker can do this either by overwriting or erasing the record, or by masking the existence of the record by overwriting or erasing the index. We assume that the attacker would not like to draw attention to his actions, for instance by removing or physically destroying the storage system or parts thereof, and that the attacker would like to cover his tracks.

In terms of the threat model of Hasan et al. [14], the *attacker capability* is that of a powerful insider wielding influence over systems and the personnel responsible for the systems. The attacker has root permission on all systems connected to the storage device. The *asset goal* is the integrity and availability of specific files that the attacker wishes to compromise. The *access entry point* is the whole system stack including direct access to the storage device. The attacker is expected to be able to disconnect the storage device temporarily from the system, then to connect it to a laptop with the appropriate interface for a limited period of time, and after he has finished to reconnect the device to the system.

This threat model represents a formidable challenge to the design of any secure storage system. For example some of the existing commercial WORM-based storage systems make it difficult to tamper with data, but on most systems tampering cannot be detected. We are not able to prevent tampering either, but we are able to detect tampering. We believe this to be a significant step towards addressing the challenge of secure storage.

WORM storage is geared towards providing integrity and availability. Therefore we will analyse to what extent our SERO system can cope with threats on integrity and availability. To ensure confidentiality or authenticity cryptographic techniques should be used, but this is beyond the scope of our paper.

5.1 Integrity

Assume that the attacker issues a write command, either indirectly via the file system (which is easy) or directly, to the device (which is harder) to alter a heated file. (Files that have not been heated are trivial to attack and are therefore beyond the scope of the security analysis.) Then there are four possibilities.

- mwb hash: Changing the magnetisation of an electrically written bit of the hash has no effect, as only the presence or the absence of a magnetic dot is relevant for a heated hash.

- mwb inode/data: Changing the magnetisation of a magnetically written bit of the data is detected by the verify operation as evidence of tampering.

- ewb hash: The only changes possible to an electrically written hash are $UH \rightarrow HH$ or $HU \rightarrow HH$. HH is an illegal code, and thus represents evidence of tampering.

- ewb inode/data: Data is read magnetically, so an electrically written bit in the data, which destroys the magnetic properties of the relevant dot, appears as a read error. However, a more subtle attack would be an attempt to split a file or to coalesce two files. To illustrate such an attack imagine a heated file as shown below, where the data block d_p is carefully crafted to look like a valid hash h' and where the data block d_{p+1} looks like a valid inode i':

before:	h	i	$d_0 \ldots d_{p-1}$	d_p	$d_{p+1} \ldots d_q$
after:	h	i	$d_0 \ldots d_{p-1}$	h' i'	$\ldots d_q$

  Assume that when instructed to heat the file with inode $d_{p+1} = i'$, the device has no way of telling whether this is a true file, or just part of the data of another file. Hence after heating, the original file with inode i would appear corrupted whereas the new file with inode i' appears to be genuine, quite the contrary of what we expect. Similarly, if the hashes are not in well-defined locations it is possible to coalesce two files making the result look genuine instead of the original. To prevent splitting or coalescing attacks, the device insists that hashes are written at known physical addresses.

In all four cases either the attempt to interfere with the integrity of the data is detected or the integrity is maintained.

5.2 Availability

As stated in the threat model, the device (or parts thereof) is not assumed to be taken off line for extended periods of time, or to be removed entirely. Therefore, the only way in which the availability of a file can be affected is when the access path to a heated file is blocked, or when another file masks the desired file.

Assume that the attacker tries to delete a heated file using the `rm` command. This removes the directory entry and tries to decrement the reference count in the inode. This implies writing the inode, which will be tamper-evident because the hash is invalidated. (Incidentally, it will not be possible to use the `ln` command on a heated file either, as this would increase the reference count in the inode.) A possible protection against malicious use of the `rm` command would be to maintain the directory as a fossilised index [57].

Assume that the attacker would like to create an exact copy of file to mask the existence of the original. This cannot be done since the physical addresses of the blocks are included in the calculation of the hash. Therefore, a copy can always be distinguished from an original.

Assume that the attacker clears the directory structure, then a `fsck` style scan of the medium would definitely recover (albeit slowly) all the heated files.

Assume that the attacker clears the entire medium, for example using a bulk eraser. If done properly [12], this would clear all magnetically written information. However all electrically written information is still present, thus providing the required evidence of tampering.

There are many attacks possible that our system cannot detect. For example assume that an attacker creates a new file with data that conflicts with the file the attacker wishes to remove. Firstly, the notion of conflicting data is a semantic notion that can only be resolved by the application. Secondly, this is not an attack on the integrity of the file per se (as the original remains untouched), but an attack on the authenticity. To prevent such attacks, cryptographic means are needed.

This concludes the preliminary security evaluation of the system, and also the speculative part of the paper. The next two sections describe the components of a SERO device and experimental evidence that heating is a feasible WO operation.

6 Probe storage on a patterned medium

A patterned medium needs an actuator, appropriate read/write heads, etc. to access the medium; a probe storage device would be highly suitable for this purpose. We discuss as an example the Twente Micro Scanning Probe Array Memory (μSPAM) (Figure 4), which is made out of two or more silicon wafers bonded to each other. One

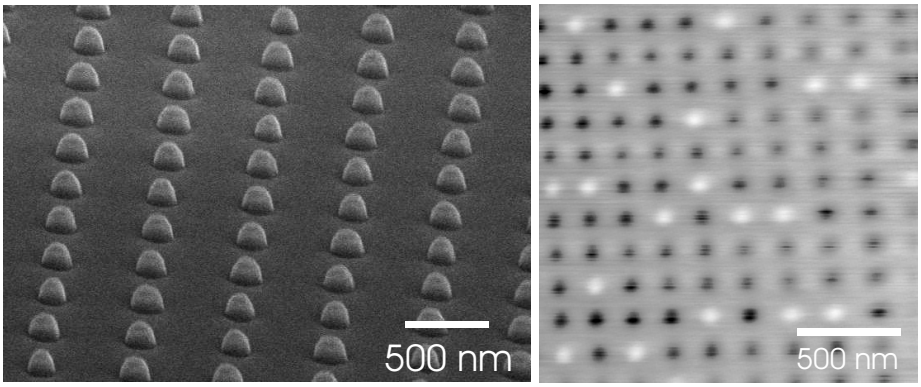

Figure 5: Scanning Electron Microscopy (left, 500 nm pitch) and Magnetic Force Microscopy image (right, 200 nm pitch) of two different patterned media. In the SEM image, the dots are still covered by a thick resist layer, and SEM images have a long depth of focus which gives the illusion that the dots are elliptic, whereas in reality they are not.

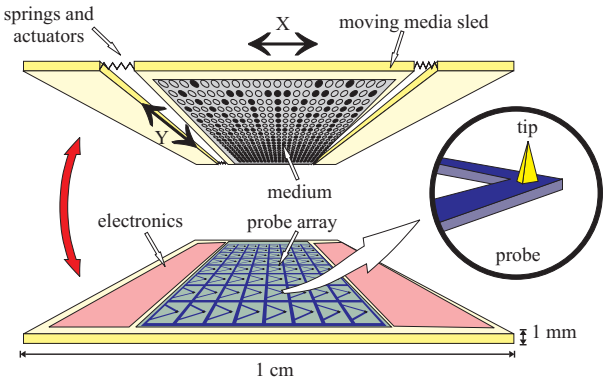

Figure 4: Principle of probe-based storage [39]. The system consists of two components, which are mounted on top of each other – one with the recording medium and the actuator, the other with the read/write probe array and the electronics.

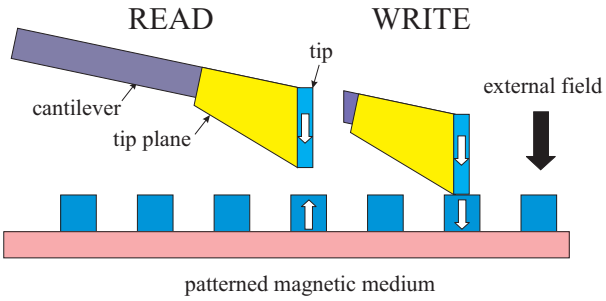

Figure 6: The principle of an MFM-measurement

half contains the (magnetic) medium. An electrostatic stepper actuator, such as the μWalker [48] or Harmonica drive [43] is used to move the medium. The other half consists of one large array of probes.

The patterned medium The medium for the μSPAM is a regular matrix of magnetic single domain dots. Such a discrete medium is expected to be able to support higher bit densities compared to the continuous polycrystalline medium used in the hard disk today [51].

A matrix with a period of 200 nm can be achieved [53]. A scanning electron microscope and magnetic image is shown in Figure 7. An improved setup with periodicities down to 150 nm has recently been realised [25], and a period of 100 nm (being 50 nm dot size and 50 nm spacing) should be achievable. This will give a capacity of 10 Gbit/cm^2 (=65 Gbit/inch^2).

The probes For reading, the μSPAM uses the MFM (Magnetic Force Microscopy)-principle [38]. An MFM-probe is made by placing a small magnetic element, the tip, on a cantilever spring. Typical dimensions are a cantilever length of 200 μm, element length of 4 μm and diameter of 50 nm and a distance from the surface of 30 nm.

Figure 6 shows the principle of an MFM-measurement. The magnetic tip is attracted or repelled, depending on the stray field of the medium. The tip is affected by the magnetic orientation of a dot. The displacement of the cantilever might be measured by means of the change in capacity between the cantilever and the medium. Bits can be written by the combined field of the magnetic tip on one side of the medium and an externally applied field generated by a coil placed on the other side of the medium [53].

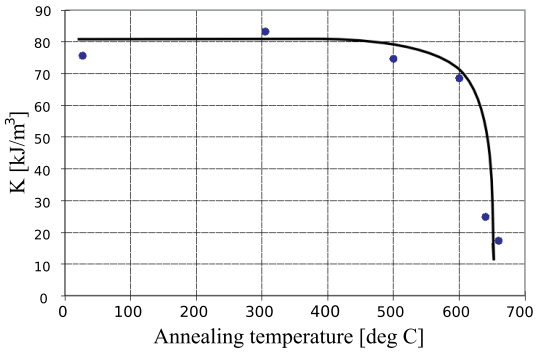

Figure 7: Perpendicular anisotropy as a function of the heating temperature

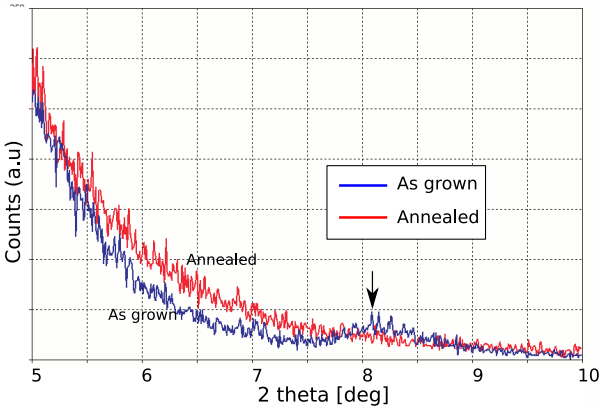

Figure 8: X-ray diffraction under a low angle of two samples, one with (labelled: Annealed) and one without annealing (labelled: As grown).

7 Heating changes magnetic properties

To support the heat operation, it should be possible to destroy the out-of-plane magnetic property of the dots. For this we need to discuss in more detail the internal structure of a dot and its relation to the magnetic properties.

The magnetic field energy is minimal when the magnetisation lies in the long axis of an object. The preferential direction of magnetisation in a needle is for instance along the needle, and not perpendicular to it. Since our dots are circular disks with a diameter much larger than the thickness, the magnetisation prefers to lie within the plane of the disk in the absence of any other energy contributions. The fact that the energy depends on the orientation of the magnetisation is called *anisotropy*. The preferred direction is called an *easy axis*. In the case of a dot which is perfectly circular, we speak of an easy plane. Normally dots will not be exactly circular, but elliptic. The magnetisation of the dot will prefer to lay in-plane along the long axis of the dot. By intentionally realising elliptic dots with their long axis along the track direction [32], data detection will be more robust and one can even imagine writing data into damaged dots (See the discussion of the erb operation in Section 3). Since the anisotropy is low, data density cannot be high however. In any case, magnetic dots with a diameter larger than their thickness will *a priori* have an in-plane easy axis.

For our system to work, we initially need dots with a perpendicular easy axis. Therefore a second strong energy contribution is needed to overcome the stray field energy and force the magnetisation perpendicular to the dot. This second energy term originates from the asymmetric arrangement of the atoms in the dot. In conventional perpendicular hard disk media, specific crystal structures are used to induce perpendicular anisotropy. These can however not easily be destroyed. In our case therefore we use interface properties. The magnetic material used in the dots consists of a stack of extremely thin Co and Pt layers, each no more than 1 nm thick [53]. The interfaces between the Co and Pt films cause anisotropy with the easy axis perpendicular to the interfaces.

Due to the delicate structure of these films, they do not support high temperatures over long periods of time. Above a certain temperature, the interface between the Co and Pt mixes, and the perpendicular interface anisotropy is destroyed. As a result the easy axis of magnetisation rotates back into the film plane. This is an irreversible process. After heat treatment, the interfaces cannot be restored.

To determine at which temperature interface mixing occurs, we have measured the anisotropy constant K of samples subjected to six different temperatures. The anisotropy constants were calculated by a Fourier transformation of the torque curve obtained with an applied field of 1350 kA/m. Figure 7 shows the dependence of the anisotropy value as a function of the heating, or annealing, temperature. (In materials science it is common to use the word annealing rather than heating, since it describes the proces rather than the method.)

The perpendicular anisotropy of the unannealed film is 80 kJ/m^3. This value is maintained up to an annealing temperature of 500 °C. Above 600 °C the value of K drops dramatically. This means that for this particular film, heating temperatures over 500 °C will be required for permanent modification of the magnetic properties.

To investigate what happens to the interface between the Co and Pt in the films, we performed X-ray diffraction experiments. In this method the film is exposed to a non-destructive X-ray. The beam penetrates metals, and reflects from discontinuities such as atomic crystal planes or film interfaces. By varying the angle of inci-

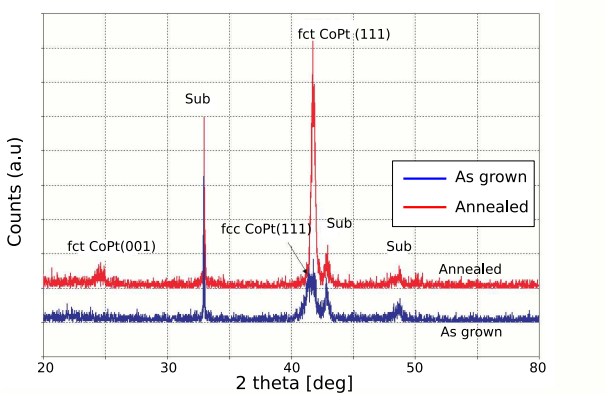

Figure 9: X-ray diffraction under a high angle of the same two samples as for low angle XRD, with annealing (labelled: Annealed) and without annealing (labelled: As grown).

dence, reflections from parallel planes at specific spacing add up and we observe a peak in the reflected intensity. In conventional operation (at high angles of incidence, so we observe spacings in the order of Angstroms), we can therefore determine the crystal structure of the film. At low angle of incidence we are sensitive to much larger spacing (1 nm) and we can observe the multilayer structure. The unannealed sample and a sample annealed at 700 °C were investigated by low angle X-ray diffraction (XRD) (Figure 8). A peak around 8 degrees on the 2 θ axis is visible on the sample without annealing. This peak is due to the periodicity of the Co and Pt multilayers. From this angle, we can calculate that layer has a thickness of 0.6 nm. In the annealed sample, this peak has disappeared, which clearly shows that after an annealing treatment at a temperature higher than 600 °C, the interfaces have mixed, the perpendicular anisotropy is lost and the out-of-plane magnetic properties of the film are destroyed.

One might worry that by heating the interfaces are destroyed, but crystal structures are formed which induce perpendicular anisotropy. To study the change in crystal structure, we measured the samples by high-angle-XRD, so that we are sensitive to Angstrom spacing (Figure 9). In the annealed sample, we can find a strong reflection peak around 41.7 degrees in the 2 θ axis. This peak can be characterized to a specific Co-Pt (111) crystal plane (face centered cubic, fcc). It suggests that indeed a new crystalline structure of fct Co-Pt was formed in the film. This crystal exhibits however magnetic anisotropy in the [001] direction, i.e., there are tilted magnetic easy axes in the film (not perpendicular, not in plane). So there is no risk that after excessive heating the perpendicular anisotropy can be restored by crystallisation.

We envisage that heating of the magnetic dots will be realised by passing a current from the probe tip to the dot. It has been shown in earlier work that these currents are even capable of evaporating the material, so the energy density is sufficiently high [36, 35]. This method is not only limited to probe storage however. Active research is being performed into hard disks with heat assisted writing strategies [28]. It is not fundamentally impossible that the supplied energy can be high enough to modify the magnetic properties of the disk permanently. In principle this method could therefore also be used in magnetic disk drives, although the implementation would be far more difficult.

More research will be needed to determine the time required, the amount of energy dissipated, the wear on the tip, and the effect of heating one dot on the neighbouring dots. Especially the last effect could be detrimental, since the magnetic state, or even the write-ability of the adjacent dot could be affected. However, it is not unlikely that by tailoring the materials and layer structures, the interface mixing temperature can be reduced, which will reduce the risk of thermal erasure of the neighbouring dots. Furthermore, by properly designing the thermal properties of the dot and the substrate, most of the heat can be conducted away into the substrate, rather than dissipating away laterally, like is done in magneto-optic medium [29]. In this way the heated area can be limited and damage to adjacent dots can be reduced. In any case it will be necessary to use the write-once operation sparingly.

8 Discussion

We have described an experiment in material science and discussed a number of questions about how probe-based storage on a patterned medium can be used to build a tamper-evident storage device and file system. The experiments and discussion raise many more issues that must be addressed in future work. We describe the most relevant questions below.

Efficiency The storage efficiency of the system merits some discussion. Firstly, we have explained the low level system operations using a simple Manchester encoding for the hash. For large N the amount of space wasted is negligible (1 block out of 2^N), but the price to pay is lack of flexibility. For small values of N we could employ more efficient coding techniques [33].

Secondly, the storage system as we have described it behaves as mass storage that can be read and written any number of times as one would expect, except that once an area has been heated, it can no longer be rewritten with impunity. This means that over the lifetime of the device,

the read/write area gradually shrinks, and the read-only area grows, until the device has become a pure read-only device. The medium can safely be decommissioned by the time all data has expired. This means that the lifetime of the data must be matched to the lifetime of the medium.

Deletion Once heated, data will remain until the medium is decommissioned. This is not desirable if there is a large variation in the lifetime of the data, particularly in cases where retention periods are carefully controlled by regulation. There are several ways to deal with this problem. Firstly, data could be written encrypted, disposing of the encryption key as soon as the expiry date of the data is reached [8]. Secondly, it is possible to implement a physical shred operation on the device (similar to what has been achieved for optical storage [45]), which in our case would physically destroy the expired data by precise local heating. However, both approaches are vulnerable to attacks by a dishonest CEO and as such not wholly satisfactory. We would advocate data to be segregated by expiry date, thus making it possible to take a device physically out of service. Given the enormous volume of data subject to compliance regulation [54] this should be possible to arrange.

Forensics A typical server is responsible for so much data that the traditional disk imaging approach, which copies an entire disk at the lowest level possible (i.e., including unused and bad blocks), is becoming infeasible. Firstly the volume of data may be prohibitively large, and secondly, to image the disks the server must be stopped, possibly for hours, thus losing valuable production time. Live forensics methods [1] would benefit from a storage device that can be instructed to heat evidence without having to copy it. One of the most difficult problems in this field is to speed up the collection of evidence [9] in a kind of digital evidence bag. Our heated files could be the basis of such an evidence bag. It should be kept in mind that a forensic investigation carried out by the police is relatively rare, and probably still requires whole disk imaging. A forensic investigation by company staff is more common, since companies will try to deal with the problems such as harassment, and theft in house. Problems such as child pornography and money laundering must always be reported to the police [13].

We are confident that even a skilled focused ion beam (FIB) operator would find it difficult to reconstruct a perfect out-of-plane dot because she would have to remove the debris of an in-plane dot first, and then deposit several thin Co and Pt layers in a sub-micron area with the correct delicate layer structure to obtain perpendicular anisotropy, just to reconstruct one dot. Using magnetic imaging techniques [27], a forensics team would probably have no difficulty identifying a reconstructed out-of-plane dot from an original out-of-plane dot.

Tamper-evident storage as a building block Our system offers tamper-evident storage, which could be used as a building block in other systems. For example the idea of self-securing storage [47] takes the view that the storage system should place only limited trust in the host that controls it, since the host is more likely to become compromised than the storage system. Thus the storage system itself maintains a log of the instructions it is given, and ensures that earlier versions of any file (within a given time window) can be recovered. Our approach could strengthen the defences of a self-securing storage device because the logs can be heated.

9 Conclusions and future work

Probe storage on patterned media is a promising technology for developing tamper-evident storage. The capacity of such devices will be huge, and the tamper evidence is good. The measurements reported in the paper demonstrate that in principle it is possible to use a patterned magnetic medium in two essentially different ways: for normal read-write purposes and for read-only purposes after the data has been heated. It is physically impossible to alter the data without being detected after the heat operation has been used. We discuss the main issues that must be addressed when designing a device and a file system for tamper-evident SERO storage. The strong point of the SERO approach is its combination of the advantages of WORM storage with the advantages of WMRM storage.

We have identified the most relevant issues in the design of the system. However, much work remains to be done. On the software side we plan to design and build a simulation of the device and the file system, such that we can study the performance/security tradeoffs. The next step would be to develop a time-accurate emulator for the device, as well as an implementation of the file system to validate the simulation results. The time-accurate emulator could probably be built using anti-fuse based write once semiconductor memory technology as used in FPGAs. On the hardware side we plan to develop materials that change magnetic properties by interface mixing at lower temperatures, and tips that generate enough heat for interface mixing, studying the efficiency and reliability of the mechanisms involved.

10 Acknowledgements

We thank Sebastiaan Konings, Rogelio Murillo, and Takahiro Onoue for their help with the measurements. Jeroen Doumen, Sape Mullender, and Berend-Jan van der Zwaag provided helpful comments on the paper. The efforts of our shepherd Petros Maniatis are gratefully acknowledged.

References

[1] ADELSTEIN, F. Live forensics: diagnosing your system without killing it first. *Commun. ACM 49*, 2 (Feb 2006), 63–66.

[2] ALON, N., KAPLAN, H., KRIVELEVICH, M., MALKHI, D., AND STERN, J. Scalable secure storage when half the system is faulty. *Information and Computation 174*, 2 (May 2002), 203–213.

[3] ANDERSON, R. J., AND KUHN, M. G. Tamper resistance - A cautionary note. In *2nd Int. Usenix Workshop on Electronic Commerce* (Oakland, California, Nov 1996), USENIX Association, pp. 1–11.

[4] ANDERSON, R. J., AND KUHN, M. G. Low cost attacks on tamper resistant devices. In *Security protocols: 5th Int. Workshop* (Paris, France, Apr 1997), M. Lomas and B. Christianson, Eds., vol. LNCS 1361, Springer, pp. 125–136.

[5] APVRILLE, A., HUGHES, J., AND GIRIER, V. Streamed or detached triple integrity for a time stamped secure storage system. In *1st Int. IEEE Security in Storage Workshop (SiSW)* (Greenbelt, Maryland, Dec 2002), IEEE Computer Society, pp. 53–64.

[6] BALDWIN, A., AND SHIU, S. Enabling shared audit data. *International Journal of Information Security 4*, 4 (Oct 2005), 263–276.

[7] BOBETH, M., HECKER, M., POMPE, W., SCHNEIDER, C. M., THOMAS, J., ULLRICH, A., AND WETZIG, K. Thermal stability of nanoscale Co/Cu multilayers. *Zeitschrift fuer Metallkunde/Materials Research and Advanced Techniques 92*, 7 (2001), 810–819.

[8] BONEH, D., AND LIPTON, R. J. A revocable backup system. In *6th USENIX Security Symp. Focusing on Applications of Cryptography* (San Jose, California, Jul 1996), USENIX Association, pp. 91–96.

[9] CASEY, E. Investigating sophisticated security breaches. *Commun. ACM 49*, 2 (Feb 2006), 48–55.

[10] GENDRON, Y. Reforming auditor independence: Voicing and acting upon auditors' concerns and criticisms. *Advances in Public Interest Accounting 12* (2006), 103–118.

[11] GORDON, L. A., LOEB, M. P., LUCYSHYN, W., AND RICHARDSON, R. *10th Annual CSI/FBI Computer crime and security survey*. Computer Security Institute, San Francisco, California, 2005.

[12] GUTMANN, P. Secure deletion of data from magnetic and solid-state memory. In *6th USENIX Security Symp.* (San Jose, California, Jul 1996), USENIX Association, pp. 77–89.

[13] HAGGERTY, J., AND TAYLOR, M. Managing corporate computer forensics. *Computer Fraud & Security 2006*, 6 (Jun 2006), 14–16.

[14] HASAN, R., MYAGMAR, S., LEE, A. J., AND YURCIK, W. Toward a threat model for storage systems. In *1st ACM Workshop on Storage Security and Survivability (StorageSS)* (Fairfax, Virginia, Nov 2005), ACM, pp. 94–102.

[15] HASAN, R., TUCEK, J., STANTON, P., YURCIK, W., BRUMBAUGH, L., ROSENDALE, J., AND BOONSTRA, R. The techniques and challenges of immutable storage with applications in multimedia. In *Storage and Retrieval Methods and Applications for Multimedia*, R. W. Lienhart, N. Babaguchi, and E. Y. Chang, Eds., vol. 5682. SPIE, Jan 2005, pp. 41–52.

[16] HASAN, R., AND YURCIK, W. A statistical analysis of disclosed storage security breaches. In *2nd ACM Workshop on Storage Security and Survivability (StorageSS)* (Alexandria, Virginia, Oct 2006), ACM, pp. 1–8.

[17] HASAN, R., YURCIK, W., AND MYAGMAR, S. The evolution of storage service providers: techniques and challenges to outsourcing storage. In *1st ACM Workshop on Storage Security and Survivability (StorageSS)* (Fairfax, Viginia, Nov 2005), ACM, pp. 1–8.

[18] HONG, B., WANG, F., BRANDT, S. A., LONG, D. D. E., AND SCHWARZ, T. J. E. Using MEMS-based storage in computer systems–MEMS storage architectures. *Trans. Storage 2*, 1 (Feb 2006), 1–21.

[19] HSU, W. W., AND ONG, S. WORM storage is not enough. *IBM Systems Journal 46*, 2 (Apr 2007), 363–372.

[20] HURLEY, J. The CSO's security compliance agenda: Benchmark research report. *Computer Security Journal 22*, 1 (Dec 2006), 37–44.

[21] JAQUETTE, G. A. Tamper resistant write once recording of a data storage cartridge having rewritable media. International Business Machines Corporation (Armonk, NY), Mar 2007. Patent Nr. 7,193,803.

[22] KIM, Y.-S., JANG, S., LEE, C. S., JIN, W.-H., CHO, I.-J., HA, M.-H., NAM, H.-J., BU, J.-U., CHANG, S.-I., AND YOON, E. Thermo-piezoelectric Si_3N_4 cantilever array on CMOS circuit for high density probe-based data storage. *Sensors and Actuators, A: Physical 135*, 1 (Mar 2007), 67–72.

[23] KURTAS, E. M., ERDEN, M. F., AND YANG, X. Future read channel technologies and challenges for high density data storage applications. In *IEEE Int. Conf. on Acoustics, Speech and Signal Processing (ICASSP)* (Philadephia, Pennsylvania, Mar 2005), IEEE, pp. V737–V740.

[24] LI, J., KROHN, M., MAZIÈRES, D., AND SHASHA, D. Secure untrusted data repository (SUNDR). In *6th Symp. on Operating Systems Design and Implementation (OSDI)* (San Francisco, California, 2004), USENIX Association, pp. 9–9.

[25] LUTTGE, R., VAN WOLFEREN, H. A. G. M., AND ABELMANN, L. Nanolithography for patterned magnetic data storage media. *Journal of Vacuum Technolgy B* (2007), accepted for publication.

[26] MANIATIS, P., AND BAKER, M. Secure history preservation through timeline entanglement. In *11th USENIX Security Symp.* (San Francisco, California, Aug 2002), USENIX Association, pp. 297–312.

[27] MAYERGOYZA, I. D., SERPICO, C., KRAFFT, C., AND TSE, C. Magnetic imaging on a spin-stand. *J. of Applied Physics 87*, 9 (May 2000), 6824–6826.

[28] MCDANIEL, T. W., CHALLENER, W. A., AND SENDUR, K. Issues in heat-assisted perpendicular recording. *IEEE Transactions on Magnetics 39*, 4 (2003), 1972–1979.

[29] MCDANIEL, T. W., AND SEQUEDA, F. O. Design material selection for a thin film magneto-optic disk. *Applied physics communications 11*, 4 (1992), 427–445.

[30] MIN, D.-K., AND HONG, S. Design and analysis of the position detection algorithm for a probe storage. *IEEE Sensors Journal 6*, 4 (Aug 2006), 1010–1015.

[31] MOLNAR, D., KOHNO, T., SASTRY, N., AND WAGNER, D. Tamper-evident, history-independent, subliminal-free data structures on PROM storage -or- how to store ballots on a voting machine (extended abstract). In *IEEE Symp. on Security and Privacy (S&P)* (Berkeley, California, May 2006), IEEE Computer Society, pp. 365–370.

[32] MORALEJO, S., NO, F. J. C., REDONDO, C., JI, R., NIELSCH, K., ROSS, C. A., AND NO, F. C. Fabrication and magnetic properties of hexagonal arrays of NiFe elongated nanomagnets. *Journal of Magnetism and Magnetic Materials 316*, 2 (Sep 2007), e44–e47.

[33] MORAN, T., NAOR, M., AND SEGEV, G. Deterministic History-Independent strategies for storing information on Write-Once memories. In *34th Int. Colloquium on Automata, Languages and Programming (ICALP)* (Wroclaw, Poland, Jul 2007), vol. LNCS 4596, Springer, pp. 305–315.

[34] NABERHUIS, S. Probe-based recording technology. *J. of Magnetism and Magnetic Materials 249*, 3 (Sep 2002), 447–451.

[35] ONOUE, T., SIEKMAN, M., ABELMANN, L., AND LODDER, J. C. Heat assisted magnetic probe recording onto a thin film with perpendicular magnetic anisotropy. *Journal of Applied Physics D* (2007), accepted for publication.

[36] ONOUE, T., SIEKMAN, M. H., ABELMANN, L., AND LODDER, J. C. Probe recording on CoNi/Pt multilayered thin films by using an MFM tip. *Journal of Magnetism and Magnetic Materials 272-276*, III (May 2004), 2317–2318.

[37] PATZAKIS, J. New accounting reform laws push for Technology-Based document retention practices. *Int. Journal of Digital Evidence 2*, 1 (Spring 2003), paper 2.

[38] PORTHUN, S., ABELMANN, L., AND LODDER, C. Magnetic force microscopy of thin film media for high density magnetic recording. *J. of Magnetism and Magnetic Materials 182*, 1-2 (Feb 1998), 238–273.

[39] POZIDIS, H., BÄCHTOLD, P., BONAN, J., CHERUBINI, G., ELEFTHERIOU, E., DESPONT, M., DRECHSLER, U., DÜRIG, U., GOTSMANN, B., HÄBERLE, W., HAGLEITNER, C., JUBIN, D., KNOLL, A., LANTZ, M. A., PANTAZI, A., ROTHUIZEN, H. E., SEBASTIAN, A., STUTZ, R., AND WIESMANN, D. W. Scanning probes entering data storage: From promise to reality. In *IEEE Conf. on Emerging Technologies - Nanoelectronics* (Singapore, Jan 2006), IEEE, pp. 39–44.

[40] QUINLAN, S., AND DORWARD, S. Venti: A new approach to archival data storage. In *1st USENIX Conf. on File and Storage Technologies (FAST)* (Monterey, California, Jan 2002), USENIX Association, pp. 89–101.

[41] RETTNER, C. T., ANDERS, S., BAGLIN, J. E. E., THOMSON, T., AND TERRIS, B. D. Characterization of the magnetic modification of Co/Pt multilayer films by He^+, Ar^+, and Ga^+ ion irradiation. *Applied Physics Letters 80*, 2 (Jan 2002), 279–281.

[42] ROSENBLUM, M., AND OUSTERHOUT, J. K. The design and implementation of a log-structured file system. *ACM Trans. Comput. Syst. 10*, 1 (Feb 1992), 26–52.

[43] SARAJLIC, E., BERENSCHOT, E., TAS, N. R., FUJITA, H., KRIJNEN, G., AND ELWENSPOEK, M. C. Fabrication and characterization of an electrostatic contraction beams micromotor. In *IEEE Int. Conf. on Micro Electro Mechanical Systems (MEMS)* (Istanbul, Turkey, Jan 2006), IEEE, pp. 814–817.

[44] SELTZER, M. I., SMITH, K. A., BALAKRISHNAN, H., CHANG, J., MCMAINS, S., AND PADMANABHAN, V. N. File system logging versus clustering: A performance comparison. In *Technical Conf. on UNIX and Advanced Computing Systems* (New Orleans, Louisiana, Jan 1995), USENIX Association, pp. 249–264.

[45] SKEETER, B. J., WORBY, B. L., HOLSTINE, K. R., AND BOLT, D. A. Optical disk shred operation with detection. United States Patent and Trademark Office, Mar 2007. Patent Application Nr. 20070047395.

[46] SPOERL, K., AND WELLER, D. Interface anisotropy and chemistry of magnetic multilayers: Au/Co, Pt/Co and Pd/Co. *Journal of Magnetism and Magnetic Materials 93* (Feb 1991), 379–385.

[47] STRUNK, J. D., GOODSON, G. R., SCHEINHOLTZ, M. L., SOULES, C. A., AND GANGER, G. R. Self-Securing storage: Protecting data in compromised systems. In *Foundations of Intrusion Tolerant Systems (OASIS)*. IEEE Computer Society, 2003, pp. 195–209.

[48] TAS, N. R., WISSINK, J., SANDER, A. F. M., LAMMERINK, T. S. J., AND ELWENSPOEK, M. C. Modeling, design and testing of the electrostatic shuffle motor. *Sensors and Actuators A (Physical) 70*, 1-2 (Oct 1998), 171–178.

[49] TAYLOR, M. The EU data retention directive. *Computer Law & Security Report 22*, 4 (2006), 309–312.

[50] TERRIS, B. D., FOLKS, L., WELLER, D., BAGLIN, J. E. E., KELLOCK, A. J., ROTHUIZEN, H., AND VETTIGER, P. Ion-beam patterning of magnetic films using stencil masks. *Applied Physics Letters 75*, 3 (Jul 1999), 403–405.

[51] TERRIS, B. D., AND THOMSON, T. Nanofabricated and self-assembled magnetic structures as data storage media. *J. of Physics D: Applied Physics 38*, 12 (Jun 2005), R199–R222.

[52] TERRIS, B. D., THOMSON, T., AND HU, G. Patterend media for future magnetic data storage. *Microsystem Technologies 13*, 2 (Jan 2007), 189–196.

[53] VALLEJO, R. M., SIEKMAN, M. H., BOLHUIS, T., ABELMANN, L., AND LODDER, J. C. Thermal stability and switching field distribution of CoNi/Pt patterned media. *Microsystem Technologies 13*, 2 (Jan 2007), 177–180.

[54] VAN WANROOIJ, W., AND PRAS, A. Data on retention. In *16th IFIP/IEEE Int. Workshop on Distributed Systems: Operations and Management (DSOM)* (Barcelona, Spain, Oct 2005), vol. LNCS 3775, Springer, pp. 60–71.

[55] WANG, Y., AND ZHENG, Y. Fast and secure magnetic WORM storage systems. In *2nd IEEE Int. Security in Storage Workshop (SISW)* (Washington, DC, Oct 2003), IEEE Computer Society, pp. 11–11.

[56] WINARSKI, C. J., AND DIMITRI, K. E. Write-once read-many hard disk drive. International Business Machines Corporation (Armonk, NY), Apr 2005. Patent Nr. 6,879,454.

[57] ZHU, Q., AND HSU, W. W. Fossilized index: the linchpin of trustworthy non-alterable electronic records. In *ACM Int. Conf. on Management of Data (SIGMOD)* (Baltimore, Maryland, Jun 2005), ACM, pp. 395–406.