LONG TERM DIGITAL PRESERVATION

Syeda Majeed Muneer
Green Fort Engineering College,
Bandlaguda ,Hyderabad, Andhra Pradesh,
syeda_mm@yahoo.com

Abstract . The field of digital preservation is being defined by a set of standards developed top-down, starting with an abstract reference model (OAIS) and gradually adding more specific detail. Systems claiming conformance to these standards are entering production use. Work is underway to certify that systems conform to requirements derived from OAIS.

The fundamental goal of these systems is to ensure that the information they contain remains accessible for the long term. We develop a parallel set of requirements based on observations of how existing systems handle this task, and on an analysis of the threats to achieving that goal. On this basis we suggest disclosures that systems should provide as to how they satisfy their goals.

Dynamic Preservation

The storage of digital data will require a dynamic form of preservation, and a new definition of "archival" may have to be developed. The concept of long-term storage of a paper- or photographic-based item that remains unchanged over time may not be applicable with electronic publishing. Instead, the information will have to be re-recorded on new media to be used with existing file formats and computer operating systems as storage media degrade and systems, formats, and encoding systems evolve.

There are programs that convert from one encoding system to another. Over time, these programs will become more reliable and allow data to be reformatted to the current standard approach. But the conversion will have to take place in order to keep the information in a "current" format. Usually there is a two-year transition between one form of storage and its successor. This is both a management and a technical issue and tracks the organizational issues—the permanence

and commitment of the archiving organization—cited in the previous section.

1. Open Archival Information System

The field of digital preservation systems has been defined by the Open Archival Information System (OAIS) standard ISO 14721:2003, which provides a high-level reference model. This model has been very useful. It identifies the participants, describes their roles and responsibilities, and classifies the types of information they exchange. However, because it is only a high-level reference model, almost any system capable of storing and retrieving data can make a plausible case that it satisfies the OAIS conformance requirements.

Several digital preservation systems are in, or are about to enter, production use preserving content society deems important. It seems an opportune moment to complement the OAIS top-down effort to generate requirements for such systems with a bottom-up approach.

2. Goal

The goal of a digital preservation system is that the information it contains remains accessible to users over a long period of time.

The key problem in the design of such systems is that the period of time is very long, much longer than the lifetime of individual storage media, hardware and software components, and the formats in which the information is encoded. If the period were shorter, it would be simple to satisfy the requirement by storing the information on suitably long-lived media embedded in a system of similarly long-lived hardware and software.

No media, hardware or software exists in whose longevity designers can place such confidence. They must therefore anticipate failures and obsolescence, designing systems with three key properties:

- At minimum, the system must have no single point of failure; it must tolerate the failure of any individual component. In general, systems should be designed to tolerate more than one simultaneous failure.
- Media, software and hardware must flow through the system over time as they fail or become obsolete, and are replaced. The

system must support diversity among its components to avoid monoculture vulnerabilities, to allow for incremental replacement, and to avoid vendor lock-in.

- Most data items in an archive are accessed infrequently. A system that detected errors and failures only upon user access would be vulnerable to an accumulation of latent errors]. The system must provide for regular audits at intervals frequent enough to keep the probability of failure at acceptable levels.

3. Threats

To assist in the development of these threat models, we present the following taxonomy of threats. Threat models should either include or explicitly exclude at least these threats:

- Media Failure. All storage media must be expected to degrade with time, causing irrecoverable bit errors, and to be subject to sudden catastrophic irrecoverable loss of bulk data such as disk crashes or loss of off-line media
- Hardware Failure. All hardware components must be expected to suffer transient recoverable failures, such as power loss, and catastrophic irrecoverable failures, such as burnt-out power supplies.
- Software Failure. All software components must be expected to suffer from bugs that pose a risk to the stored data.
- Communication Errors. Systems cannot assume that the network transfers they use to ingest or disseminate content will either succeed or fail within a specified time period, or will actually deliver the content unaltered. A recent study "suggests that between one (data) packet in every 16 million packets and one packet in 10 billion packets will have an undetected checksum error
- Failure of Network Services. Systems must anticipate that the external network services they use, including resolvers such as those for domain names] and persistent URLs , will suffer both transient and irrecoverable failures both of the network services and of individual entries in them. As examples, domain names will vanish or be reassigned if the registrant fails to pay the registrar, and a persistent URL will fail to resolve if the resolver

service fails to preserve its data with as much care as the digital preservation service.

- Media & Hardware Obsolescence. All media and hardware components will eventually fail. Before that, they may become obsolete in the sense of no longer being capable of communicating with other system components or being replaced when they do fail. This problem is particularly acute for removable media, which have a long history of remaining theoretically readable if only a suitable reader could be found.
- Software Obsolescence. Similarly, software components will become obsolete. This will often be manifested as format obsolescence when, although the bits in which some data was encoded remain accessible, the information can no longer be decoded from the storage format into a legible form.
- Operator Error. Operator actions must be expected to include both recoverable and irrecoverable errors. This applies not merely to the digital preservation application itself, but also to the operating system on which it is running, the other applications sharing the same environment, the hardware underlying them, and the network through which they communicate.
- Natural Disaster. Natural disasters, such as flood, fire and earthquake must be anticipated. Other types of threats, such as media, hardware and infrastructure failures, will typically manifest then.
- External Attack. Paper libraries and archives are subject to malicious attack; there is no reason to expect their digital equivalents to be exempt. Worse, all systems connected to public networks are vulnerable to viruses and worms. Digital preservation systems must either defend against the inevitable attacks, or be completely isolated from external networks.
- Internal Attack. Much abuse of computer systems involves insiders, those who have or used to have authorized access to the system. Even if a digital preservation system is completely isolated from external networks, it must anticipate insider abuse.
- Economic Failure. Information in digital form is much more vulnerable to interruptions in the money supply than information on paper. There are ongoing costs for power, cooling, bandwidth, system administration, domain registration,

and so on. Budgets for digital preservation must be expected to vary up and down, possibly even to zero, over time.

- Organizational Failure. The system view of digital preservation must include not merely the technology but the organization in which it is embedded. These organizations may die out, perhaps through bankruptcy, or their missions may change. This may deprive the digital preservation technology of the support it needs to survive. System planning must envisage the possibility of the asset represented by the preserved content being transferred to a successor organization, or otherwise being properly disposed of. For each of these types of failure, it is necessary to trade off the cost of defense against the level of system degradation under the threat that is regarded as acceptable for that cost.

The degradation may be evaluated in terms of the following questions:

- What fraction of the system's content is irrecoverably lost?
- What fraction of the user population suffers what delay in accessing the impaired but recoverable fraction of the system's content?

Designers should be aware that these threats are likely to be highly correlated. For example, operators stressed by responding to one threat, such as hardware failure or natural disaster, are far more likely to make mistakes than they are when things are calm .Equally, software failures are likely to be triggered by hardware failures, which present the software with conditions its designers failed to anticipate and under which it has never been tested. Mean Time between Failure estimates are typically based on the assumption that failures occur independently even small correlations between the failures can render the estimates wildly optimistic.

4 Strategies

We now survey the strategies that system designers can employ to survive these threats.

4.1 Replication

The most basic strategy exploits the fundamental attribute that distinguishes digital from analog information, the possibility of copying it without loss of information, to store multiple replicas of the information to be preserved. Clearly, a single replica subject to the threats above has a low probability of long-term survival, so replication is a necessary attribute of a digital preservation system but it is far from sufficient, as anyone who has had trouble restoring a file from a backup copy can appreciate.

4.2 Migration

The creation and management of replicas that lies at the base of a digital preservation system involve processes of migration: between instances of the same type of storage medium, from one medium to another, and from one format to another. Migrations can be exceptional events, handled by the system operators perhaps on a batch basis, or routine events, handled automatically by the system without operator intervention.

Migration between instances of the same medium, for example network transfers from mass storage at one site to mass storage at another, is typically used to implement replication and to refresh media. All systems employing replication appear to use it. It can be effective against media and hardware failures.

The classic example of migration between media is tape backup, used by many systems. It can be effective against media, hardware and software failures and obsolescence.

4.3 Transparency

Digital preservation technology shares some attributes with encryption technology. Perhaps the most important is that in both cases the customer has no way to be sure that the system will continue to perform its assigned task of preserving or preventing access to the system's content, (as the case may be). An encryption system may be broken or misused and therefore reveal content. However long you

watch a digital preservation system, you can never be sure it will continue to provide access in the future.

In both cases transparency is key to the customer's confidence in the system. Just as open source, open protocols and open interfaces provide the basis for the public review that allows customers to have confidence in encryption systems such as AES, similar reviews based on similar introspection are needed if customers are to have confidence that their digital preservation systems will succeed. Examples of open-source digital preservation systems include the LOCKSS system and MIT's DSpace system

An essential precaution against the software of a digital preservation system becoming obsolete is that it be preserved with at least as much care as the information that it is preserving. Open source makes this easy. Open protocols and open interfaces are a necessary but not sufficient precondition for diverse implementations of system components.

Despite the best efforts of system designers and implementers, and despite the certifications expected to be available for digital preservation systems, data will be lost. To improve the performance of systems over time, it is essential that lessons be learned from incidents that risk or cause data loss. We can expect that such incidents will be infrequent, making it important to extract the maximum benefit from each. Past incidents suggest that an institution's reaction to data loss is typically to cover it up, preventing the lessons being learned. This paper shows this problem, in that we have no way to cite or discuss the details of several incidents of this kind known to practitioners via the grapevine.

4.4 Diversity

Systems lacking diversity, in the extreme monocultures, are vulnerable to catastrophic failure. Ideally, a digital preservation system should provide diversity at all levels, but most systems provide it at only a few, citing cost considerations:

- Most systems use off-line media to provide diversity in media for storing replicas, and to isolate some replicas as far as possible from network-borne threats.

- Many systems use geographic dispersion of on-line replicas to counter threats of natural disaster (e.g. DAITSS and the BL's system). Most systems using off-line backups store them off-site, again providing geographic diversity. The LOCKSS system has replicas scattered around the world.
- The BL's system is an example of explicit planning for diversity in hardware and vendors to support a process of "rolling procurement" and "rolling replacement". The library's continuous collection program means that the system must grow incrementally, its availability requirements mean that replicas must be replaced incrementally (a sound approach to preventing correlated administration errors ,and its long planned lifetime means that vendor lock-in is unacceptable.
- Similar considerations apply to software. There should be a diversity of software among the replicas. The BL's system anticipates that at any one time different replicas will be running earlier or later versions of their management software, and that the different manufacturers of the underlying storage technologies will provide some level of software diversity.
- The BL and LOCKSS systems are examples of diversity of system administration. Each replica is independently administered; there is no single password whose compromise could affect all replicas. Given the prevalence of human error and insider abuse of computer systems, unified system administration should be an unacceptable feature of digital preservation.
- The Portico and LOCKSS systems are striving for diversity of funding. As regards the peers actually storing content, the LOCKSS system is already diverse; each peer is owned and supported by its host library so no single budget cut or administrative decision can cause the system as a whole to lose content. Portico as a whole and the team that supports the LOCKSS system are both in the process of transition from sole-source grant funding, to support by the libraries using the service. In this model no single budget decision would affect more than a few percent of the team's total income.
- The risk of inadequate diversity is particularly acute for networked computer systems such as digital preservation systems. Techniques have been available for some years by

which an attacker can compromise in a very short period of time almost all systems that share a single vulnerability]. Worms such as Slammer have used them in the wild. System designers would be unwise to believe that they can construct, configure, upgrade, and expand systems for the long term that would not be exploitable in this way.

4.5 Economy

Techniques for reducing the cost of systems are always valuable, but they are especially valuable for digital preservation systems. Few if any institutions have an adequate budget for digital preservation; they must practice some form of economic triage. They will preserve less content than they should, or take greater risks with it, to meet the budget constraints. Reduced costs of acquiring and operating the system flow directly into some combination of more content being preserved or lower risk to the preserved content.

We discuss cost reduction at each of the stages of digital preservation, ingesting the content, preserving it, and disseminating it to the eventual readers. At each stage we identify a set of cost components, not all of which are applicable to all systems.

4.6 Economy in Preservation

The cost of preserving the content and its associated metadata has three components: the cost of acquiring and continually replacing the necessary hardware and software; operational costs such as power, cooling, bandwidth, staff time and the audits needed to assure funders that they are getting their money's worth; and the cost of the necessary format migrations. Systems with few replicas have to be very careful with each of them, using very reliable enterprise-grade storage hardware and expensive off-line backup procedures.

- Storage
- The economics of high-volume manufacturing means that consumer-grade disk drives are vastly cheaper and only a little less reliable than enterprise-grade drives. Based on Seagate's

Mean Time To Failure (MTTF) specifications, a 200GB consumer Barracuda drive has a 7% probability of failing in a 5-year service life where a 146GB enterprise Cheetah has a 3% probability of failing .Consider, however, that the Cheetah costs about $8.20/GB whereas the Barracuda costs only about $0.57/GB (Prices from TigerDirect.com 6/13/05).

- In addition to the severe failures predicted by the MTTF specifications, drives specify a rate of unrecoverable bit errors, 10-14 for the Barracuda and 10-15 for the Cheetah. This is a very low probability, but the disks contain over 1012 bits. About one in every 62 attempts to read every bit from a Barracuda will encounter an unrecoverable bit error; the corresponding figure for the Cheetah is about 1 in 860. The disks also transfer data very fast. Even if the drive averages 99% idle, over a 5-year service life the Barracuda will suffer about 8 and the Cheetah about 6 unrecoverable bit errors. The relationships between these specified error rates and those experienced in practice are currently being studied. Several large disk farms report more disk failures than would be predicted from the specified MTTF numbers. Although an experiment with short-lived data encountered fewer unrecoverable bit errors than predicted], a preliminary analysis of data from the Internet Archive suggests that long-lived data is more at risk.
- Because the in-service failure probability even for expensive drives is so high, enterprise storage systems use replication techniques such as RAID. These "internal" replicas are costly but of little value in digital preservation .They provide high availability, but spending heavily to improve availability is hard to justify for systems such as dark archives where the probability of a user access during the recovery time from a disk failure is low. They improve the reliability of the data, but not enough to justify their cost. The replicas are tightly coupled to each other and are thus subject to many correlated failure modes .
- Another reason why digital preservation systems might not want to use enterprise-grade hardware is the cost of power and cooling, which can be substantial over the long lifetime of the system. Enterprise hardware has to meet exacting performance

targets and typically does so by using power extravagantly. Preservation systems have much lower performance targets and can save power both by using consumer-grade hardware and by under-clocking it. The Internet Archive has led the way in engineering low-power storage systems in this way, spinning off a company called Capricorn Technologies to build them.

- Operation
- As with any activity involving humans, system administration is expensive and error-prone. Yet digital preservation requires very low rates of system administration error over very long periods of time. The obvious technique is to assign each replica to its own administrative domain, so that a single administrative error can affect at most one replica. In a peer-to-peer system, such as LOCKSS, this is naturally the case; other distributed architectures may require more costly measures to achieve separate administrative control of each replica.
- Attempts are sometimes made to reduce the visible cost of system administration by running the digital preservation system as one of a large number of services offered by a large shared server, or as one of a large number of services sharing a storage infrastructure such as the Storage Resource Broker. This is often a false economy. Layering systems in this way adds significant complexity and introduces many failure modes, including hardware, software, and network, operational and administrative failures, which are absent or much less significant in dedicated systems. These add greatly to the risks to the stored content. In particular, it is impossible to prevent errors in other systems, which share the infrastructure but are unrelated to digital preservation, damaging preserved content. Machine and administrative boundaries can be very effective at preventing faults propagating.
- The only approach to reducing operational costs while maintaining low rates of operator error is to eliminate, as far as possible, the system's need for operator intervention. The large number of replicas envisaged for the LOCKSS system forced it to adopt this "network appliance" approach, which has been successful in making the per-replica cost of administration affordable.
- Format Migration

- Format migration involves both engineering costs, in implementing the necessary format converters, and operational costs, in applying them to the preserved content. The engineering costs will be equivalent whatever approach is taken, but the operational costs will vary. The operational cost of batch migration may be large and will be incurred at unpredictable intervals, making it difficult to budget. This raises the specter of economic triage, discarding material whose migration cost exceeds its perceived value. The operational costs of the LOCKSS approach of transparent on-access migration are minimal.

4.7 Sloth

Digital preservation is almost unique among computer applications in that speed is neither a goal nor even an advantage. There is normally no hurry to ingest content, and no large group of readers impatient for it to be disseminated. As described above, the lack of a need for speed can be leveraged to reduce the cost of hardware, power and cooling. It can also reduce the cost of system administration by increasing the window during which administrator response is required. Tasks that can be scheduled flexibly and well in advance are much cheaper than those requiring instant action. But the most important reason for sloth is that a system that operates fast will tend to fail fast, especially under attack. Slow failure, with plenty of warning during the gradual failure, is an important attribute of digital preservation systems, as it allows time for recovery policies to be implemented before failure is total.

5 Requirements

Digital preservation systems have a simple goal, that the information they contain remains accessible to users over a long period of time. In addressing this goal they are subject to a wide range of threats, not all of which are relevant to all systems. We have also shown a wide range of strategies, each of which is used by at least one current system. But the various systems use various techniques to implement each strategy.

The failure of a digital preservation system will become evident in finite time, but its success will forever remain unproven. Given this, and the diversity of threats and strategies, it seems premature to be imposing requirements in terms of particular technical approaches. Rather, systems should be required to disclose their solutions to the various threats, and other aspects of the strategies they are pursuing. This will allow certification against a checklist of required disclosures, and allow customers to make informed decisions as to how their digital assets may most economically reach an adequate level of preservation against the threats they consider relevant.

Here is the list of suggested disclosures our bottom-up process generated:

1. Systems should have an explicit threat model, disclosing against which of the threats of they are attempting to preserve content, and how they are addressing each threat.
2. Systems should disclose how their replicas are created and administered, and how any damage is detected and repaired.
3. Systems should disclose the policies and mechanisms they implement to protect intellectual property. Specifically:
    - If a system is intended to hold only material when the copyright belongs to the host institution, it should disclose how it assures that this is in fact the case.
    - If a system is intended to hold material whose copyright belongs to others, it should disclose information about the agreement under which it is held, such as whether and under what terms the agreement can be revoked by the copyright holder, and how the permission granted is verified, recorded as metadata and preserved.
    - If a system is intended to hold material not covered by copyright, such as US government documents within the US, it should disclose how it assures that this is verified, recorded as metadata and preserved.
4. Systems should disclose their external interfaces, in particular their SIP and DIP specifications. They should disclose whether, to assist external auditing, they are capable of disgorging a DIP identical to the SIP that caused the content in question to be

stored, including not just the content but also all the metadata originally provided (and none of the metadata that it subsequently acquired).
5. Systems should disclose their source code access policy, and how their source code is to be preserved.
6. Systems should disclose who will conduct audits, how they will be conducted, and to whom the results will be provided.
7. Systems should disclose their policy for handling incidents of data loss. To whom are such incidents reported and in what form?

The work underway to add certification requirements to OAIS is proceeding along similar lines, but from a top-down perspective. We note that, while there are strong relationships between the criteria in the current draft of these requirements and our suggested disclosures, there are very few exact correspondences.

7 References

1. ALESSANDRO SENSERINI, ROBERT B. ALLEN, GAIL HODGE, NIKKIA ANDERSON AND DANIEL SMITH, JR. Archiving and accessing web pages: The Goddard library web capture project. D-Lib Magazine 10, 11 (Nov. 2004).
2. BAKER, M., KEETON, K., AND MARTIN, S. Why Traditional Storage Systems Don't Help Us Save Stuff Forever. In Proc. 1st IEEE Workshop on Hot Topics in System Dependability (2005).
3. BUNGALE, P., GOODELL, G., AND ROUSSOPOULOS, M. Conservation vs. consensus in peer-to-peer preservation systems. In IPTPS (Feb. 2005). <http://iptps05.cs.cornell.edu/PDFs/CameraReady_214.pdf>.
4. CANTARA, L. Archiving Electronic Journals. <http://www.diglib.org/preserve/ejp.htm>, 2003.
5. HESLOP, H., DAVIS, S., AND WILSON, A. National Archives Green Paper: An Approach to the Preservation of Digital Records. <http://www.naa.gov.au/recordkeeping/er/digital_preservation/Green_Paper%25.pdf>, 2002.
6. JEROEN BEKAERT AND HERBERT VAN DE SOMPEL. A standards-based solution for the accurate transfer of digital assets.

D-Lib Magazine 6, 11 (June 2005). <doi:10.1045/june2005-bekaert>.
7. MENAFEE, S. Drivesavers cuts price for lost data recovery. <http://www.findarticles.com/cf_dls/m0NEW/n39/20324409/p1/article.jhtml>, Feb. 1998.
8. NASA. Aviation Safety Reporting System. <http://asrs.arc.nasa.gov/>.
9. NATIONAL LIBRARY OF AUSTRALIA. Preservation Metadata for Digital Collections. <http://www.nla.gov.au/preserve/pmeta.html>.
10. RONALD JANTZ AND MICHAEL J. GIARLO. Digital preservation: Architecture and technology for trusted digital repositories. D-Lib Magazine 11, 6 (June 2005). <doi:10.1045/june2005-jantz>.
11. ROSENTHAL, D. S. H. A Digital Preservation Network Appliance Based on OpenBSD. In Proceedings of BSDcon 2003 (San Mateo, CA, USA, Sept. 2003). <http://lockss.stanford.edu/david1.htm>.
12. ROSENTHAL, D. S. H., LIPKIS, T., ROBERTSON, T. S., AND MORABITO, S. Transparent format migration of preserved web content. D-Lib Magazine 11, 1 (Jan. 2005). <doi:10.1045/january2005-rosenthal