Threat Models for Digital Preservation
The LOCKSS and CLOCKSS Program

Victoria Reich, Director, LOCKSS Program, Stanford University
David S.H. Rosenthal, Chief Scientist, LOCKSS Program, Stanford University
www.lockss.org

Last year, in a report to the National Archives, a panel of the National Research Council stressed the importance for digital preservation systems to be explicit about their "threat model," the threats against which they do and do not protect content. Which threats to preserve against is a fundamental preservation system design decision.

As context for this presentation, the LOCKSS and CLOCKSS programs will be compared and contrasted as to ingest methods, scope of content, access models, and business plans.

The LOCKSS Program's list of threats and our key techniques for preserving against each is:

- **Media Failure**. Replication, auditing, media diversity and media migration.
- **Hardware Failure**. Replication, proactive monitoring (e.g. SMART), rolling procurement and hardware diversity.
- **Software Failure**. Simplicity, Open Source, randomization and software diversity.
- **Communication Errors**. End-to-end error detection, fault tolerant architectures.
- **Failure of Network Services**. System autonomy and fault tolerant architectures.
- **Media & Hardware Obsolescence**. Media migration, technology diversity and rolling procurement.
- **Software Obsolescence**. Format migration, software diversity and rolling upgrade policy.
- **Operator Error**. Fault tolerant architectures with independently administered, mutually suspicious replicas, dual-key authorization.
- **Natural Disaster**. Geographical distribution of independently administered replicas in fault-tolerant architectures.
- **External Attack**. Proactive security audits, software and hardware diversity, fault tolerant architectures with mutually suspicious, independently administered replicas.
- **Internal Attack**. Replicas distributed across jurisdictions, fault tolerant architectures with mutually suspicious, independently administered replicas.
- **Economic Failure**. Low cost technology and system design, high level of automation, distribution of replicas and administration across organizations.
- **Organizational Failure**. Distribution of replicas and administration across organizations, secession planning, DIP=SIP architecture.

The LOCKSS technology was designed around a generic threat model[1]. The status of both the LOCKSS and CLOCKSS systems and plans for improving both LOCKSS and CLOCKSS' defenses will be described. . How defenses against the threats in the model can be audited and benchmarked will be discussed.

---

[1] David S. H. Rosenthal, Thomas S. Robertson, Tom Lipkis, Vicky Reich, Seth Morabito, "Requirements for Digital Preservation Systems: A Bottom-Up Approach", D-Lib Magazine, Volume 11 Number 11 November 2005. http://www.dlib.org/dlib/november05/rosethal/11rosenthal.html