Audit Control Environment

Mike Smorul
ADAPT Group
University of Maryland, College Park

ACE Motivation

- Many archives use digests to monitor the integrity of their data.
- Most cannot assert their digests have not been tampered with.
- Should be lightweight
  - No Public/Private key infrastructure
- Must be able to be audited by any party
  - Auditor has no prior relationship with archive or depositor
  - Audit based only publically available information

ACE Concept

- Issue a small token that can be stored alongside an object to be preserved.
- The token secures the digest of the object.
- The token is cryptographically linked to an external witness value.
- Witness value is a single number/digest produced daily.
  - Easy to secure.
  - Small amount of data (several dozen KB/yr)

Components

- ACE Integrity Management Service
  - Issues tokens
  - Generates witness values
  - Provides token proof values
- ACE Audit Manager
  - Resides at archive, local auditor
  - Monitors files based on archive policy
  - Registers files, requests tokens, stores audit trails
  - Open Source / BSD license

All Components Auditable

- Local Audit
  - Provide a local audit of storage
  - ACE is local, but independent of the archive system
- IMS Audit
  - Prove that the keeper of round summaries isn’t acting malicious
- External Auditor
  - Prove to any outside party that any stored object is valid.
  - Financial, legal audit. Provide object along with proof

What can we prove?

- Witness to token validation shows
  - – Object is intact if its digest matches the token
  - – IMS and AM have not been compromised
- The file’s state can be linked to a 24 hour time window.
  - – Token links to witness which covers 1 day.

How can it be used?

- Tokens can be created for items still at producer
  - Witness links file creation to point in time
- Proof can be provided during data distribution
  - 3rd party trusted distributor
- Facilitate secure transfer of digests and objects

Chronopolis Deployment

- Three sites
  - UMD, SDSC, NCAR
  - Differing hardware (linux/sun/filesystem/SAM QFS)
- 20+Tb monitored, 5+ million files
- UMD complete audit in a little over a week
- Bottleneck was underlying storage system

Additional Information

- http://adapt.umiacs.umd.edu/ace
  - Papers, results, etc..
  - Audit Manager, release and source
- E-mail: msmorul@umiacs.umd.edu