

## Sleeping Disks

## Traces

- From last time:
  - MSR filesystem traces are available
  - Soon at <http://iota.snia.org/>
  - For now: DVDs with Greg Ganger
- Ping me if you want me to put them online

## Digital Preservation

- This is a bigger topic than just power (but power is important!)
- What threats?
- How long?
- How much data?

## Threats

- Large-scale disaster (flood, fire, famine, earthquake, war, hurricane, locusts)
- Human error (major cause in most systems)  
Accidental deletion; intentional but wrong deletion; turning off A/C; replacing wrong disk; yanking wrong plug; typing configuration
- Component faults (hw -- ALL hw), software (transient; heisenbugs; permanent - y2k); software licenses? domain name registration? IP addresses?

- Media Faults - bit flips, sector errors, media failures, device failures
- Obsolescent media (thriving business in reading old tapes...)
- Obsolescent format (thriving business in reading WordPerfect 1.0 docs... -- EBCDIC?) (proprietary, undocumented, ...)
- Loss of context - encryption keys, linked or embedded objects
- Malice (always malice) - and censorship
- Cash. Does it require ongoing cost or just sit quietly in a basement?

## Correlated failures

- Large-scale disaster (9/11 destroyed a datacenter whose only replica was also in NYC; staff couldn't get to the other version in time to keep it running)
- Correlated human error
- RAID correlated failures
- Going out of business

## Defining Faults

- Error *detection* - discovering that there is an error
- Error *containment* - limiting how far the effects of an error can propagate (see "module")
- Error *masking* - assuring correct operation despite the error (redundancy, etc) -- error *correction* is one form
- *Fault* - an underlying defect that has the potential to cause problems  
Latent fault - a fault that has not yet manifested in a failure
- *Failure* - not producing the intended result at the interface of a module

defs. loosely from Kaashoek & Saltzer

## Measuring Reliability

- TTF: Time to Failure
- TTR: Time to Repair
- Availability: time system running / time it should have been running
- MTTF = mean time to failure  
MTTR = mean time to repair  
MTBF = mean time *between* failure = MTTF + MTTR
- Availability:  $MTTF / MTBF = (MTBF - MTTR) / MTBF$
- Can improve availability by reducing MTTF or MTTR

## Some #s

- Shang dynasty (1200BC): Carved bone.  
Still going strong today.
- Paper: >> 100 years acid-free, no handling
- Mag tape & optics: 10-20 years +
- Magnetic disk: ? *device* failures are a few %  
per year, but media may be recoverable  
much longer; depends on app