Fault-tolerance

6.033 Lecture 15
Frans Kaashoek
With slides from Sam Madden
Where are we in 6.033?

- **Strong form of modularity: client/server**
  - Compose using names (e.g., DNS)
  - Limit propagation of errors

- **Implementations of client/server:**
  - In a single computer using virtualization
  - In a network using protocols
How to respond to failures?

- Return error to user
- Can we do better?
  - Keep computing despite failures?
  - Defend against malicious failures (attacks)?
- Rest of semester: handle these “failures”
  - Fault-tolerant computing
  - Computer security
Fault-tolerant computing

- General introduction: today
  - Replication/Redundancy
- The hard case: transactions
  - updating permanent data in the presence of concurrent actions and failures
- Replication revisited: consistency
Windows

A fatal exception OE has occurred at 0028:C00068F8 in PPT.EXE<01> + 000059F8. The current application will be terminated.

* Press any key to terminate the application.
* Press CTRL+ALT+DEL to restart your computer. You will lose any unsaved information in all applications.

Press any key to continue
Availability in practice

- Carrier airlines (2002 FAA fact book)
  - 41 accidents, 6.7M departures
    ✓ 99.9993% availability

- 911 Phone service (1993 NRIC report)
  - 29 minutes per line per year
    ✓ 99.994%

- Standard phone service (various sources)
  - 53+ minutes per line per year
    ✓ 99.99+% 

- End-to-end Internet Availability
  ✓ 95% - 99.6%
Data Sheet

Barracuda® 7200.10
Experience the industry's proven flagship perpendicular 3.5-inch hard drive

60 GB to 750 GB • SATA 1.5Gb/s or 3Gb/s and PATA 100

Key Advantages
• First 3.5-inch drive to utilize capacity- and reliability-boosting perpendicular recording technology
• First drive to reach 760 GB—a full year ahead of competition—enabling new solutions for data-intensive applications.
• Industry’s most proven and established desktop hard drive available today—more than 16 million shipped to date
• “One-stop shopping” with a broad range of capacity, cache and interface options for all your computing needs
• Best-in-class environmental specifications and reliability features
• Adaptive Fly Height offers consistent read/write performance from the beginning to the end of your computing workload.
• Clean Sweep automatically calibrates your drive.
• Directed Offline Scan runs diagnostics when storage access is not needed.
• RoHS-compliant design assures an environmentally conscious product.
• Enhanced G-Force Protection™ defends against handling damage.
• Seagate® SoftSonic™ motor enables whisper-quiet operation.

Best-Fit Applications
Desktop and High-Performance PCs
• Gamer PCs
• Workstations
• High-end PCs
• Desktop RAID
• Mainstream PCs
• Point-of-sale devices/ATMs
• USB/FireWire/eSATA personal external storage

*8 million Barracuda 7200.10 drives/shipped as of 4/18/07

<table>
<thead>
<tr>
<th>Contact Start-Stops</th>
<th>50,000</th>
</tr>
</thead>
<tbody>
<tr>
<td>Nonrecoverable Read Errors per Bits Read</td>
<td>1 per $10^{14}$</td>
</tr>
<tr>
<td>Mean Time Between Failures (MTBF, hours)</td>
<td>700,000</td>
</tr>
<tr>
<td>Annualized Failure Rate (AFR)</td>
<td>0.34%</td>
</tr>
</tbody>
</table>
### Reliability/Data Integrity

<p>| | |</p>
<table>
<thead>
<tr>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Mean Time Between Failures (MTBF, hours)</td>
<td>1.2 million</td>
</tr>
<tr>
<td>Reliability Rating at Full 24x7 Operation (AFR)</td>
<td>0.73%</td>
</tr>
<tr>
<td>Nonrecoverable Read Errors per Bits Read</td>
<td>1 sector per 10E15</td>
</tr>
<tr>
<td>Error Control/Correction (ECC)</td>
<td>10 bit</td>
</tr>
<tr>
<td>Interface Ports</td>
<td></td>
</tr>
<tr>
<td>SATA</td>
<td>Single</td>
</tr>
<tr>
<td>SAS</td>
<td>Dual</td>
</tr>
</tbody>
</table>

1 TB, 750 GB, 500 GB and 250 GB • 7200 RPM • SATA 3Gb/s, SATA 1.5Gb/s and SAS 3Gb/s
Disk failure conditional probability distribution

- Infant mortality
- Burn out
- Stable failure period
- Expected operating lifetime

1 / (reported MTTF)
Human Mortality Rates (US, 1999)

Disk Age vs. \( \Pr(\geq 1 \text{ Reported Read Failure}) \)

Pr(Reported Read Failure)

Disk Age (Months)

Bairavasundaram et al., SIGMETRICS 2007
Relative frequency of hardware replacement

<table>
<thead>
<tr>
<th>COM1 Component</th>
<th>%</th>
</tr>
</thead>
<tbody>
<tr>
<td>Power supply</td>
<td>34.8</td>
</tr>
<tr>
<td>Memory</td>
<td>20.1</td>
</tr>
<tr>
<td><strong>Hard drive</strong></td>
<td>18.1</td>
</tr>
<tr>
<td>Case</td>
<td>11.4</td>
</tr>
<tr>
<td>Fan</td>
<td>8.0</td>
</tr>
<tr>
<td>CPU</td>
<td>2.0</td>
</tr>
<tr>
<td>SCSI Board</td>
<td>0.6</td>
</tr>
<tr>
<td>NIC Card</td>
<td>1.2</td>
</tr>
<tr>
<td>LV Power Board</td>
<td>0.6</td>
</tr>
<tr>
<td>CPU heatsink</td>
<td>0.6</td>
</tr>
</tbody>
</table>

10,000 machines

\( \text{Pr(failure in 1 year)} \sim 0.3 \)
Fail-fast disk

```c
failfast_get (data, sn) {
    get (s, sn);
    if (checksum(s.data) = s.cksum) {
        data ← s.data;
        return OK;
    } else {
        return BAD;
    }
}
```
careful_get (data, sn) {
    r ← 0;
    while (r < 10) {
        r ← failfast_get (data, sn);
        if (r = OK) return OK;
        r++;
    }
    return BAD;
}
Replicated Disks

write (sector, data):
    write(disk1, sector, data)
    write(disk2, sector, data)

read (sector, data):
    data = careful_get(disk1, sector)
    if error
        data = careful_get(disk2, sector)
        if error
            return error
    return data
## Technical specifications

<table>
<thead>
<tr>
<th>Feature</th>
<th>Specification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Processors</td>
<td>2–16 per node&lt;br&gt;Intel Itanium processor 9100 series processors, 1.6 GHz single core processors</td>
</tr>
<tr>
<td>Cache</td>
<td>12 MB L3</td>
</tr>
<tr>
<td>RAM standard/maximum</td>
<td>Minimum: 4 GB&lt;br&gt;Maximum: 16 GB (32 GB&lt;sup&gt;2&lt;/sup&gt;)</td>
</tr>
<tr>
<td>RAM type/speed</td>
<td>PC2100 ECC registered DDR266A/B</td>
</tr>
<tr>
<td>ServerNet I/O</td>
<td>Minimum: 10&lt;br&gt;Maximum: 60</td>
</tr>
<tr>
<td>I/O adapters supported</td>
<td>Fibre Channel, Gigabit Ethernet</td>
</tr>
<tr>
<td>Fibre Channel disk modules</td>
<td>14 disks per module</td>
</tr>
<tr>
<td>Disk drives supported</td>
<td>146 GB and 300 GB 15K RPM Fibre Channel internal hard disk drive&lt;br&gt;HP Disk Array family (e.g., XP24000, XP20000, XP12000, and XP10000 disk arrays)</td>
</tr>
<tr>
<td>Standard features</td>
<td>N + 1 power supplies&lt;br&gt;N + 1 fans</td>
</tr>
</tbody>
</table>

<sup>2</sup> Although 32 GB possible, the Integrity NonStop NS16200 Server support availability is up to 16 GB.
How about an error in software?

• Big problem!
• Software for fault tolerant systems must be written with great care
  • Stringent development practices
  • Well-defined stable specification
  • Modeling, simulation, verification, etc.
  • N-version programming is tricky
• Will also be a problem for secure software
• Good design: small fraction is critical