

Fast and secure distributed read-only file system:

Presented by Kevin Fu (fubob@mit.edu)

MIT Lab for Computer Science

<http://www.fs.net/>

Prof. David Mazières (NYU) and Prof. Frans Kaashoek(MIT)

Goal

Integrity protection of public, read-only data

Motivation I

- **Content on the Internet has no guarantee of authenticity**



Paul Folino
Emulex CEO

Hoax briefly shaves \$2.5 billion off Emulex's market cap

By [Corey Grice](#) and [Scott Ard](#)
Staff Writers, CNET News.com
August 25, 2000, 3:45 p.m. PT

update A fake press release rocked the shares of networking equipment company Emulex today, causing the company's market value to briefly plunge by \$2.5 billion and creating anxiety for thousands of investors.

Around the same time trading began for the day, at 6:30 a.m. PT, a press release purportedly from Emulex was posted on Internet Wire, a Web-based distributor of corporate announcements that charges \$275 for the service.

According to the release, which contained formats similar to previous Emulex announcements and listed an actual investor relations executive as a contact, the company's chief executive was resigning and recent quarterly earnings were being revised from a profit to a loss.

Today's Hot Topics

- [Web auctions](#)
- [Apple Computer](#)
- [Napster](#)
- [Storage](#)
- [Microsoft](#)
- [Wireless](#)

Search

Latest Headlines

Host

A I S

Red Hat Linux**Updates**

A = alpha, I = intel, S = sparc

Canada

ftp.crc.ca	■ ■ ■	/pub/systems/linux/redhat/ftp.redhat.com	/pub/systems/linux/redhat/ftp.redhat.com/updates
ftp.muug.mb.ca	■ ■ ■	/mirror/redhat/redhat	/mirror/redhat/redhat/updates
sunsite.ualberta.ca	■ ■ ■	/pub/Mirror/Linux/redhat/ftp.redhat.com	/pub/Mirror/Linux/redhat/ftp.redhat.com/redhat/updates
redhat.eyetap.org	■ ■ ■	/	/updates
redhat.pjs.scitech.on.ca	■	/pub/redhat/current	/pub/redhat/updates

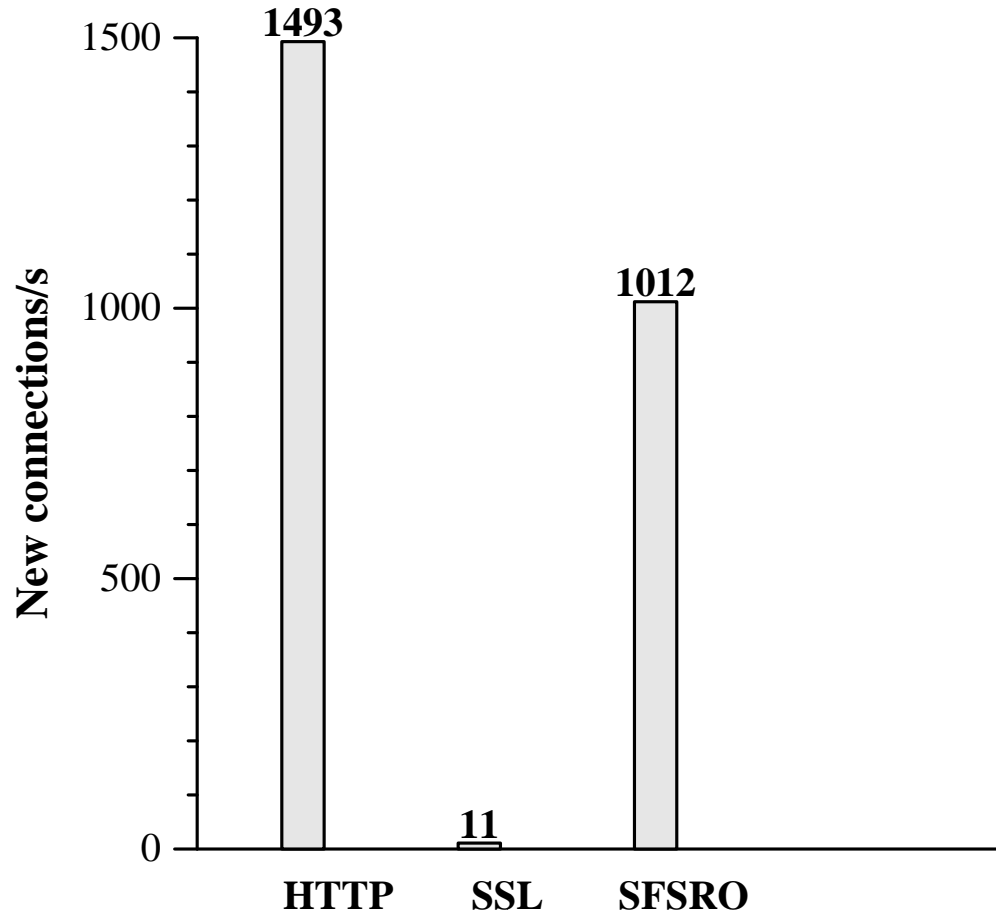
.com

austin.jhcloos.com	■	/pub/mirror/redhat/	/pub/redhat/updates
emperor.alpha-processor.com	■ ■	/pub/redhat	/pub/redhat/updates
mrhankey.bizserve.com	■ ■ ■	/pub/linux/redhat/ftp.redhat.com	/pub/linux/redhat/ftp.redhat.com/redhat/updates
ftp.freesoftware.com	■ ■ ■	/pub/linux/redhat	/pub/linux/redhat/updates
ftp.codemeta.com	■ ■ ■	/pub/mirrors/redhat/distributions	/pub/mirrors/redhat/updates
ftp.cybertrails.com	■ ■ ■	/pub/redhat	/pub/redhat/updates
opnsrc.support.compaq.com	■ ■ ■		/linux/redhat/updates.redhat.com

Motivation II: Untrusted replicas

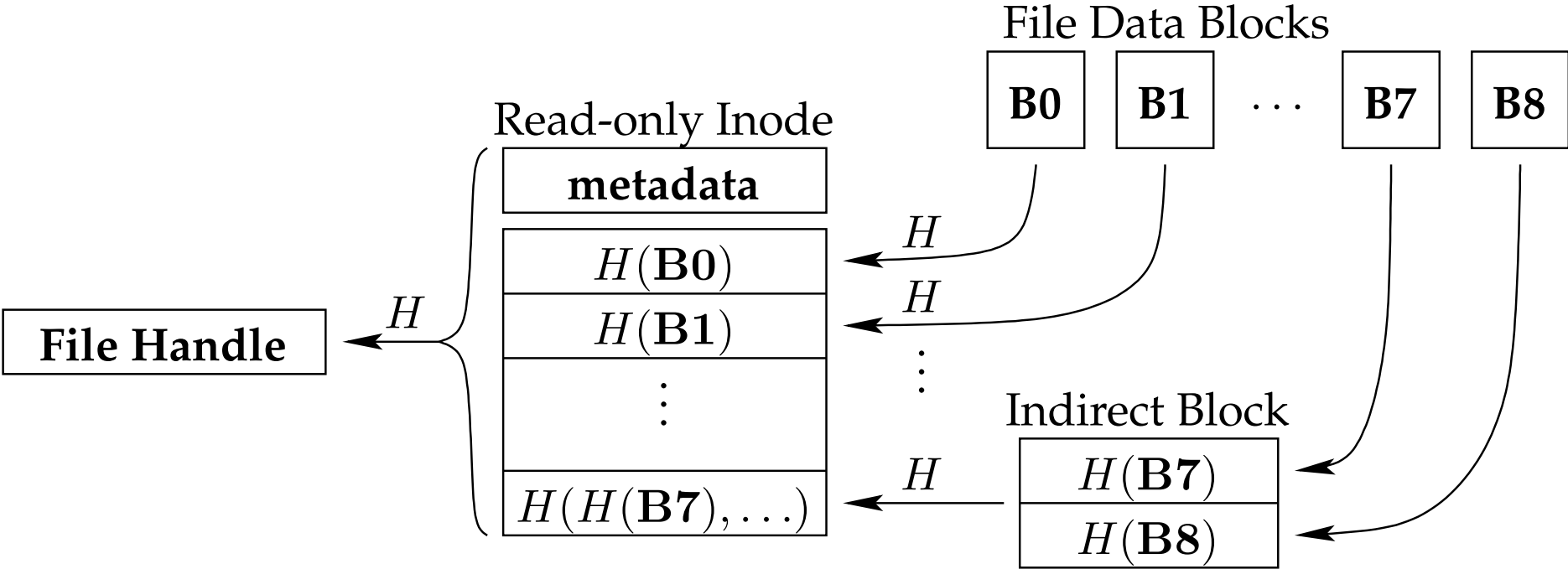
- No security publishing system supports untrusted replicas
- Avoid situation where compromise to ANY replica compromises the WHOLE system (e.g., SSL)

Motivation III: No system is fast enough



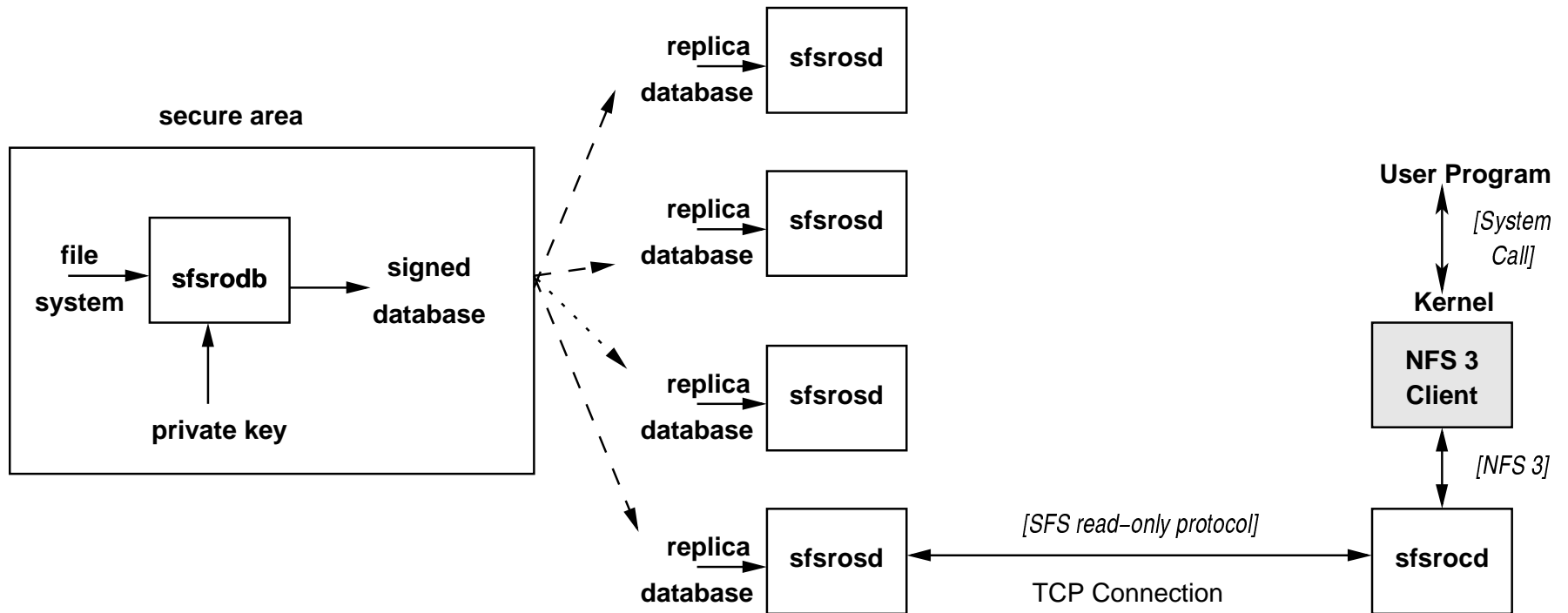
For comparison, the root DNS servers handle about 4000 connections/sec.

Tree of cryptographic hashes



All file system structures are named by cryptographic hashes rather than traditional index numbers.

Architectural Overview



Applications

- **Software distribution (e.g., Redhat mirrors)**
- **Certificate Authorities (e.g., Verisign)**

Conclusions

- **Integrity protection of public, read-only data**
- **Replication on untrusted servers**
- **Scales well to the number of clients**