Security of Online Information

Barbara Liskov
MIT CSAIL
March 2009
The Vision

- All information of interest will be
  - Stored online
  - Accessible from anywhere
  - Persistent
  - Sharable
  - Easy to locate/query/use
Examples

- All your files
- Medical records
- Corporate data
- Scientific data
Scenario 1

- All my data from any device
  - Laptop, pc, telephone, kiosk, …

- Saved automatically
- Uploaded as needed
- Automatic archive/backup
- Controlled sharing
Scenario 2

- Medical records
  - From many hospitals
  - Available everywhere
  - Access control and privacy
Storage System Requirements

- Scalability
- Performance
- Security, Security, Security
Security

- Confidentiality
- Integrity
Security

- Confidentiality
- Integrity
- Reliability (information isn’t lost)
- Availability (information available 24/7)

- Reliability and availability require replication
Single Server

Server

Clients
Single Server

Server

Clients
Replicated Servers
Replication Protocols

- Goal: information is preserved and accessible in spite of failures
  - Network failures
  - Machine failures
- Benign failures
- Byzantine failures
Replication

Servers

Clients
Replication

Servers

Clients

State:

A  ●  ●  ●

State:

●  ●  ●  ●

State:

A  ●  ●  ●
Replication

Servers

Clients

State:

A

State:

......

State:

A

......
Replication

Servers

State: A

State: 

State: A

Clients

write B

write B

write B
Replication

State:

A B ···

State:

B ···

State:

A ···

Servers

Clients

write B

write B

write B
Ordering Solution

- Use a primary
  - It orders the operations
  - Other replicas obey this order
Ordering Solution

- Use a primary
  - It orders the operations
  - Other replicas obey this order

- BUT: the primary might fail
  - Replicas watch the primary and elect a new one if it fails
Issues

- Insuring correct behavior
  - Dealing with all possibilities
- Handling node recovery
- Providing competitive performance
Timeline

- 1987-1992: protocols developed
- > 2000: use in industry
- 1996 approximately: more challenging failure models
Byzantine Failures

- Machines fail arbitrarily
  - They lie
  - They collude

- Causes
  - Malicious attacks
  - Software errors
Byzantine Behavior

Servers

Clients
Byzantine Behavior

**Servers**

<table>
<thead>
<tr>
<th>State:</th>
<th>A</th>
<th>B</th>
<th>...</th>
</tr>
</thead>
</table>

**Clients**

- Write B
- Write B
- Write B
- Write B
Strategy

- The same!

- Key difference: replicas might lie
  - More replicas
  - More messages
Where next?

- 1996-2002: BFT
- Replication
  - Better protocols
  - Scaling up
- Other security issues
  - Integrity
  - Confidentiality