Trusted Storage

Anjo Vahldiek, Eslam Elnikety, Ansley Post, Peter Druschel,
Deepak Garg, Johannes Gehrke, Rodrigo Rodrigues

MAX-PLANCK-GESELLSCHAFT

Max Planck Institute for Software Systems

1. Problem

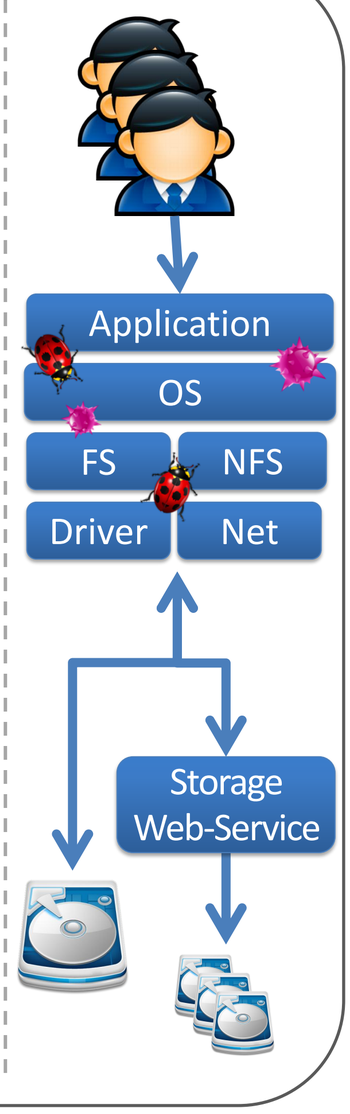
Complex storage systems threaten data integrity & confidentiality.

- **Bugs**, security **vulnerabilities**, operator errors, sabotage
- Lack of **transparency/accountability** in third-party storage

Problem:

Lack of **storage level control**

- Who can read what & when?
- Who can modify what & when?
- Where is data stored?
- How many replicas?
- What is the access history?



2. Trusted Storage

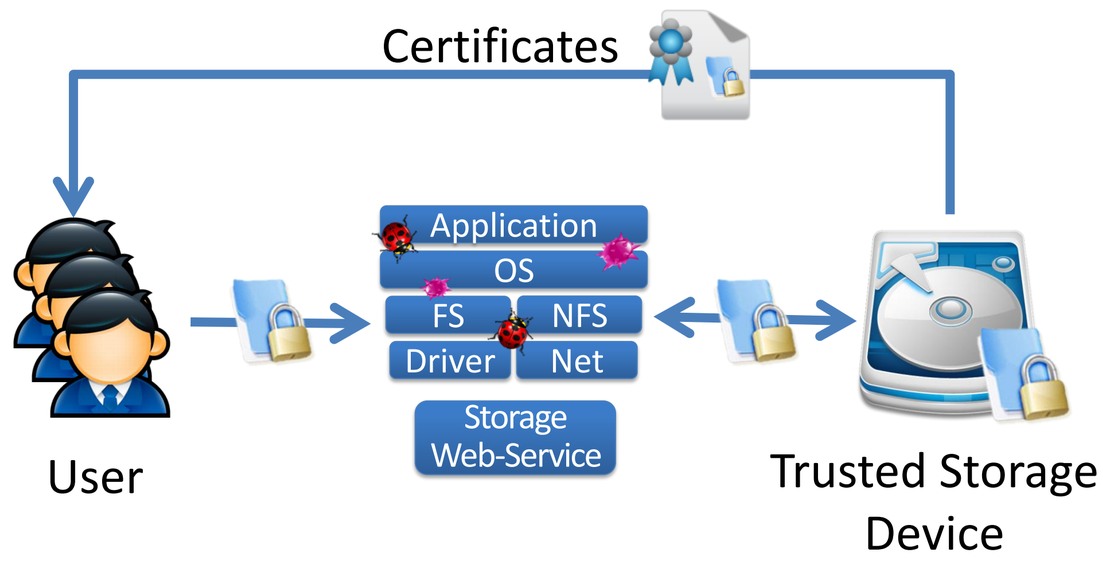
Enforces a policy per named application object (e.g. file) and certifies its state.

Key Idea:

- User provides a **policy** for every application object
- Storage device **enforces** compliance with policy
- Storage device **certifies**
  - its properties (location, type, reliability, etc.)
  - current policies associated with stored objects
  - index and access history of stored objects

Benefits:

- Resilient against viruses, bugs, FS corruption
- Policies give users control over provider data use
- Certificates make provider accountable
- Minimizes trusted computing base



3. Example Policies

User-provided specification of access restrictions.

Identity: Requires proof of identity

Attestation: Requires proof of hw/sw configuration

Quota: Limit number of read accesses

Location Aware: Allow writes at specified locations

Storage Lease: Allow writes after given date

Time Capsule: Allow reads after given date

Expiration: Allow reads prior to given date

4. Certificates

Signed by trusted storage device.

Certificates testify

- **Properties for application objects**: Full path name, size & hash of data, physical layout, policy, access history
- **Device properties**:
  - Type, firmware, service life
  - Speed, capacity, # of disks/heads
  - Location, time, reliability

5. Trusted Storage Device

A device (e.g., single disk or enclosure) that provides trusted primitives.

- **Trusted firmware** with secure updates (manufacturer-certified)
- **Cryptographic support** (credentials, encryption, …)
- **Secure channel** between two trusted storage devices
- **Trusted network servers** for time & location

6. Properties & Guarantees

Data confidentiality, integrity & accountability guarantees only depend on firmware integrity.

- Trusted storage implementation within firmware
- Assumes no physical attacks

7. Status

Implementation in progress, promising simulation results:

- Additional flash memory (0.05 % of device capacity)
- < 3% latency increase