

# New Approaches for Recovery

Peng Liu (PSU), Sushil Jajodia (GMU), and Meng Yu (WIU)

CNS-0716479, CNS-0716323, and CNS-0757210



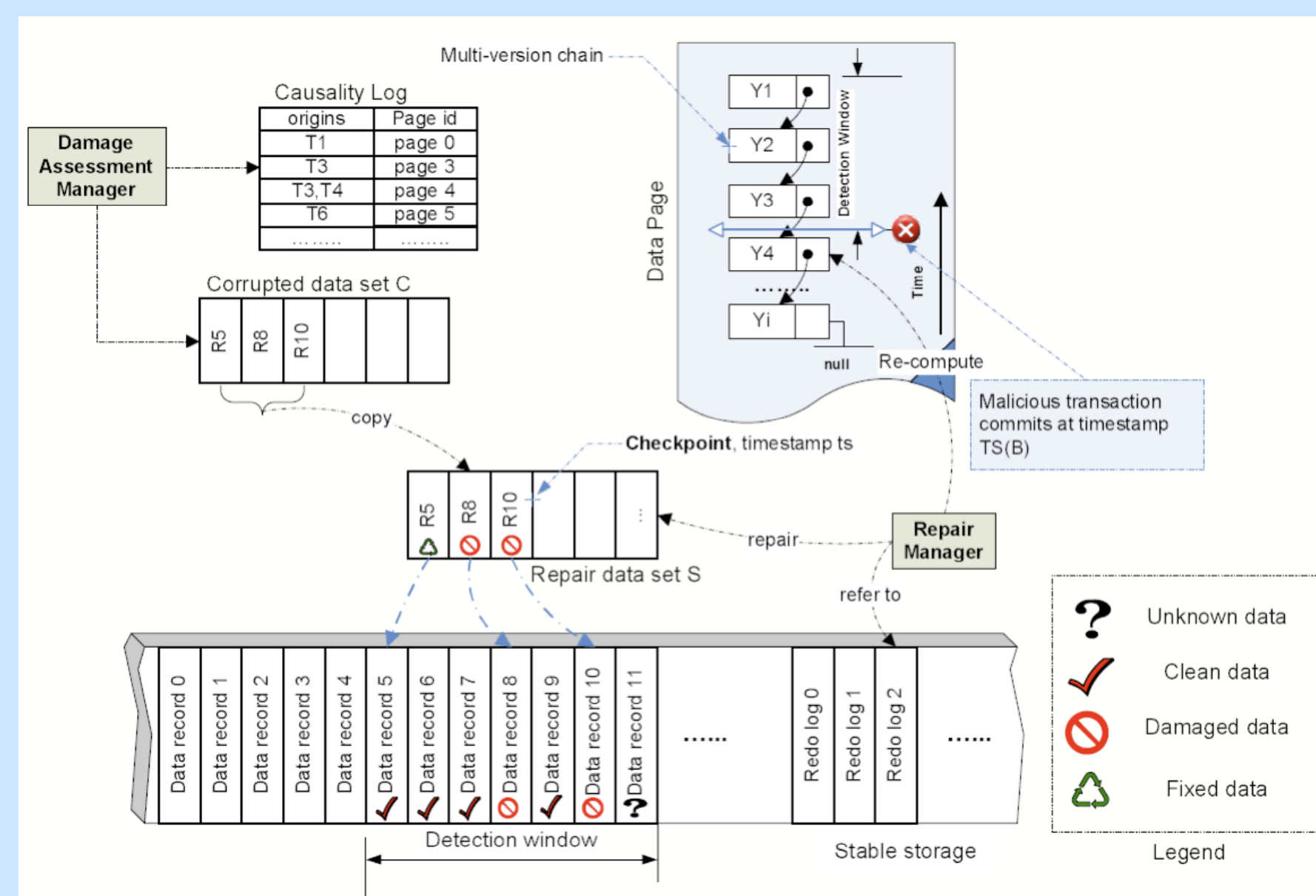
## Collaborative Research - Transparent Damage Quarantine and Recovery

Develop new approaches for damage management (assessment, quarantine, repair, etc.) in critical applications to survive ongoing attacks.

### Applications

Providing 24/7 services is critical for e-business, e-governments, and other similar applications. Attacks to such applications may cause cascading effects of damage at the transaction level.

This research studies new approaches to quarantine and repair such damage without interrupting services.



The processing structure for damage tracking/quarantine/repair

### Approach and Impact

#### New approach

- Tag-based dynamic damage tracking
- Multi-version based recovery
- Shadow database based isolation

#### Research Impact

- Instant damage assessment
- Conflict-free fast recovery
- Defensive protection against attacks

### Problem

Data processing services are provided through highly connected web and database servers. Attacks to a single server may cause cascading effects (domino effects) of data corruption through dependencies and network connections. Manually tracking damage spread and repairing data corruption become infeasible.

Existing techniques highly depend on log analysis *before* or *after* attacks so they are not suitable for critical applications providing 24/7 services that require online attack recovery.

### Solutions

- Dynamically generated causality relations to replace log analysis
- Multi-version switch to avoid concurrency conflicts caused by recovery
- Shadow-database isolation to sandbox malicious transactions

### Results

- Significantly improved performance of damage assessment and repair
- New isolation of pending transactions from trusted transactions
- A prototype built into PostgreSQL