Weakly Consistent but Eventually Convergent: Access Control in the Matrix Messaging System

Florian Jacob, Hannes Hartenstein
Lightning Talk @ SACMAT 2023
Centralized Applications and Access Control

A single logical entity…
- …executes the application
- …defines a total order on incoming access requests
- …knows all current policies & permission assignments
- …decides and enforces policies

Centralization is a standard assumption
- Example: Scot Stoller’s keynote “WebSheets: A Framework for Privacy-Centric Web Applications by Non-Programmers”
Problem: Distributing Apps and Access Control

- One wants to make an application distributed to get...
  - Scalability
  - Low Latency
  - Availability
  - Fault Tolerance
- …while keeping Strong Consistency
  - “Behave as if still centralized!“

► Everyone wants Strong Consistency
► but no one wants to pay its price!

![Diagram of CAP Theorem]

Partition Tolerance
Availability
Strong Consistency

Problem:
Distributing Apps and Access Control

Weakly Consistent but Eventually Convergent: Access Control in the Matrix Messaging System
Does Matrix have a Solution?

Matrix is a relevant decentralized messaging middleware
- ≥100 000 000 accounts, ≥100 000 servers
- Universities, Mozilla Foundation, French and German Public Sector, …

Matrix provides access control in an unconventional environment
- weakly consistent, no consensus
- servers independently decide
- …but decisions still eventually converge.
Replicated Building Blocks: Sets and Maps

1st building block: partially-ordered sets of events
- Authorized accesses in partially-ordered time

2nd building block: derived key-value maps
- Policy information attributes

Extend partial to linear order:
- $x_3 \parallel x_4 \text{? } h(x_3) < h(x_4) \Rightarrow x_3 < x_4$
- $x_1 \parallel x_2 \text{? } h(x_1) < h(x_2) \Rightarrow x_1 < x_2$
Matrix’ Approach to Distributed Access Control

- Decentralized access control in partially-ordered time is challenging

- Matrix’ approach: compose weakly-consistent, replicated Sets and Maps to get a form of lattice-based access control
  - Never reject authorized concurrent updates
  - …but maybe collectively ignore them after linearization

- But: What does it mean to have “eventually convergent access control”?
Future Work

Access Control

Consistency

Achievable strength of access control in distributed, weakly-consistent systems?
- Supported invariants and semantics
- Expected quirks and anomalies