The Challenge

Traditional math specs are unreadable

The Challenge

Traditional math specs are unreadable

Access Control Rules

$$\forall\, u \in \text{Users},\ r \in \text{Resources},\ a \in \text{Actions}:$$

$$\text{allowed}(u, r, a) \iff (\text{role}(u) = \text{admin}) \lor (\text{role}(u) = \text{user} \land \text{type}(r) \in \{\text{public}, \text{shared}\} \land a = \text{read}) \lor$$

$$(\text{role}(u) = \text{user} \land \text{owner}(r) = u \land a \in \{\text{read}, \text{write}, \text{delete}\}) \lor (\text{role}(u) = \text{guest} \land \text{type}(r) = \text{public} \land a = \text{read})$$

Problems

- Few people can read this fluently
- Hard to verify completeness (did we cover all cases?)
- Hard to verify disjointness (do cases overlap?)
- Doesn't translate obviously to code or domain expert language

The Solution

Parnas Tables (Tabular Notation)

User Role	Resource Type	Action	Owner?	Result
Admin	* (any, DC)	*	*	✓ Allow
User	Public	Read	*	✓ Allow
User	Shared	Read	*	✓ Allow
User	*	Read	Yes	✓ Allow
User	*	Write	Yes	✓ Allow
User	*	Delete	Yes	✓ Allow
User	Public	Write	No	✗ Deny
User	Public	Delete	No	✗ Deny
User	Shared	Write	No	✗ Deny
User	Shared	Delete	No	✗ Deny
User	Private	*	No	✗ Deny
Guest	Public	Read	*	✓ Allow
Guest	Private	Read	*	✗ Deny
Guest	*	Write	*	✗ Deny
Guest	*	Delete	*	✗ Deny