Row-level MAC in H2

Chris Martin
chris.martin@gatech.edu

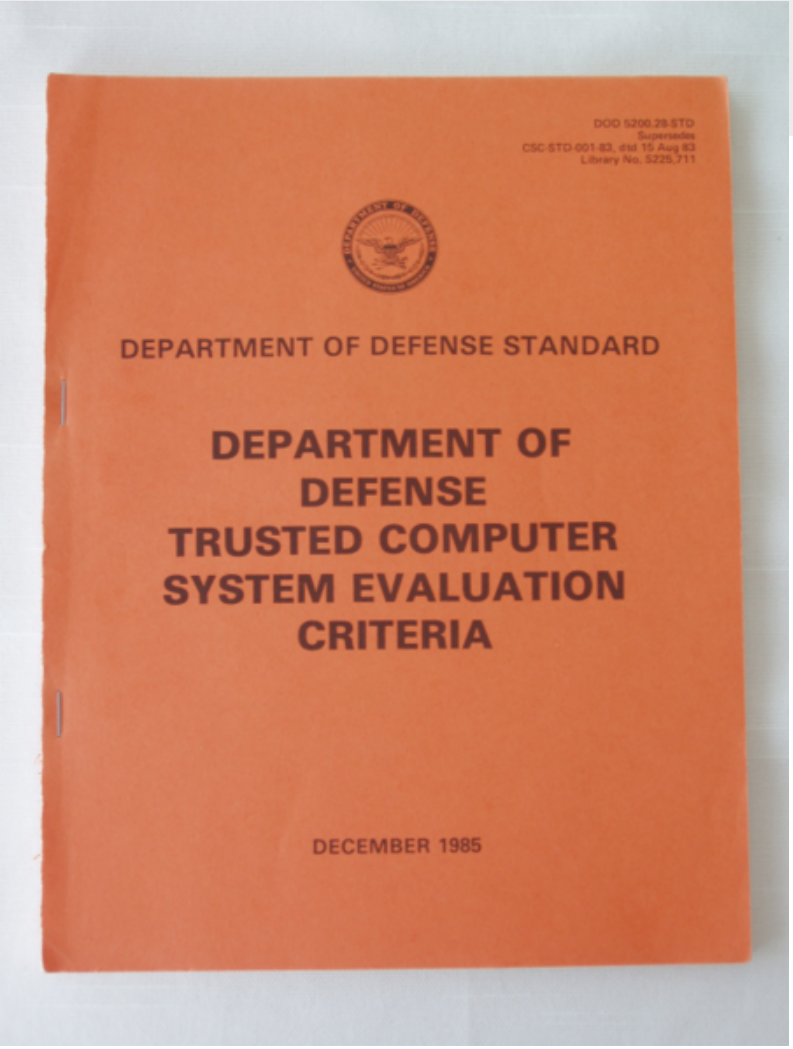
Mandatory/Discretionary

MAC

- Labeled objects
- Centralized policy

DAC

- ACLs
- Decentralized

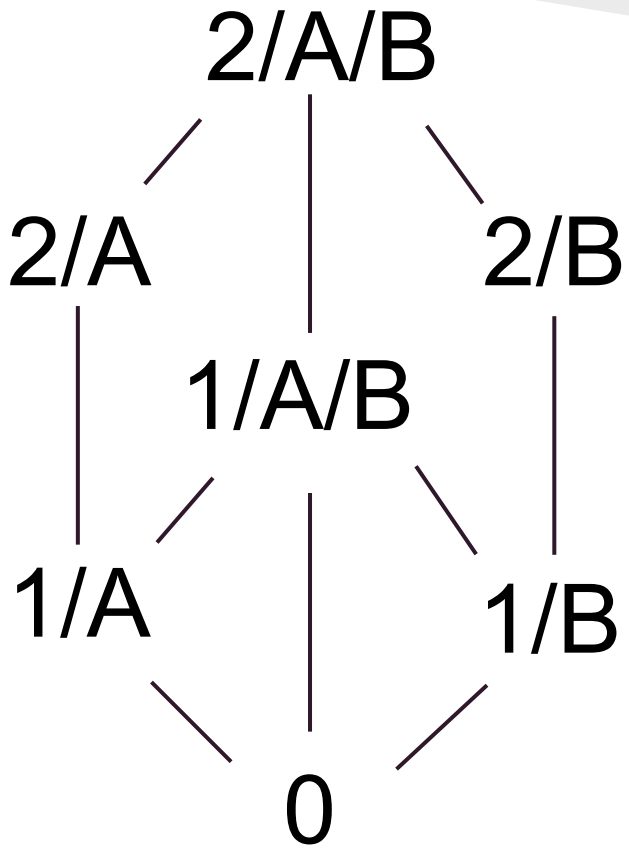


Multilevel Security (MLS)

Marking

- Sensitivity
- Compartments

S/C1/C2/C3/...



Row-level access control

Actual data:

Apple	1/A
Banana	3/A
Carrot	2/B

User with '2/A' sees:

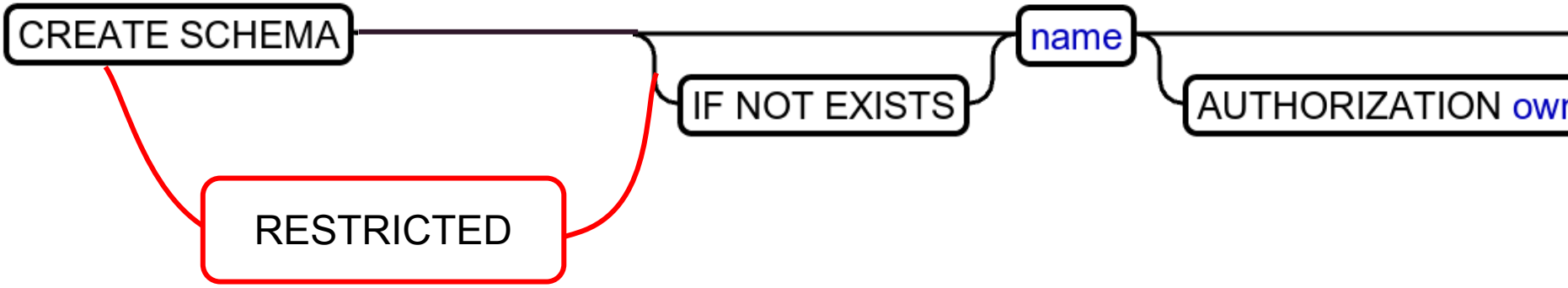
Apple	1/A

User with '2/B' sees:

Carrot	2/B

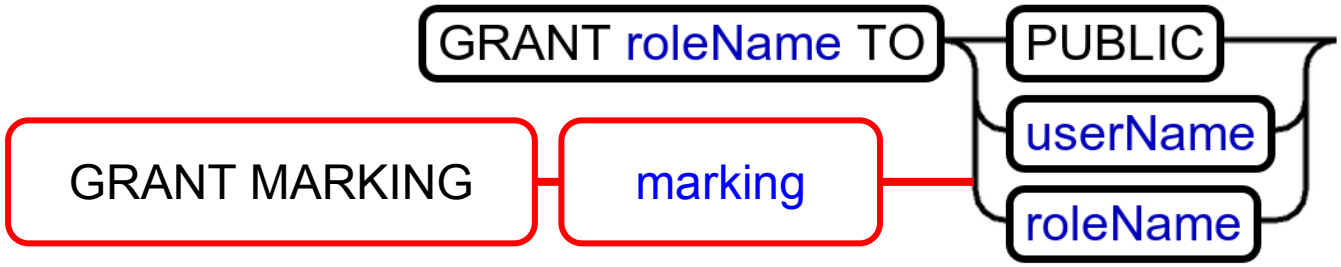
SQL grammar

```
CREATE SCHEMA things;

CREATE RESTRICTED SCHEMA things;
```



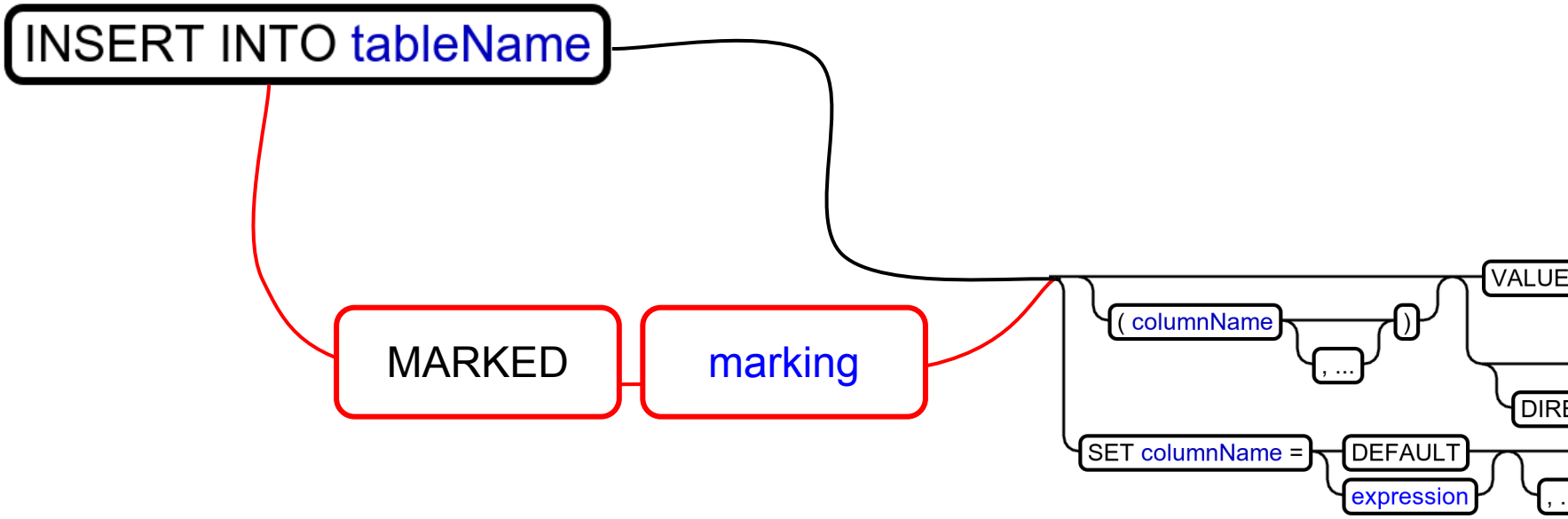
SQL grammar

```
GRANT administrators TO alice;

GRANT MARKING '3/B' TO alice;
```



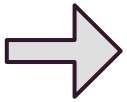
SQL grammar

```
INSERT INTO people ( name ) VALUES ( 'Bob' );

INSERT INTO people MARKED '2/B/C' ( name ) VALUES ( 'Bob' );
```



Shadow schema

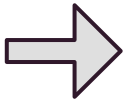
```
CREATE RESTRICTED SCHEMA
vault;
```



```
CREATE SCHEMA vault;

CREATE SCHEMA vault_shadow;
```

Shadow table

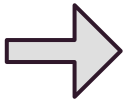
```
CREATE TABLE vault.doc (
  title VARCHAR(20)
);
```



```
CREATE TABLE vault_shadow.doc (
  title       VARCHAR(20),
  marking_id  BIGINT
);

CREATE VIEW vault.doc AS
SELECT
  title,
  RENDER_MARKING(marking_id)
FROM vault_shadow.doc
JOIN mac.session_marking;
```

Shadow table

```
INSERT INTO vault.doc
  MARKED '2/A'
  ( title ) VALUES ( 'hi' )
```



```
INSERT INTO vault_shadow.doc
  ( title, marking_id )
  VALUES ( 'hi', ... );
```

Future features

`REVOKE MARKING` …

Grant-marking role

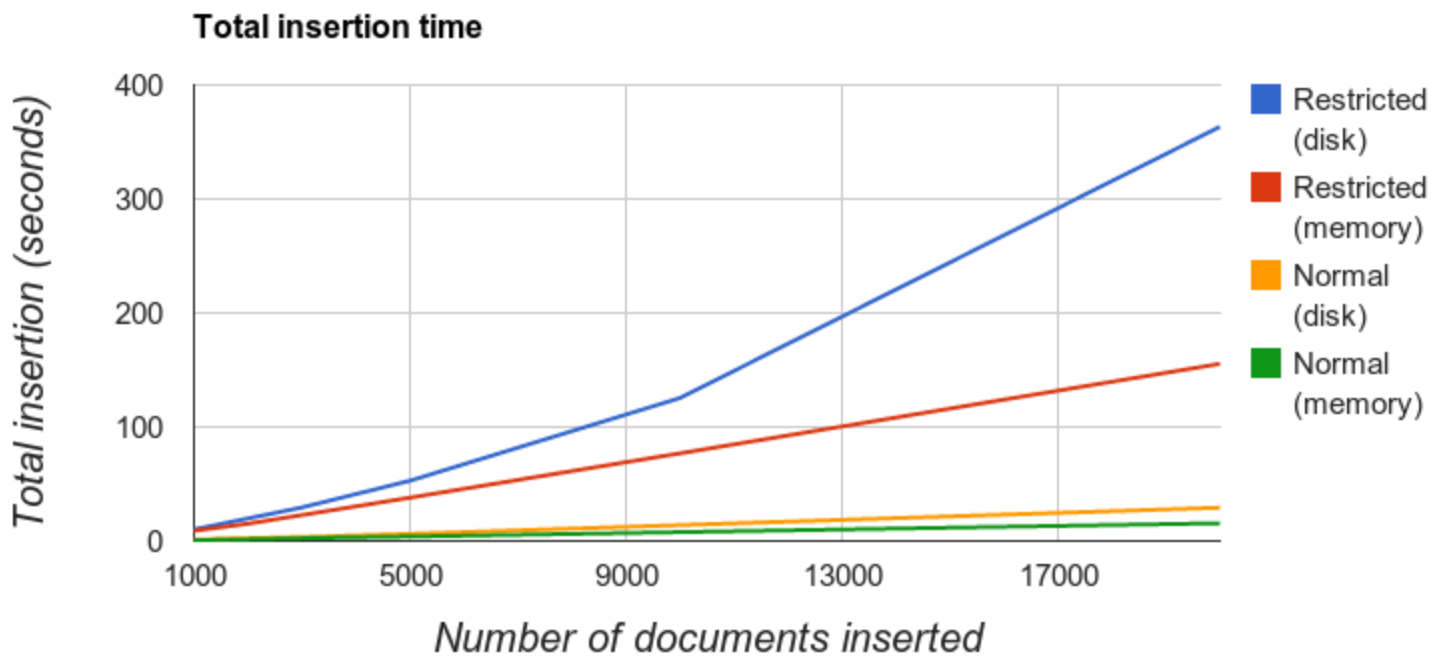
Permission-checking for marking grants

`UPDATE` and `DELETE` on shadow tables

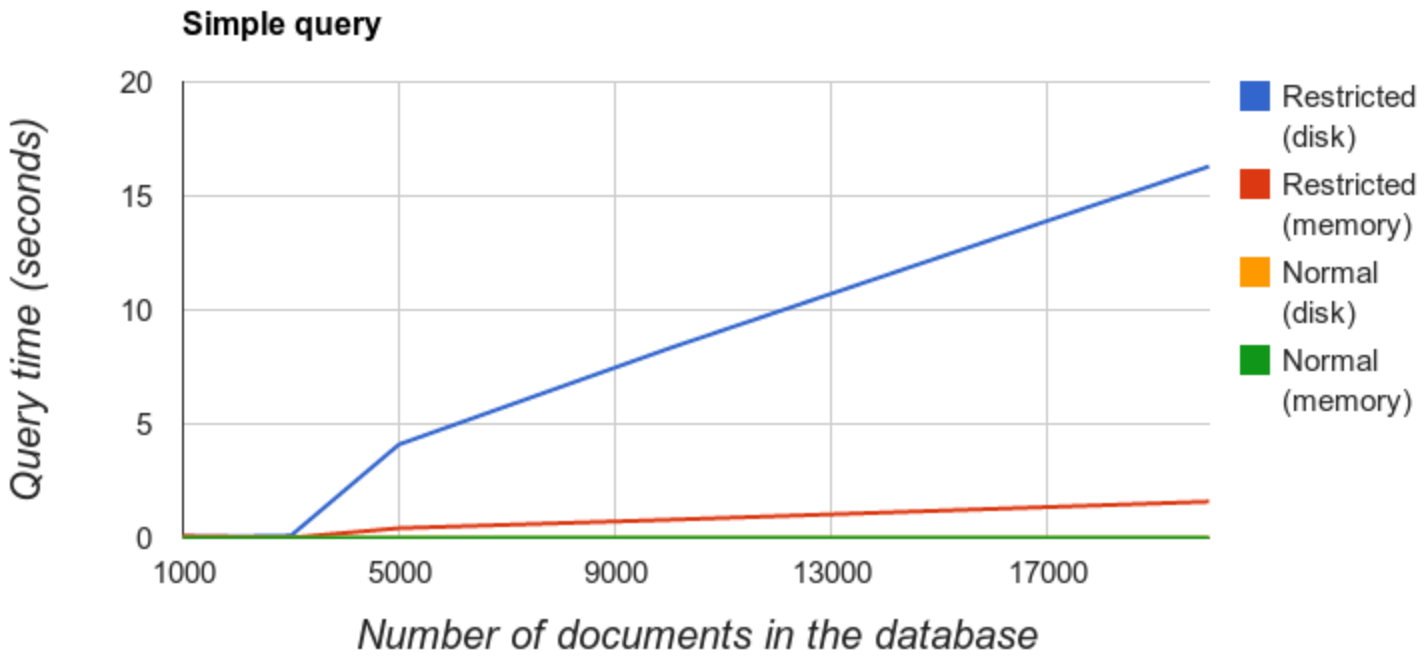
Test setup

```
Public.Person
  user_id       identity
  user_name     varchar
Vault.Document
  doc_id        identity
  title         varchar
  released      date
  author        int      FK: Person.user_id
Vault.Page
  doc_id        int      FK: Document.doc_id
  page_number   int
  page_text     clob
```

Insertion Performance



Query performance

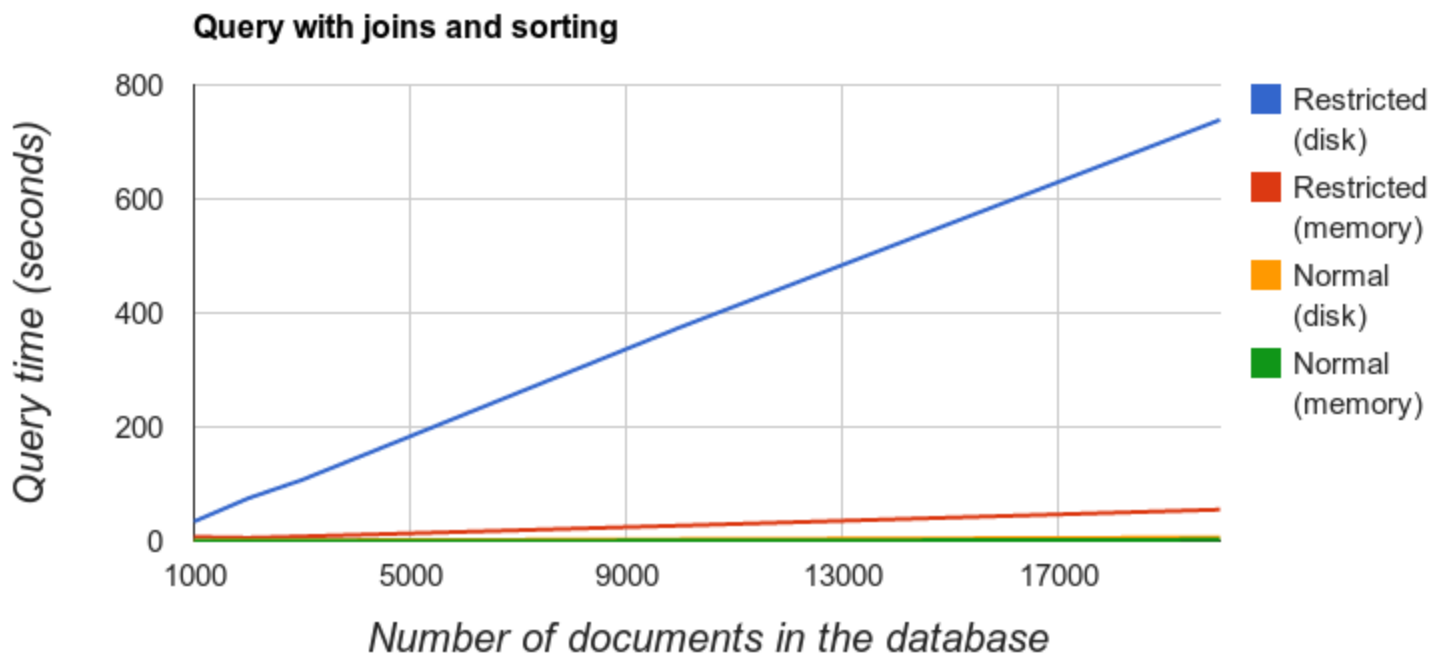



```
SELECT title FROM vault.document
WHERE released < PARSEDATETIME('1971 1 Jan', 'yyyy d MMM')
```

Query with joins and sorting

```
SELECT document.doc_id, document.title, document.released,
  document.author_id, author.person_name author_name,
  page.page_number page, page.page_text
FROM vault.document
LEFT JOIN vault.page
ON document.doc_id = page.doc_id
LEFT JOIN public.person author
ON document.author_id = author.person_id
ORDER BY released DESC, page DESC
LIMIT 1000
```

Query performance #2



Improving performance

The MAC schema:

mac.marking

marking_id	identity
sensitivity_id	bigint
compartment_id_list	clob

mac.sensitivity

sensitivity_id	identity
name	varchar(255)

mac.compartment

compartment_id	identity
name	varchar(255)

mac.marking_compartment

marking_id	bigint
compartment_id	bigint

mac.credential

credential_id	identity
sensitivity_id	bigint
compartment_id	bigint

mac.user_credential

user_name	varchar(255)
credential_id	bigint