BPD Side Channel

Swapnil
Mona

Possible Side Channel Attacks in our Systems

- Information Leakage Attack:
  - Officers 1001 and 1002 not only share the same rank but also are stationed in the same city and neighborhood.
- Time Leakage
  - Sequential Filtering: state and neighborhood -> using execution time to reveal the distribution of police or victims
  - **Inference Attack: title ⇒ The proportion of police officers who have the rank of 'patrol officer' (ptl) relative to the total number of Boston police**

employee_id	rank	city	neighborhood
1001	Sgt	Boston	Dorchester
1002	Sgt	Boston	Dorchester
1003	Det	Cambridge	East Cambridge
1004	Sgt	Boston	Roxbury

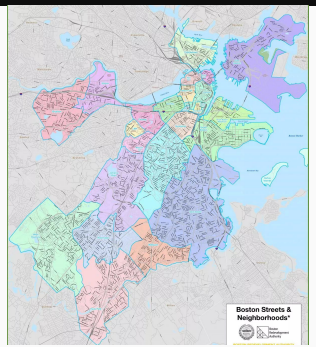

Figure 1. Boston Neighborhood Map

Queries Used for Timing Attack

Query | Query History

```
1  SELECT
2      first_name,
3      last_name,
4      COUNT(allegation)/2 AS allegation_count
5  FROM
6      AllegationCountOnOfficers.AllegationCountOnOfficers
7  WHERE
8      active = TRUE
9  GROUP BY
10     first_name,
11     last_name
12 ORDER BY allegation_count DESC
```

Figure 2. Adjusted Allegation Counts per Officer

Query | Query History

```
1  SELECT
2      first_name,
3      last_name,
4      COUNT(allegation)/2 AS allegation_count
5  FROM
6      AllegationCountOnOfficers.AllegationCountOnOfficers
7  WHERE
8      active = TRUE and ranking = 'ptl'
9  GROUP BY
10     first_name,
11     last_name
12 ORDER BY allegation_count DESC
```

Figure 3. Adjusted Allegation Counts per Officer with Condition Title = “ptl”

Runtime Results **without Prevention**

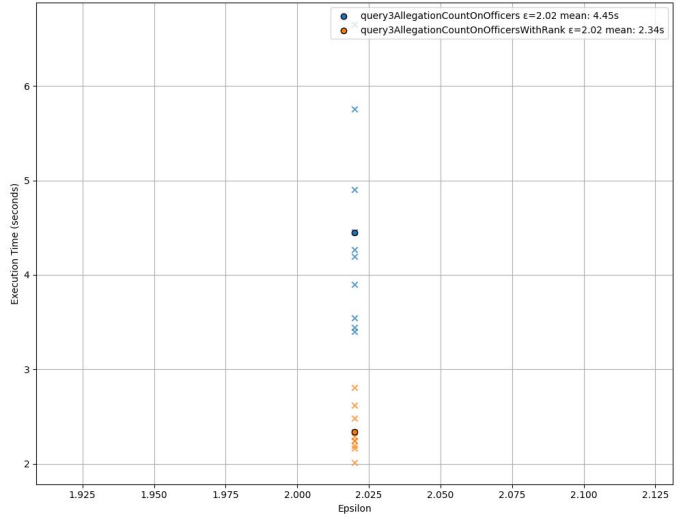

Figure 4. 10 executions: 2.34/4.45 seconds = **52.6%**

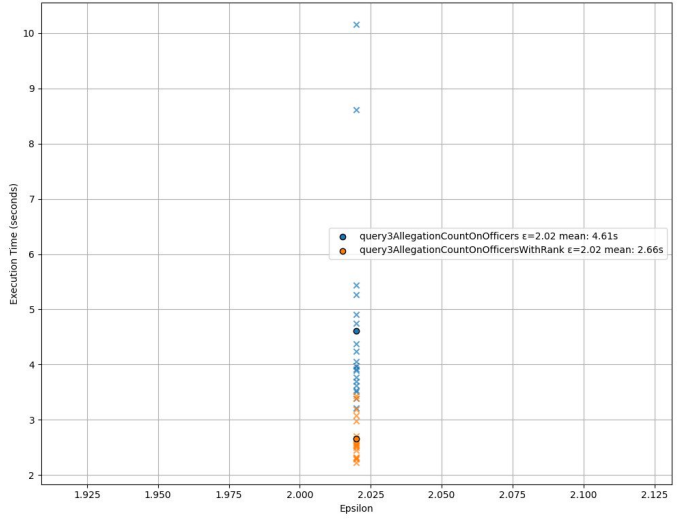

Figure 5. 20 executions: 2.66/4.61 seconds = **57.7%**

Actual percentages: 8672/15960 rows = **54.3%**

Preventing Timing Attack

- Random delays with variable range of seconds to each of the response times of the queries.
- For this query, we chose a range of 4% - 21% delays that corresponds to 0.1 to 0.5 seconds delay

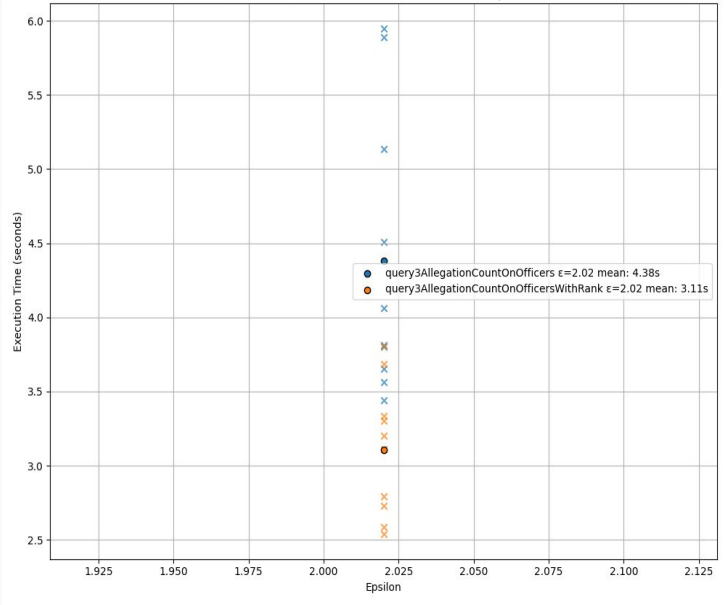

Figure 6. Random delays added to runtime for 2 slightly different queries

Affected Runtime (with/without delay)

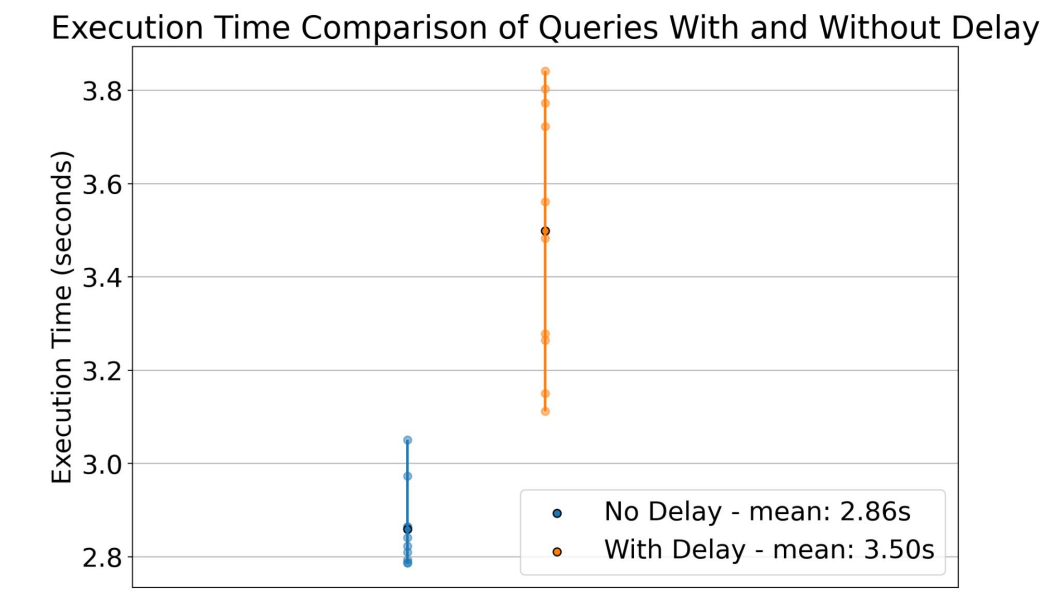

Figure 7. Random delays added to runtime for the same query

Thank you for listening!

Any question?