Semester: VI Subject: CSS

Academic Year: 2023-2024

## INFERENCE ATTACKS

* Databases introduce a number of unique security requirements for their users and administrators.
* On one hand, databases are designed to promote open and flexible access to data
* On the other hand, it is this same open access that makes databases vulnerable to many kinds of malicious activity.
* Inference occurs when users are able to piece together information at one security level to determine a fact that should be protected at a higher security level. It best explained through a practical example.
* Imagine that you are a database administrator for a military transportation system. You have a table named Cargo in your database that contains information on the various cargo holds available on each outbound airplane.
* Each row in the Table represents a single shipment and lists the contents of that shipment and the flight identification number.
* The flight identification number may be cross-referenced with other tables to determine the origin, destination, flight time and similar data.

Semester : VI Subject : CSS Academic Year: 2023-2024

The cargo table appears as follows

| Flight ID | Cargo Hold | Contents | Classification. |
|---|---|---|---|
| 1254 | A | Boots | Unclassified |
| 1254 | B | Guns | Unclassified |
| 1254 | C | Atomic Bomb | Top Secret. |
| 1254 | D | Butter | Unclassified. |

Suppose that General Jones (who has a Top-Secret security clearance) comes along and request information on the cargo carried by flight 1254.

The general would (correctly) see all four shipments. On the other hand, if Private Smith (who has no security clearance) requests the data, the private would see the following table:

Cargo Table as visible to no security clearance level.

| Flight ID | Cargo Hold | Contents | Classification. |
|---|---|---|---|
| 1254 | A | Boots | Unclassified |
| 1254 | B | Guns | Unclassified |
| 1254 | D | Butter | Unclassified. |

This correctly implements the security rules that prohibit someone from seeing data classified above their security level. However, assume that there is a unique constraint on flight ID and cargo hold (to prevent scheduling two shipments for the same hold).

Semester: VI Subject: CSS Academic Year: 2023-2024

When Private Jones sees that nothing is scheduled for hold C on flight 1254, he might attempt to insert a new record to transport some vegetables on that flight.

→ However, when he attempts to insert the record, his insert will fail due to the unique constraint. At this time, private Jones has all the data he needs to infer that there is a secret shipment on flight 1254.

→ He could then cross-reference the flight information table to find out the source and destination of the secret shipment and various other informations.

## MULTILEVEL DATABASE SECURITY:

The term multilevel arises from the defense community's security classification: Unclassified, Confidential, Secret and TopSecret.

Individuals must be granted appropriate clearances before they can see classified information. Those with Confidential clearance are only authorized to view confidential documents, they are not trusted to look at Secret or Top Secret information. The rules that apply to data flow operate from lower levels to higher levels, and never the reverse. This is illustrated below: