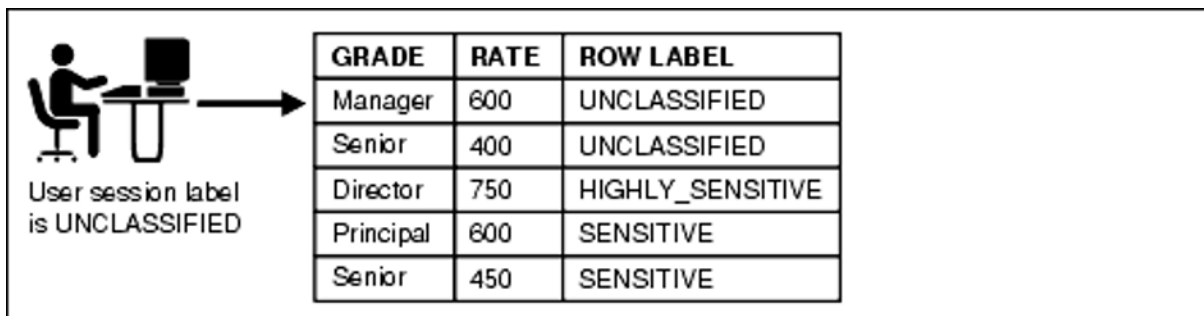


Forum Response

Nice post and an interesting topic one I feel often gets overlooked when talking about security with the external risks being the ones that generally get the attention without looking at internal risks. As someone who has been poking around in databases professionally for at least the last decade I can say that if you have access to the backend database you more than often have the keys to the kingdom and in a lot of cases you can bypass application-level security and auditing by directly editing the data in the DBMS.

One way that security can be implemented to prevent this type of attack and I'm speaking with my oracle hat on having implemented it in a commercial environment is the use of Oracle label Security (OLS) within the database as this allows sensitive data to be restricted within a database at the row level while still allowing access to the non-sensitive data Oracles Description of the technology is

"Oracle Label Security (OLS) provides row-level security for your database tables. You can accomplish this by assigning one or more security labels that define the level of security you want for the data rows of the table." (Oracle 2022)



The diagram illustrates Oracle Label Security (OLS) in action. On the left, a user icon is shown with the text "User session label is UNCLASSIFIED". An arrow points from the user to a table. The table has three columns: GRADE, RATE, and ROW LABEL. The table contains five rows of data. The first two rows (Manager and Senior) are labeled UNCLASSIFIED, while the last three rows (Director, Principal, and Senior) are labeled SENSITIVE or HIGHLY_SENSITIVE.

| GRADE | RATE | ROW LABEL |
|-----------|------|------------------|
| Manager | 600 | UNCLASSIFIED |
| Senior | 400 | UNCLASSIFIED |
| Director | 750 | HIGHLY_SENSITIVE |
| Principal | 600 | SENSITIVE |
| Senior | 450 | SENSITIVE |

References

<https://docs.oracle.com/database/121/TDPSG/GUID-72D524FF-5A86-495A-9D12-14CB13819D42.htm#TDPSG30351> [Accessed 16.03.2022]