Hello all,

The security model I chose was Role Based Access Control(RBAC). Currently I write finance software for the military as a civilian contractor for Deloitte, so the example given about military database systems felt a little familiar. Obviously, I cannot write about the details of that project, but I can refer to some previous RBAC systems I have worked with. My previous project was America’s largest car rental company, where I worked on high revenue websites and inherited an internal legacy application that all used some type of RBAC discretion.

In the car rental field,

An example of RBAC discretions went similar too this…

Administrators could create car rental deals and contracts.

Administrators and Marketers could sell deals and contracts to Small/Medium Businesses (SMB’s) to push the car rental product.

SMB’s could use the contracts and deals to resale to consumers, but Marketers and Administrators could not activate these contracts and deals for their own gain.

This is an example of how the roles Administrator, SMB, and Marketers all were allowed or denied access based on their roles.

A popular tool I have used that has a RBAC is called Liferay. This is an open source project I have used to deploy Java jars in its embedded Tomcat server. Liferay has a nice GUI that allows you to apply RBAC discretions by creating Roles and Groups via its GUI.

<https://learn.liferay.com/dxp/7.x/en/installation-and-upgrades/securing-liferay/securing-liferay.html?highlight=rbac>

Thanks again!

-ERIC WEBB

Then use an example of a real-life application (healthcare system, military system, school system, banking system, etc..), and discuss how features from this model can be used to support complex policies. Please give examples of such policies, (e.g. "Doctors cannot read patients information unless they are their primary care provider") and indicate which current (or older) commercial database systems implement the discussed features.

For example, if you select the multilevel model, you can take the example of a military database system, in which users' security level can be based on their military rank (General are granted a Top Secret Clearance, while Lieutenants are granted a Confidential clearance, etc.), and in which categories can correspond to the continent where they are deployed. Relations in the database are also labeled with a security level (Top Secret, Secret,...) and a category. Policies such as "Lieutenants cannot read Top Secret Documents", or  "Lieutenants can read Confidential documents only for the continent where they are deployed. " can be supported by this model. The label security mechanism in Oracle implements these features...