**COMP718 Tutorial - Information Security Models**

**Task 1**

The basic rules s of the Bell-LaPadula and Biba access control models are described below. Study the descriptions and answer the questions posted in the table below.

Bell-LaPadula Confidentiality Model:  **“no read up, no write down”**

* The ‘simple security’ BLP propertyprevents the flow of information from a level of higher security to a level of lower security: a subject at a lower clearance cannot read an object at a higher clearance level but a subject at a higher clearance level can read an object at a lower clearance Level
* The BLP \* (star) property.: prohibits a subject at a f higher clearance level to write to an object at a lower clearance level

The Biba Integrity Model: “**higher levels of integrity are more trustworthy than lower levels”**

* The simple integrity property: a subject can have read access to an object only if the security level of the subject is lower or equal to the one of the object.
* The Biba (integrity) \* property,: subject can write to an object only if the security level of the subject is equal to or higher than that of the object.

**Questions**

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **Subject** | **Object** | **BLP Simple security property y** | **BLP \* security property** | **Biba simple integrity property** | **Biba \* integrity property** |
| John BLP 5 | Book 1 BLP4 | Can John read Book 1 ? | Can John write to Book 1? | ------- | ------ |
| John BLP 5 | Book 2 BLP 6 | Can John read Book 2 ? | Can John write to Book 2? | ------- | ------- |
| Mary Biba 5 | Book 3 Biba 4 | ------- | ------- | Can Mary read Book 3? | Can Nary write to Book 3 ? |
| Mary Biba 5 | Book 4 Biba 6 | ------- | ------- | Can Mary read Book 4? | Can Mary write to Book 4 ? |
|  |  |  |  |  |  |

**Answers: (delete can or cannot , as appropriate)**

* John (BLP 5) can read Book 1 (BLP4)
* John (BL 5) cannot write to Book 1 (BLP4)
* John (BLP 5) cannot read Book 2 (BLP6)
* John (BL 5) cannot write to Book 2 (BLP6)
* Mary (Biba5) can read Book 3 (Biba4)
* Mary (Biba 5) can write to Book 3 (Biba4)
* Mary (Biba5) cannot read Book 4 (Biba6)
* Mary (Biba 5) cannot write to Book 4 (Biba6)

**Question:** If you are to select one of these access control methods, to be implemented in an organization similar to AUT, which one you will choose and why?

**Task 2**

Study the AWS report found at <https://d1.awsstatic.com/whitepapers/compliance/AWS_Data_Classification.pdf> and also available in Canvas.

Using the data classification schemes presented in the document, create a data classification scheme for a sample of the information contained in yourpersonal computer, and provide examples for each of the levels of your data classification scheme.

Level 0: Open Data

**Description**: Information that is openly available to anyone without any restrictions.

**Examples:**

-Public domain books

-Government-published datasets

-Open-source software repositories

Level 1: Public Data

**Description:** Information that can be freely disclosed without any risk.

**Examples:**

-Public blog posts

-Public social media updates

-Open-source project files

Level 2: District Data

**Description:** Information intended for internal use within an organization or among a group of trusted individuals.

**Examples:**

-Personal notes and to-do lists

-Internal emails and memos

-Draft versions of documents

Level 3: Confidential Data

**Description:** Information that requires protection due to the risk of harm or competitive disadvantage if disclosed.

**Examples:**

-Personal financial records (e.g., bank statements)

-Personal identification documents (e.g., scanned copies of IDs)

-Private correspondence (e.g., personal emails)

Level 4: Restricted Data

**Description:** Highly sensitive information that requires the highest level of protection due to the significant risk of severe harm if disclosed.

**Examples:**

-Legal documents and contracts

-Passwords and encryption keys

-Sensitive personal information (e.g., Social Security numbers, tax records)