Name: Hayden Cordeiro
Roll No.: 05
BECOMPS
Batch:D

Advance Security Systems and Digital Forensics

Assignment no 3

Answer the following questions after reading the research paper in brief
Research Paper on: Secured Information Access based on Bell LaPadula Model A Case of Novel Publishing Company

1) How is the security system structure taking care of the security management for the Novel publishing company?
The security structure has **three layers** like host link layer, application layer, and database layer of an IT based business system.
i) Host link layer:
The security system incorporated in this section uses a password that may be encrypted and stores the password field of the database. This encrypted information cannot be accessed and used by unauthorized users without having a proper decryption key.

User blocks: This module blocks unauthorized users when they fail to login to the system.

Log Tracing: A log view is maintained by the system used by the user to access the information. It provides the information's about the users they tried to access the information like the different resources or files.

Digital signature: Digital signature can realize the deification of the integrity of the original message also for non-repudiations.

ii) Application layer security:

ODBC Data store: Stores various databases

Session login authentication: This security mechanism avoids illegal users making attempts to access the information.

Stored procedures: Using stored procedures, web applications communicate with databases only through several specific strict parameters so as to separate user‟s identity from data processing, increasing the safety of data access.

Data access control: Access control can be divided into three categories; Independent access control, forcible access control, and role based access control.

iii) Database layer security:

Database: The database system contains customers data, company data and all types of transaction data.

Database backup: The database has to create a backup at periodic intervals.

Restore: In a database is to bring back or rebuild the affected database.

Data recovery: It provides the management, monitoring and automation of software to create and maintain one or more standby database to protect the corporate data from failures, disasters, human error, and data corruptions.

In order to secure the NOVEL's information generated and used both internally and externally for various purposes, it has signed up for **three security measures** that include firewall, antivirus, and Intrusion Detection Service.

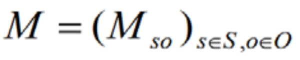
2) Discuss the BELL LAPADULA MODEL applied in this paper to achieve the security goals.

According to BLP permissions use an access control matrix and security levels. **The security policy prevents information following from a higher level to a lower level.**

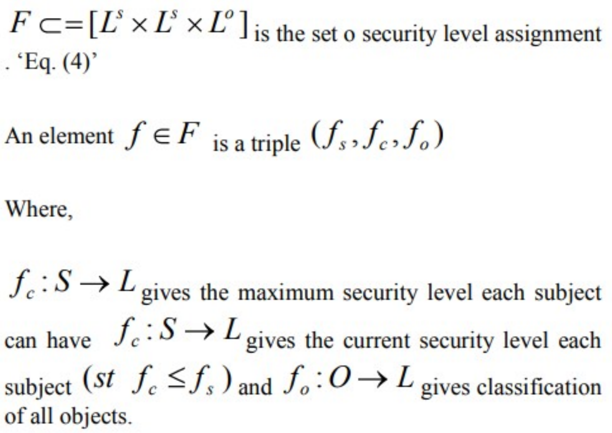
Consider the parameters: Subject S, Object O, Accesses A
A= [exec,read,write]
A set L, of security level with a partial ordering, the state set BxMxF captures the current permissions and subjects accessing objects.
The three parts are;
B= Possible current accesses
M= Permission matrices
F= Security assignment
The BLP state is triple (b, M, F) ,

B= P(S O A) is the set of all possible current access. An element bϵB is a set of triples (s,o,a) . It means that **s** is performing operations **a** on an object **o**.

M is the set of permission matrices.



$$M = (M_{so})_{s \in S, o \in O}$$



$F \subset = [L^s \times L^s \times L^o]$ is the set o security level assignment . 'Eq. (4)'

An element $f \in F$ is a triple (f_s, f_c, f_o)

Where,

$f_c : S \to L$ gives the maximum security level each subject can have $f_c : S \to L$ gives the current security level each subject $(st \;\; f_c \leq f_s)$ and $f_o : O \to L$ gives classification of all objects.

BLP Mandatory Access Control Policy (MAC):
Consider a state (b,M, f) where b is the set of current accesses.

Simple Security Property: The ss-Property states for each access (s,o,a) b. where
a {read,write},then **f (o) ≤ fs (S)**- no read-up

The Star Property Rule -
The *-Property states for each access **(s,o,a)ϵ b**.
Where, **a {append,write} then fs (S) ≤ fo (O)** and
Moreover, we must have **fo (O)≤ fo (O)** for all o’ with(s,o,a) b.
A person in a higher classification level, cannot write messages to someone in a lower classification level.
a' {read,write}(O must dominate any other object s can read).

3) What kind of security system is suggested for Novel India in this paper
The following systems are suggested to the company:

1.**Biometrics device:** for desktop systems and also it would be a better solution for the new venture where it provides online education programs. Here it may help to authenticate a user in case the registered user may give his ID and Password to some one known.

2. **RSA Token/Secure ID:** To have security where the system extends multiple login and enables the system to identify the authorized user and establish accountability for authorized user. It mitigates the two major risks of e-learning such as identity fraud by outsiders and hard to detect misdeeds by insiders. It will also enable its clients to feel and ensure reliability in its services.

3. **VPN:** Since E business needs validation of user identity and to achieve this, the enterprise must routinely expose its high value applications and data to diverse users both internal and external. Unless reliable authentication, it may not be possible to make the source available to its clients without any vulnerability to fraud, theft and malicious activities. Here VPN comes as an alternative. It also ensures the safety in the process when an user uses mobile devices such as laptop, PDA etc.,
4. In future Novell as well can think of venturing into the implementation of **retina scanning** and go for **security certification.**