**YILDIZ TECHNICAL UNIVERSITY**
**FACULTY of ELECTRICAL & ELECTRONICS ENG. / DEPT. of COMPUTER ENGINEERING**

| **Student Name Surname:** | **Number:** | | | **Signature:** | |
|---|---|---|---|---|---|
| **Course: BLM4011 Gr1,2** | **Date/Time: 02/01/2023 09:00** | | | **Duration: 60 min.** | |
| **Exam. Type: Midterm** | **MidT 1** | **MidT 2** | **MakeUp ☒** | **Final** | **MUFinal** |
| **Instructors: Prof. Dr. Hasan Hüseyin BALIK** | | | | | |

**Q1** Assume a system with N job positions. For job position i, the number of individual users in that position is and the number of permissions required for the job position is $P_i$.

a. For a traditional DAC scheme, how many relationships between users and permissions must be defined? **(10p)**
b. For a RBAC scheme, how many relationships between users and permissions must be defined? **(10p)**

**A2)**

**a.** $\sum_{i=1}^{N}(U_i \times P_i)$

**b.** $\sum_{i=1}^{N}(U_i + P_i)$

**Q2)** Consider a database table that includes a salary attribute. Suppose the three queries **sum**, **count**, and **max** (in that order) are made on the salary attribute, all conditioned on the same predicate involving other attributes. That is, a specific subset of records is selected and the three queries are performed on that subset. Suppose the first two queries are answered, and the third query is denied. Is any information leaked? **(20p)**

**A2)** If the first two queries are answered, then the max query is denied whenever its value is exactly equal to the ratio of the sum and the count values (which happens when all the selected rows have the same salary value). Hence the attacker learns the salary values of all the selected rows when denial occurs.

**Q3)** The question arises as to whether it is possible to develop a program that can analyze a piece of software to determine if it is a virus. Consider that we have a program D that is supposed to be able to do that. That is, for any program P, if we run D(P), the result returned is TRUE (P is a virus) or FALSE (P is not a virus). Now consider the following program:

```
Program CV :=

   {. . .

   main-program :=

         {if D(CV) then goto next:

            else infect-executable;

         }

next:

   }
```

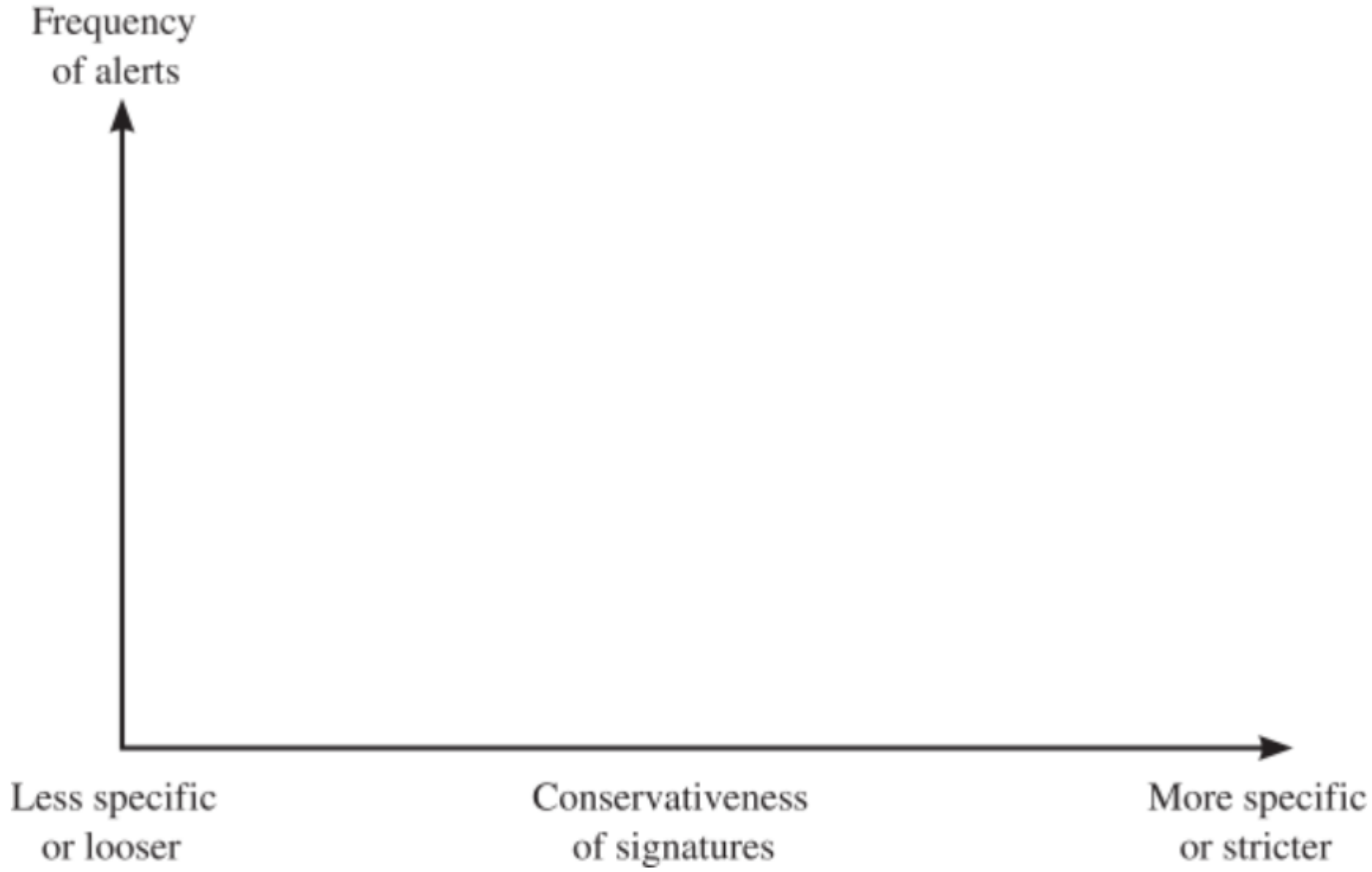
In the preceding program, infect-executable is a module that scans memory for executable programs and replicates itself in those programs. Determine if D can correctly decide whether CV is a virus. **(20p)**

**A3)** D is supposed to examine a program P and return TRUE if P is a computer virus and FALSE if it is not. But CV calls D. If D says that CV is a virus, then CV will not infect an executable. But if D says that CV is not a virus, it infects an executable. D always returns the wrong answer.

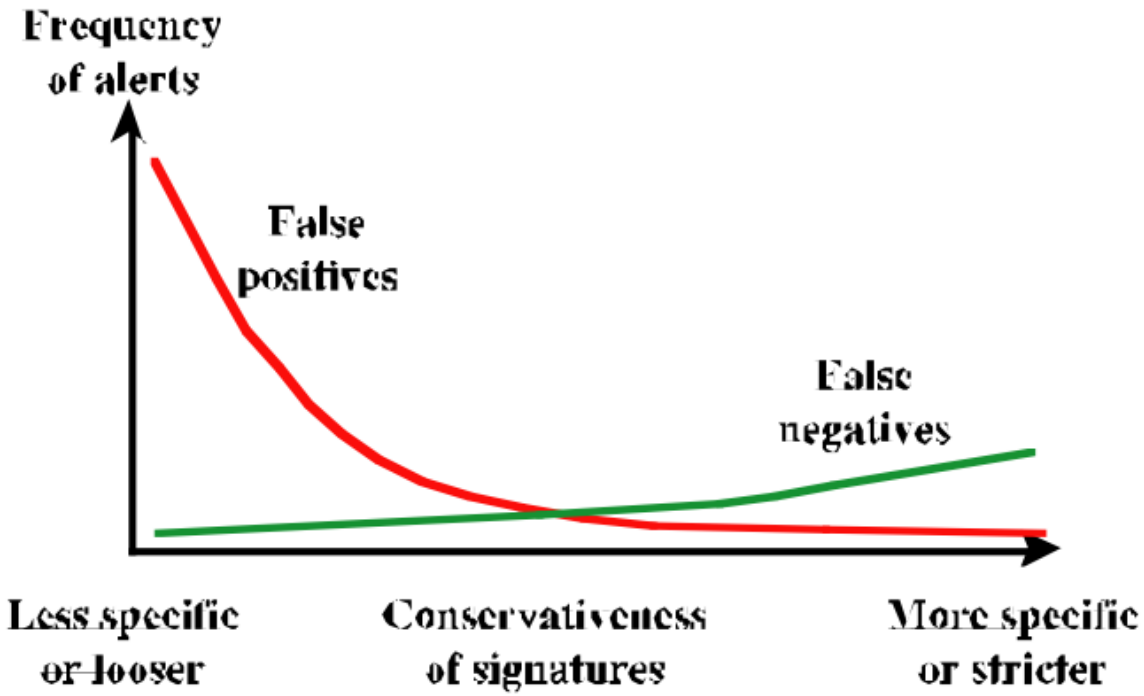


Hepinize sınavınızda başarılar dilerim.

**Q4)** In the context of an IDS, we define a false positive to be an alarm generated by an IDS in which the IDS alerts to a condition that is actually benign. A false negative occurs when an IDS fails to generate an alarm when an alert-worthy condition is in effect. Using the following diagram, depict two curves that roughly indicate false positives and false negatives, respectively: **(20p)**




**A4)**




**Q5)** Consider an automated audit log analysis tool (e.g., swatch). Can you propose some rules which could be used to distinguish "suspicious activities" from normal user behavior on a system for some organization? **(20p)**

**A5)** 'Normal' behavior would generally involve users creating, using or deleting files belonging to either the individual user or to a group to which they belong. Normal behavior would not involve attempting to gain



Hepinize sınavınızda başarılar dilerim.

superuser or root privileges or in any other way altering the operating system or attempting to perform what could be considered administrator functions. In particular the rules should watch for:

- bad or repeated login attempts
- copying large numbers of files to either external media or remote locations
- attempts to access system files or log files;
- accessing directories, files or programs that are not usually accessed;
- changing security settings.
- attempts to become a superuser using the su or sudo commands.



Hepinize sınavınızda başarılar dilerim.