Tutorial #10

Security in Computing COSC2356/2357

Q1: Why intrusion detection system (IDS) is important?

(Discuss with your peers and do it yourself)

Q2: The anomaly-based intrusion detection example presented in Lecture-10 is based on file-use statistics.

a) Many other statistics could be used as part of anomaly-based IDS. For example, network usage would be a sensible statistic to consider. List five other statistics that could reasonably be used in anomaly-based IDS.

b) Why might it be a good idea to combine several statistics rather than relying on just a few?

c) Why might it not be a good idea to combine several statistics rather than relying on just a few?

(Discuss with your peers and do it yourself)

Q3: Suppose in a host-based anomaly detection system, over an extended period of time, Alice has accessed four files, F_0, F_1, F_2, F_3, at the rates H_0, H_1, H_2, H_3, respectively, where the observed values of the H_i, for $i = 0,1,2,3$, *are* given in Table 3.1.

Table 3.1: Alice's Initial File Access Rates

H_0	H_1	H_2	H_3
0.20	0.10	0.05	0.20

Now suppose that, over a recent time interval, Alice has accessed file F_i at the rate A_i, for $i = 0,1,2,3$, as given in Table 3.2.

Table 3.2: Alice's Recent File Access Rates

A_0	A_1	A_2	A_3
0.10	0.05	0.15	0.25

Given, the statistics (S) of comparison of long-term access rates (H_i) to the current rates (A_i) is considered as normal if $S < 0.1$. Find the answers for the following questions:

a) Do Alice's recent file access rates represent normal use?

b) Suppose the previous values of access rates are weighted at 80%, while the current values are weighted 20%. What are Alice's updated file access rates?

Q4 Recall that the anomaly-based IDS example presented earlier is based on file-use statistics. The expected file use percentages are periodically updated using an equation, which can be viewed as a moving average.

a) Why is it necessary to update the expected file use percentages?
b) When we update the expected file use percentages, it creates a potential avenue of attack for Trudy. How and why is the case?

Q5 Recall the concept of **Proof-of-Work (PoW)** that was discussed in Lecture 7 and Tutorial 7. Think and discuss how **PoW** can be used to protect email spamming.