**CEG4430/6430 Homework 4**

(30 Points)

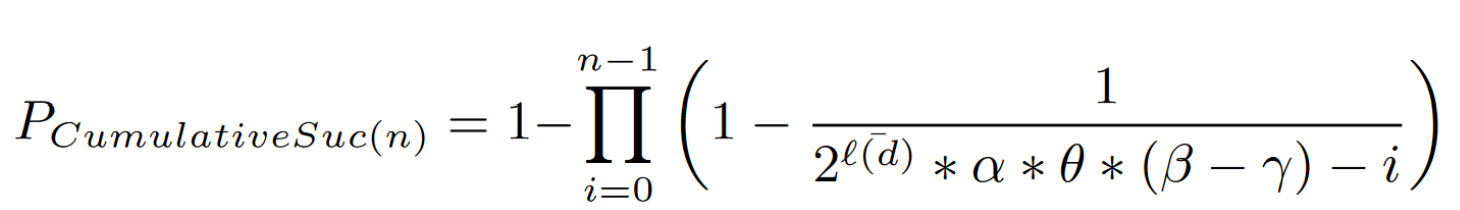
1. Please read the paper “Increased DNS Forgery Resistance Through 0x20-Bit Encoding” in the reading list (assigned previously) and answer the following questions based on the given parameter.

* α = the number of different DNS IDs
* β = the number of source ports
* ϒ = the number of source ports excluded (e.g., 1024)
* θ = the number of authority servers
* l = the length of a domain (number of letters)
  1. What is the probability for a DNS poisoning attack to be successful without 0x20? (5 Points)

Answer Question 1.a: The probability is very high if the 0x20 is not deployed, this will allow the attacker to simply brute force there way and just guess to be able to hack into whatever system they have targeted.

* 1. What is the probability for a DNS poisoning attack to be successful if 0x20 is deployed? (5 Points)

Answer Question 1.b: The probability is lower because using the 0x20 uses formulas that are found in the “Increased DNS Forgery Resistance Through 0x20-Bit Encoding” document. The formula here:



This formula is used for testing the probability of success an attacker will have with the 0x20 deployed.

1. Attackers may be actively attempting to evade a detection system. We assume that a student has developed a webserver that listens on TCP port 80. However, this webserver is vulnerable to an attack. If an HTTP request contains a string of “ATTACK” (case sensitive), the webserver will be exploited. An example is illustrated as follows:

|  |  |  |
| --- | --- | --- |
| IP Header | TCP Header | GET ATTACK http://www.google.com/ |

You have designed a signature-based (a.k.a., misuse) intrusion detection system, which will raise an alert if it finds “ATTACK” in *one* TCP packet.

* 1. How can an attacker successfully launch attacks while evading your detection system? (5 Points)

Answer Question 2.a: If the intrusion detection system will be alerted if one packet is detected with the string “ATTACK” case sensitive then if the string is split into chars each one with a packet then the detection system would not be alerted to an intrusion because it would not be detecting the the full string in a single packet. Then when the last char is sent it can go with a system() call to setup cmd to allow the attacker to do what they want.

* 1. How can you modify your detection algorithm to counteract? (10 Points)

Answer Question 2.b: Since we know the string the attacker is using is “ATTACK” case sensitive if we to a test to look for each char that matches the case sensitivity of the string the attacker will use then we can defend and stop the attacker in his/her tracks. This would be done with using basic formulas for the checking.

1. Collecting benign samples to train a model for anomaly detection is usually very expensive. Let us assume Alice and Bob accomplish the identical detection rates and false positive rates. The following figure plots how the size (e.g., memory consumption) of the model (y-axis, used to profile the benign behaviors) grows as we use more benign samples (x-axis) to train the model. Which system do you prefer according to the figure? **Give two reasons**. (dotted-Alice, line-Bob) (5 Points)

Answer Question 3: By looking at both Bob and Alice, I believe that Bob is the better option. Here are my two reasons why:

* 1. Bob has less memory usage than Alice so Bob can run quicker and have faster detection than Alice.
  2. Even as more benign samples are beign tested Bob doesn’t have to resort to using more memory and is able to stay one amount. While Alice must use more and more memory has more benign samples are beign brought in for testing.

Alice

Bob