**A Brute Force Test**

**Computer Security Project Assignment**

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Thomas Bauer

CMPS 4663 - Computer Security

July 1, 2019

The provided scenario:

**SYSTEM**: An ATM requires a four-digit pin-number (0 to 9999).

**ATTACK**: A hacker is trying to find a PIN number to access the ATM system by applying a

brute force attack. The hacker believes that he can guess the pin number in about 5000 tries, so

he starts with the value zero and without knowledge of any defense mechanism keeps

incrementing the pin by one. After trying 10,000 times, the attacker may think that the user

changed his PIN number during the attack, so he will try again the full exhaustive search 4 more

times and then give up.

**DEFENSE**: The security administrator for the ATM system implemented a mechanism that will

randomly change the PIN number if there are 50 wrong attempts.

**PROJECT**

The project starts by randomly choosing a numeric PIN of length 4 digits (0000 – 9999). It then runs an exhaustive search (brute force) to find the chosen pin. The program chooses a new random PIN after 50 wrong attempts from the attacker. From there, the program measures the number of iterations required to find a match. The program is set to run 40 times. The first twenty iterations change the PIN after 50 wrong attempts and the second twenty change the PIN after 25 wrong attempts. Each iteration has a maximum of 10,000 tries. Every time the program is run, it has a new initial random value by using the srand() function to originally seed the random number generator.

Given that it is always better to increase the number of data points for statistical analysis, I chose to run the program 20 rounds for each of the different PIN change amounts (50 and 25) for a total of 40 rounds. When the PIN number changed every 50 attempts, the results saw 75% of the rounds end up with the attacker’s brute force attempts finding the correct PIN number and gaining access. Upon switching to the rounds where the PIN number changed with every 25 attempts, it lessened the number of successful intrusions by the attacker to 60%.