Mouse-behavior Detection

Advanced OS Project Presentation

Yeganeh Azmoudeh - 97463102

INTRODUCTION

This project generally is for security purposes. Although it is a simple demo for a big purpose but hopefully a useful one.

Security in our OS systems is an important issue. We can improve our OS security to harden our OS by many different means and one of them can be mouse movement detection.

We will discuss why and how in the following slides.

OVERVIEW

We will detect and collect some parameters of a user in an specific period of time and then we will use it in testing time that if the same person is using and moving the mouse and does actions or not.

PROBLEM STATEMENT

Security in our OS systems is an important matter. We can improve our OS security to harden our OS by many different tools and one of them can be mouse movement detection.

PARAMETERS

SPEED

CLICK FREQUENCY

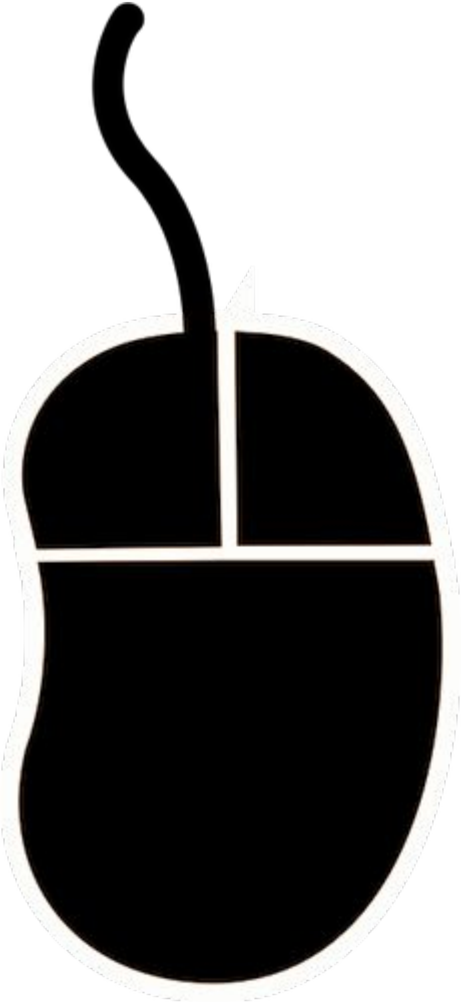
PATH CURVATURE

DUELL TIME

STRATEGY

As you just saw we will use some parameters to detect a user's behavior and then use it to specify and detect if it is the same behavior or not so we can tell if the user has changed or not.

These parameters help specify mouse movement patterns.



HOW WE PUT IT IN TEST

To test “Mouse-behavior Detection” we would gather user data (mouse-events) in a generic log file which would capture 3 types of events: move, click and scroll.

After a period of time the collected data would be processed to calculate a threshold for each parameter.

Then in the test time the collected data would be compared to the threshold.

FINDING THE RIGHT PARAMETER'S VALUE

We first create a log file that contains our mouse movement patterns. Based on that log file we are going to check user behavior on test time.

We extract 2 lower and upper values for each parameter out of the log file. If one parameter on test time is between these two lower and upper values, the user is expected to be the same.

FINDING THE RIGHT PARAMETER’S VALUE

However, this method’s accuracy is low. Since in our tests it would detect the user change when the user was the same in both steps(data collection , testing).

To solve this problem we would allow some tolerance such that for example 60 percent of metric’s match would mean that user is the same.

IMPROVEMENT IDEAS

1

Suspicious Activity Alert

We could inform the user when a suspicious activity is detected (e.g. by email)

2

Log Rotation

A new log file could be generated periodically since the user behavior could change over time.

3

System Lock

Lock the OS when too many suspicious activities are detected in a row.

Thank you for embracing the future of OS hardening with us.