MINI PROJECT: Intruder Identification System

PROBLEM STATEMENT

Introduction

In information security, intruder detection is the act of detecting intruders behind attacks as unique persons. This technique tries to identify the person behind an attack by analyzing their computational behavior. Intruder detection systems try to detect the identity of the perpetrator attacking a system by analyzing his or her computational behavior or biometric behavior.

Frequently used parameters used to identify an attacker:

- Keystroke Dynamics (aka keystroke patterns, typing pattern, typing behavior)
- Patterns using an interactive command interpreter:
    - Commands used
    - Commands sequence
    - Accessed directories
    - Character deletion
- Patterns on the network usage:
    - IP address used
        - ISP
        - Country
        - City
    - Ports used
    - TTL analysis
    - Operating system used to attack
    - Protocols used
    - Connection times patterns

Problem Statement

The problem with the current methods to classify/identify attackers is, that they are not effectively implemented in the real world, in a standardized manner.

Detecting the identity of the attacker merely on the basis of one's computational behavior is not enough. There need to be systemized programs and/or protocols put into use to identify a perpetrator's identity.