An Internal Intrusion Detection and Protection System by Using Data Mining and Forensic Techniques

Basically Intrusion Detection topics were detecting attacks is the network or outside the network, but this paper is NOT the concept one of network attack, its Internal Intrusion Detection.

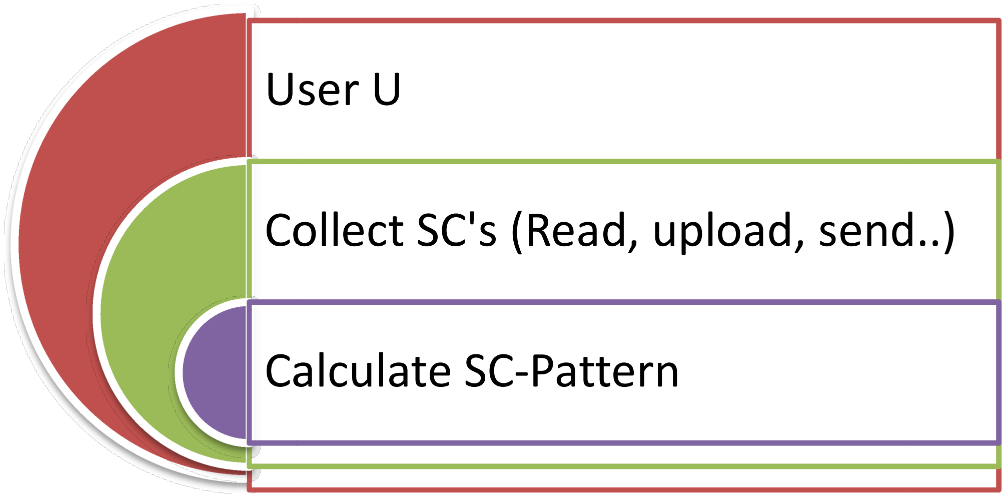
To authenticate users, currently, most systems check using login pattern using user id and password. And it's very quite common knowing login details of other user's, assistances within an organization or company, they may then log in to the system, access users' private files, or modify or destroy system settings. Those attacks we call it as Internal Intrusion Detection, and those attackers called internal intruder.

Now we proposing a framework or security system, named Internal Intrusion Detection and Protection System (IIDPS), to detect Internal Intrusion and internal intruders.

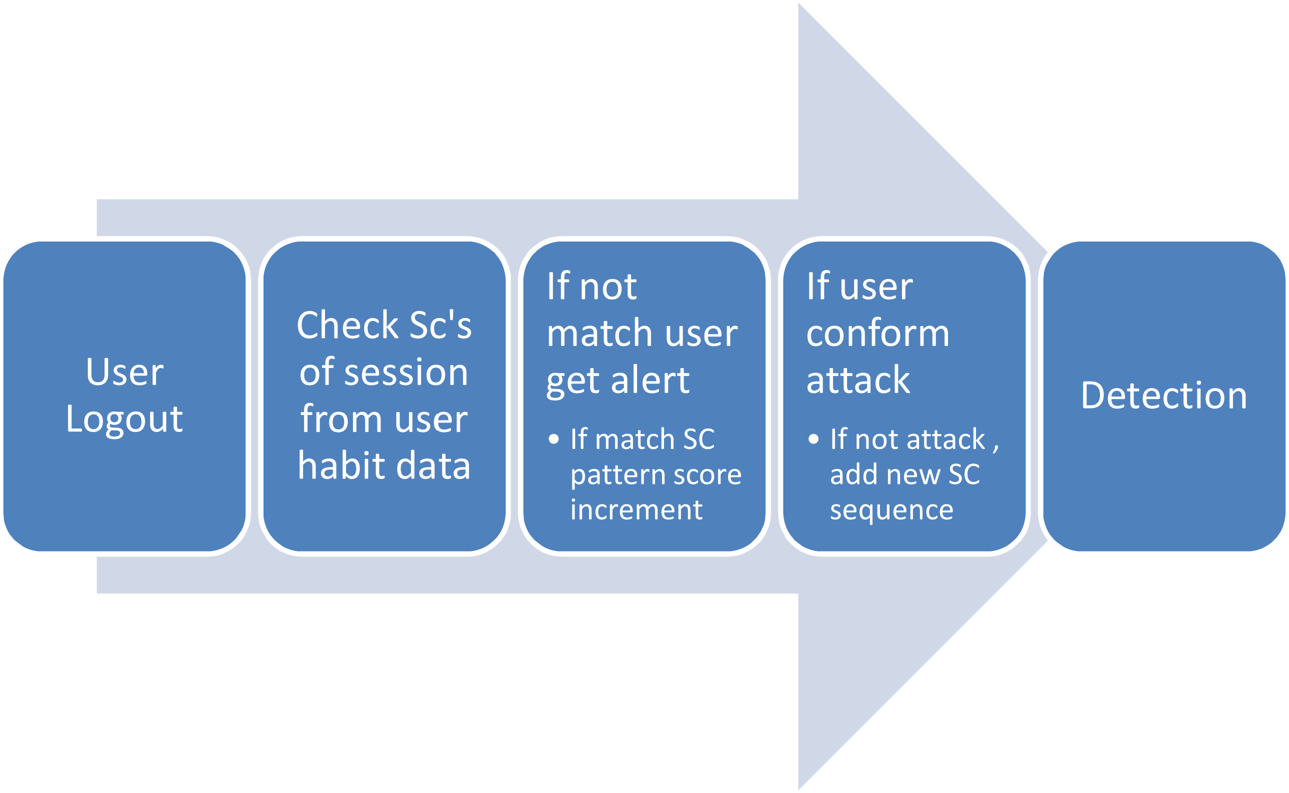
For this we are using system Calls (SC), means user operations on system. We collect SC-Sequences based on user operations, and store in user's habit data, and mine the data like calculate weight of the SC-sequence. Based on SC-sequence we mine the SC-pattern.

Execution flow

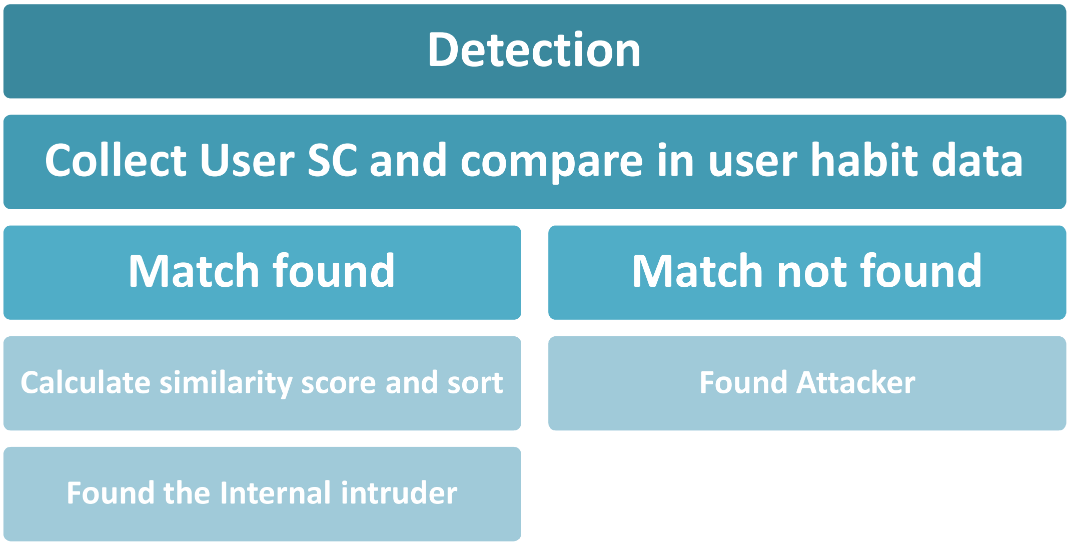
1)


User U
Collect SC's (Read, upload, send..)
Calculate SC-Pattern

2)


User Logout
Check Sc's of session from user habit data
If not match user get alert
• If match SC pattern score increment
If user conform attack
• If not attack , add new SC sequence
Detection

3)



Detection

Collect User SC and compare in user habit data

Match found

Match not found

Calculate similarity score and sort

Found Attacker

Found the Internal intruder

Attack Types

Type 1:

This attack is defined as the situation where a user (attacker) of a normal SC's like read, search, getlist, download etc..

Type 2:

This attack is an attack that launches a sensitive SC's, which is defined as sensitive data, that may delete, update, chgmod etc..

Type 3:

This attack is an attack that launches a higher access right to attack the system, e.g., cracking password.