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

By G. Sharath Chandra, S. Praneetha Reddy

***Abstract—***Currently, most computer systems use user IDs and passwords as the login patterns to authenticate users. However, many people share their login patterns with coworkers and request these coworkers to assist co-tasks, thereby making the pattern as one of the weakest points of computer security. Insider attackers, the valid users of a system who attack the system internally, are hard to detect since most intrusion detection systems and firewallls identify and isolate malicious behaviors launched form the outside world of the system only. In addition, some studies claimed that analysing system calls (SCs) generated by commands can identify these commands, with which to accurately detect attacks, and attack patterns are the features of an attack. Therefore, in this paper, a security system, named Internal Intrusion Detection and Protection System (IIDPS), is proposed to detect insider attacks at SC level by using data mining and forensic techniques. The IIDPS creates users’ personal profiles to keep track of users’ usage and forensic techniques. The IIDPS creates users’ personal profiles to keep track of users’ usage habits as their forensic features and determines whether a valid login user is the account holder or not by comparing his/her current computer usage behaviors with the patterns collected in the account holder’s personal profile.

***Index Terms—***Data mining, insider attack, intrusion detection and protection, system calls (SC), users’ behaviors.

**Existing System:**

* When people exploit powerful capabilities and processing powers of computer system, security has been one of the serious problem in computer domain since attackers very usually try to penetrate computer systems and behave maliciously.
* Attackers may install trojans to pilfer victims login patterns or issue a large scale of trials with the assistance of a dictionary to acquire users’ passwords.
* Techniques: Firewalls and intrusion detection systems (IDSs).
* Technique Definition: Insider attack is one of the most difficult ones to be detected because firewalls and intrusion detection systems (IDSs) usually defend against outside attacks.

**Drawbacks:**

* When successful, they may then log in to the system, access users’ private files, or modify or destroy system settings.
* Accuracy of detection is low.

**Proposed System:**

* We propose a system named IIDPS which detects malicious behaviour of the user, launced at a SC level. The IIDPS uses data mining and forensic profiling techniques to study System Call pattern.
* The user’s forensic pattern, defined as the SC pattern frequently appearing in a user’s submitted SC- sequences but rarely being used by other users, are retrieved from the user’s computer usage history.

**Proposed Technique:**

* Forensic and data mining.

**Advantages:**

* Techniques used for intrusion detection provide effective attack resistance.
* The average detection accuracy is higher.

**Applications:**

* Health record management.
* Organisations.
* Anywhere where confidentiality is required.

**Hardware Requirements:**

* **Processor:** Pentium 4 or higher.
* **RAM:** 4GB atleast for optimum performance.
* **Hard disk:** 40 GB

**Software Requirements:**

* **Front end:** HTML, CSS, Bootstrap, JavaScript.
* **Operating System:** Windows 7 or higher
* **Back end:** Python Django.
* **Database:** MySQL.