# Introduction

Intrusion Detection is the process used to identify intrusions, which try to violate the security policy of the system.

Based on the sources of the audit information used by each IDS, the IDSs may be classified into

* + Host-base IDSs
  + Distributed IDSs
  + Network-based IDSs

Host-based IDSs collects audit data from host audit trails and detect attacks against a single host.

Distributed IDSs collects audit data from multiple hosts and possibly the network that connects the hosts and detect attacks involving multiple hosts.

Network-Based IDSs use network traffic as the audit data source, relieving the burden on the hosts that usually provide normal computing services and detect attacks from the network.

OR

Intrusion detection is the problem of identifying unauthorized use, misuse, and abuse of computer systems by both system insiders and external penetrators. The proliferation of heterogeneous computer networks provides additional implications for the intrusion detection problem. Namely, the increased connectivity of computer systems gives greater access to outsiders, and makes it easier for intruders to avoid detection. IDS's are based on the belief that an intruder's behavior will be noticeably different from that of a legitimate user.

(or use above para in the form of motivation…with little modification+ big losses report [http://www.bzaugg.com/2010/06/an-overview-of-intrusion-detection-systems-technology-and-research/])

The above link has previous work done in IDS also…so it can be taken up for background..+take conculision also

***Motivation***

* Developing absolutely secure systems is not possible, Most existing systems have security flaws
* Abuses by privileged insiders are possible
* Not all kinds of intrusions are known

So quick detection of intrusions can help to identify intruders and limit damage, where IDS serves as a deterrent

*1.1 Intrusion Detection Techniques:*

* Misuse detection: Catch the intrusions in terms of the characteristics of known attacks or system vulnerabilities.
* Anomaly detection: Detect any action that significantly deviates from the normal behavior.

|  |  |  |
| --- | --- | --- |
|  | Advantage | Disadvantage |
| Misuse Detection | Accurately and generate much fewer false alarm | Cannot detect novel or unknown attacks |
| Anomaly Detection | Is able to detect unknown attacks based on audit | High false-alarm and limited by training data. |

*1.2 Challenge involved*

* Based on audit data collected over a period of normal operation.
  + When a noise (intrusion) data in the training data, it will make a mis-classification.
* The features selection decision requires domain experts. And it may not be completely.

*1.3 Our Aim*

* + Resources to be protected
  + Models of the “normal” or “legitimate” behavior on the resources
* Efficient methods that compare real-time activities against the models and report probably “intrusive” activities

*1.4 Our Approach*

1. Define and extract the features of behavior in system (CPU Utilisation)
2. Define and extract the Rules of Intrusion
3. Apply the rules to detect the intrusion

<<Flowchart>>

Pattern Found:

1. On holidays machine was used much..threshold set high.
2. On non-holidays machine wasn’t used much..threshold set low.

<for finding holidays…google calendar help taken..we can do this><sats n sunday>

<and yashika can u please store the CPU utilization values for continuously atleast for 3days…this data set will give us good impact, and show that we haven’t randomly selected the threshold, but it was predict using the data><similarly for night and day><pattern matching..will help actually here>

<and we can use small questionare to be filled by user, to ask few questions like…u use ur computer max on holiday or on working day, do u use any cloud service t store ur data…if yes which…so that we can detect its location, and see if much uploading to not know place is made then promp the user…this kind of thing will help us in selecting the value of threshold>…these questions can asked through system.out.println()…java code

**<and shall we include login frequency, password frequency, exexcution denied, execution frequnc…as other prameters><they won’ttake much time…round about 1hr>**

**Ways by which we are protecting…or we can put inside motivation part also**

1. Blocking access to malicious servers
2. Allowing download from only non-malicious servers
3. Continuous monitoring of the system utilization