A
presentation over term paper
on
*intrusio*n detection

- Anomaly Detection
- Misuse Detection

Definition

INTRUSION

- The potential possibility of a deliberate unauthorized attempt to:

•Access information

•Manipulate information

•Render a system unreliable or unusable

INTRUSION DETECTION

- The process of identifying and responding to intrusion activities

Types of Intrusion

There are six types of Intrusions

- Attempted break-ins
- Masquerade attacks
- Penetration of the security control system
- Leakage
- Denial of service
- Malicious use

Intrusion Detection Techniques

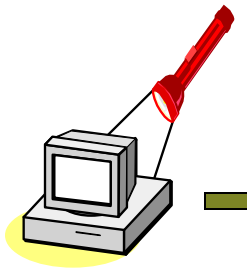
- Anomaly Detection
  - ❖ Static
  - ❖ Dynamic
- Misuse Detection

  Ex:- NIDES, MIDAS, STAT

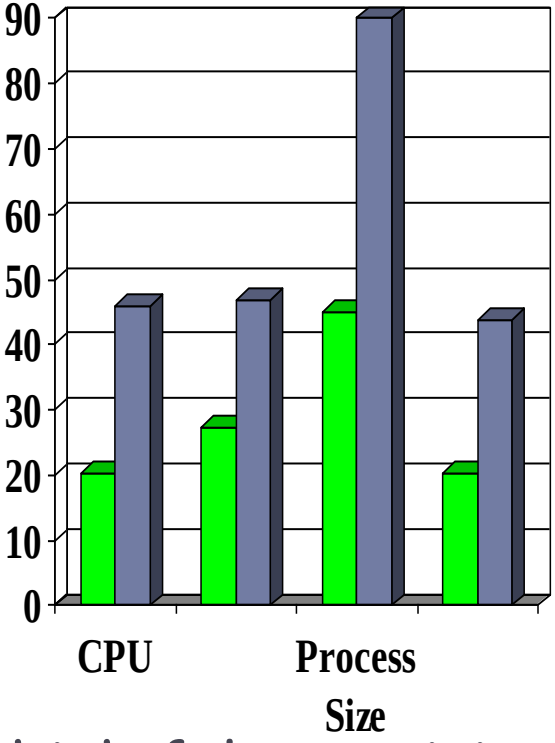
Anomaly Detection Systems

- Statistical approaches
  - ❖Tripwire, Self/Non-self
- Dynamic /Predictive pattern generation
  - ❖NIDES, Pattern Matching (UNM)

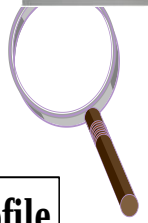
Anomaly Detection



activity measures



probable intrusion

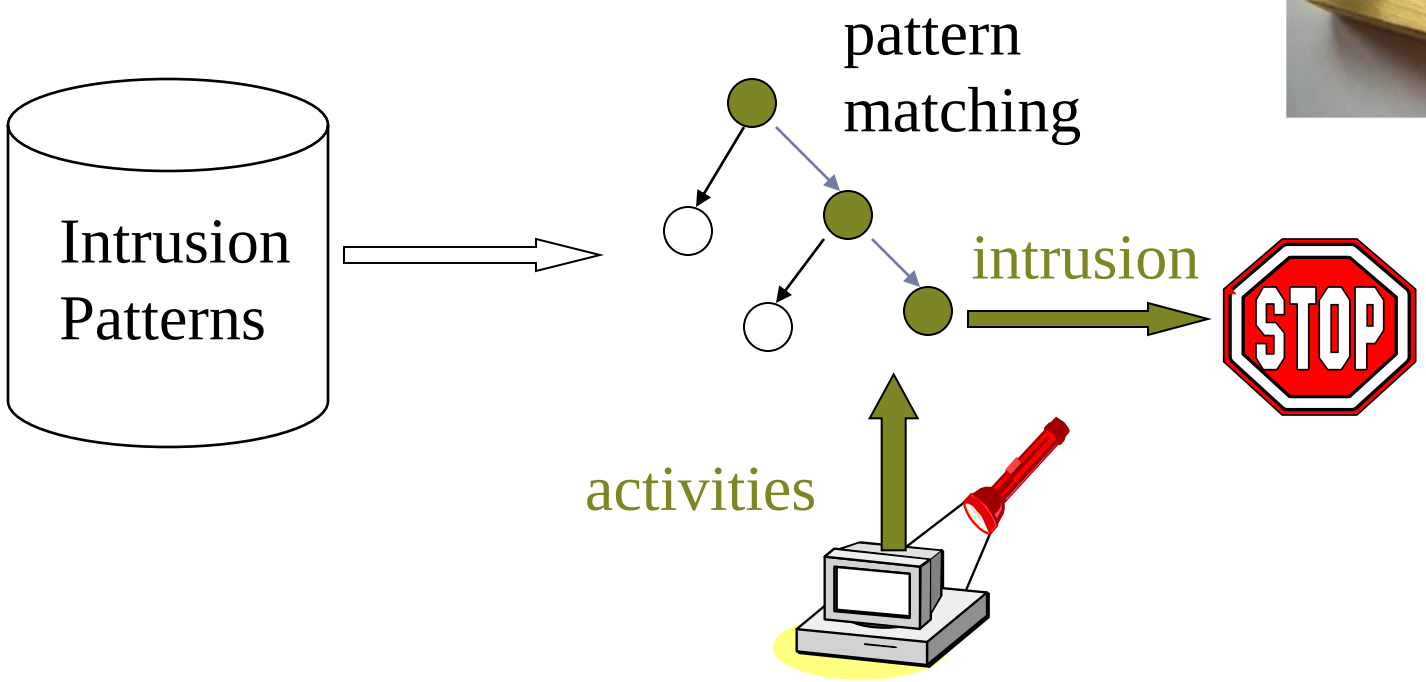


Relatively high false positive rate -
anomalies can just be new normal activities.

Misuse Detection Systems

- Expert Systems
- Keystroke Monitoring
- Model Based Intrusion Detection

Misuse Detection



Example: ***if*** (src_ip == dst_ip) ***then*** “land attack”

Can’t detect new attacks

IDS Design

Components of IDS

system activities are observable

Audit Records

Audit Data Preprocessor

Activity Data

Detection Models

Detection Engine

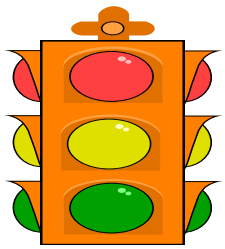
normal and intrusive activities have distinct evidence

Alarms

Decision Table

Decision Engine

Action/Report



Important Features

- Fault tolerant.
- Minimum human supervision.
- Resist subversion.
- Minimal Overhead.
- Platform Independent

Continued…

- Adaptable.
- Easy to Deploy.
- Detect different types of attacks.
  - ❖ Anomaly detection schemes
  - ❖ Misuse detection schemes
  - ❖ Combination of both
- Hardware / Software must be synchronized.
- Good data mining techniques

Data Mining

Definition: The semi-automatic discovery of patterns, associations, changes, anomalies, rules, and statically significant structures and events in data.

Data such as,

- Failed connection attempts
- Connection delays
- Source/Destination data packets

Data Mining Algorithms

Extract knowledge in the form of models from data.

- Classification
- Regression
- Clustering
- Association rule abduction
- Sequence Analysis
- Others

Data Mining Techniques

It allows the system to collect useful knowledge that describes a user's or program's behavior from large audit data sets.

Examples:

- Statistics
- Artificial Neural Network
- Rule Learning
- Neuro-Fuzzy

IDS Evaluation

- Rate of false positives
- Attack detection rate
- Maintenance cost
- Total cost

IDS for Mobile Wireless Systems

Designing for Wireless Networks

Problems with Wireless Networks

- Open Medium
- Dynamic changing network topology
- Lack of decentralized monitoring
- Less known security measures
- Data is harder to collect

One proposed IDS design by Georgia Institute of Technology

- Individual IDS agents are placed on each an every node.
  - Monitors local activities
    - User, system and communication activities
- Nodes cooperate with each other.
  - Investigate together at a broader range
- A secure communication channel among the IDS Agent.

references

•Chebrolu, S., Abraham, A., Thomas, J.P.: Feature Detection and Ensemble Design of Intrusion Detection Systems. Computers and security, http://dx.doi.org/10.1016/j.cose.2004.09.008

•Zhang, Y., Lee, W., and Huang, Y. 2003. Intrusion detection techniques for mobile wireless networks. Wirel. Netw. 9, 5 (Sep. 2003), 545-556. DOI= http://dx.doi.org/10.1023/A:1024600519144

•J.P Anderson. Computer Security Threat Monitoring and Surveillance. Technical report, James P Anderson Co., Fort Washington, Pennsylvania, April 1980

•Eugene H Spafford. Security Seminar, Department of Computer Sciences, Purdue University, Jan 1996.

•Biswanath Mukherjee, L Todd Heberlein and Karl N Levitt. Network Intrusion Detection , IEEE Network, May/June 1994, pages 26-41.