ABSTRACT

Motivation

This project has been handled to us as a 6th semester major project for the fulfillment of the requirements for the degree of the Master of Computer Application. The project work is motivated by the growth and demand of Computer Science, specially in the field of Network.

Problem Statements:

Survey And Implementation Of Behavior Model For Detecting Data Exfiltration.

Data Exfiltration or Extrusion is the unauthorized data transfer from a computer. Within an organization, the possibility of a confidential information leak ranks among the highest fears of any executive. Detecting information leaks is a challenging problem, since most organizations depend on a broad and diverse communications network. It is not always straightforward to conclude which information is leaving the organization legitimately, and which communications are malicious data exfiltrations. Sometimes it is not even possible to tell that a communication is occurring at all.

The primary focus of any data exfiltration detection technique is the ability to make a distinction between legitimate and malicious information communication. Most communications appear benign from the outside; for instance, when a coworker prints a page on a printer, or when a website is loaded over the network. Other communications and events are malicious by their very nature, such as trojan backdoor traffic or a laptop theft. Note, however, that in neither malicious example it is clearly evident whether the goal is data exfiltration, or some other nefarious purpose. Some malicious data exfiltrations require an insider, while many others can be accomplished through a computer network attack or a simple accident. For example, a disgruntled employee may be using a telephone conversation to communicate confidential customer information to a competitor, or the database administrator may have accidentally left the database open to access with no password required. This prompts many organizations (most notably governments) to adopt tiered levels of confidentiality for sensitive information, effectively protecting and auditing the access to the information instead of monitoring all of the actual communications per se.