**Hardware based Intrusion Detection System**

**A Project Synopsis**

**Presented At**

**Maharaja Surajmal Institute of Technology**



By

Amit Sharma

Nishant Kumar

Atif Ahmed

**Project Guide: Prof. Poonam Dhankar**

# Abstract

Intrusion-detection systems aim at detecting attacks against computer systems and networks or, in general, against information systems. Indeed, it is difficult to provide provably secure information systems and to maintain them in such a secure state during their lifetime and utilization. Sometimes, legacy or operational constraints do not even allow the definition of a fully secure information system. Therefore, intrusion detection systems have the task of monitoring the usage of such systems to detect any apparition of insecure states. They detect attempts and active misuse either by legitimate users of the information systems or by external parties to abuse their privileges or exploit security vulnerabilities.

# Introduction

IDS arms any business against attacks by continuously monitoring network activity, ensuring all activity is normal. If IDS detects malicious activity it responds immediately by destroying the attacker's access and shutting down the attack. IDS reads network traffic and looks for patterns of attacks or signatures, if a signature is identified, IDS sends an alert to the Management Console and a response is immediately deployed.

The reason of developing this tool was the following:

* IDS(s) are difficult to setup
* Costs are high
* Rules implemented on the IDS can clash with services

# Objective

Main objective of this tool is to create a portable hardware based IDS which can be installed easily without any technical knowledge. Thus, empowering the common user and protecting them against the attack vectors.

# Hardware & Software

The development of the tool requires

Raspberry Pi and peripheral devices

Minibian OS

Snort

# Contribution of the Project

As development of the project is complete this can be used as a commercial plug and play module that can protect the enterprise or home network from any outside intrusions and attacks.

# Conclusion

There are limited number of available IDS specially as a hardware which is cheap and easy to deploy. Most of them require an expert supervision while setting up the rules. And due to the above-mentioned reasons home users are still in a vulnerable state where and attacker can exploit the network. The tool which we are developing resolves all the issues which are suggested in the document