VISVESVARAYA TECHNOLOGICAL UNIVERSITY

BELGAUM-590014

A Project Report
On

"CHAKRAVYUHA"

A project report submitted in partial fulfillment of the requirements for the award of the degree of ***Bachelor of Engineering in Computer Science and Engineering*** *of Visvesvaraya Technological University, Belgaum*

Submitted by:

KUSHAL B R	**1RN06CS042**
ABID ALI M	**1RN06CS003**
KIRAN N	**1RN06CS040**
TARUN PAI	**1RN06CS059**

Carried out at
RNSIT

Under the Guidance of:
Dr. G T Raju
Prof. and HOD
Dept. of CSE

Department of Computer Science and Engineering
RNS Institute of Technology
Channasandra, Uttarahalli-Kengeri Main Road, Bangalore-560 061

2009-2010

ABSTRACT

Computer security is a branch of computer technology known as information security as applied to computers and networks. The objective of computer security includes protection of information and property from theft, corruption, or natural disaster, while allowing the information and property to remain accessible and productive to its intended users. The term computer system security means the collective processes and mechanisms by which sensitive and valuable information and services are protected from publication, tampering or collapse by unauthorized activities or untrustworthy individuals and unplanned events respectively. The strategies and methodologies of computer security often differ from most other computer technologies because of its somewhat elusive objective of preventing unwanted computer behavior instead of enabling wanted computer behavior.

Hardware based or assisted computer security offers an alternative to software-only computer security. Devices such as motion sensors may be considered more secure due to the physical access required in order to be compromised. While much software based security solutions encrypt the data to prevent data from being stolen, a malicious program or a hacker may corrupt the data in order to make it unrecoverable or unusable. Similarly, encrypted operating systems can be corrupted by a malicious program or a hacker, making the system unusable. Hardware-based security solutions can prevent read and write access to data and hence offers very strong protection against tampering and unauthorized access. Working of hardware based security: A hardware device allows a user to login, logout and to set different privilege levels by doing manual actions. The device uses biometric technology to prevent malicious users from logging in, logging out, and changing privilege levels. The current state of a user of the device is read both by a computer and controllers in peripheral devices such as hard disks. Illegal access by a malicious user or a malicious program is interrupted based on the current state of a user by hard disk and DVD controllers making illegal access to data impossible. Hardware based access control is more secure than logging in and logging out using operating systems as operating systems are vulnerable to malicious attacks. Since software cannot manipulate the user privilege levels, it is impossible for a hacker or a malicious program to gain access to secure data protected by hardware or performs unauthorized privileged operations. The hardware protects the operating system image and file system privileges from being tampered. Therefore, a completely secure system can be created using a combination of hardware based security and secure system administration policies.