Proposed Isomorphic Graph Model for Risk Assessment on a Unix Operating System

Prashant Kumar Patra, Department of Computer Science & Engineering, College of Engineering & Technology, Bhubaneswar, Odisha, India
Padma Lochan Pradhan, Dept. of CSE, Sikha ‘O’ Anusandhan University, Bhubaneswar, Odisha, India

ABSTRACT

Control and risk are the two parts of the coin. Risk assessment is the process of identifying uncertainties, vulnerabilities and threats to the operating system resources in order to achieve business objectives. Risk evaluation involved deciding what counter measures to take in reducing uncertainty to the lowest level of risk. Control is probably the most important aspect of communications security and becoming increasingly important as basic building block for system security. Advanced Encryption Standard (AES) is a primary method of protecting system resources. AES is inversely proportional to the Risk (C=K/R) & mean while control is directly proportional to the quality of standard. AES Control will be optimize the risk as well as improve the IS standard. Control is directly proportional to risk mitigation & mitigation is directly proportional to standard. This paper contributes to the development of an optimization method that aims to determine the optimal cost to be invested into security method, model & mechanisms deciding on the measure component of operating system resources (i.e. Processor, Memory & Encryption Key). Furthermore, the method & mechanism optimize the cost, time & resources is supposed to optimize the system risks. The proposed model would be update the value of Processor, Memory & Encryption key dynamically as per business requirement and availability of technology & resources. Proposed model is going to be optimizing risk and maximizing the performance. In this study the researchers develop an isomorphic graph model for optimizing risk in the Unix operating system.

Keywords: Advanced Encryption Standard (AES), Control, Pyramid Diagram, Risk, Standards, Unix

INTRODUCTION

Currently, the increased use of the clients, business and computer & communications system by IT industries has increased the risk of theft of proprietary information is a measure problem in around the globe. The operating system risk assessment, control and audit is a primary method of protecting system resources (Processor, Memory & Encryption Key). The system risk assessment and control is probably the most important aspect of communications security for preventive control. Therefore, the top management has to decide whether to ac-

DOI: 10.4018/ijrcm.2013070104
cept expected losses or to invest into technical
security mechanisms in order to optimize the
frequency of attacks and system down time.

There are various kinds of controls avail-
able and implemented on operating systems to
protect our information technology (IT) assets
against external & internal hackers. The operat-
ing system is consists of three main components
such as, file, shell & kernel. The processor &
memory is the core component of any types
operating system.

The processor and kernel is fully functional
dependency on each other, but file and shell is
the communication components of the OS. We
can improve the performance of OS by updating
the kernel time to time. Kernel is the Nucleus
of the operating system. The architecture of the
Unix operating system is shown in Figure 1.

The machine is consists of millions of
chips, each capable of testing a million keys
per second, such machine could be test $2^{56}$
key in 20 hours. It is easy to design a machine
with a million parallel processors, each work-
ing independent of the others. The encryption
key length size is depends Memory, Control,
Arithmetic unit, Processor etc. to perform the
functionality of the operating system.

The operating system control is the process
to address security weaknesses in operation
systems by implementing the latest OS patches,
hot fixes and updates and the procedures and
policies to reduce attacks and system down
time mean while increase the throughput of
the system.

Preventive control of the operating systems
is the first step towards safeguarding systems
from intrusion, workstations, applications; net-
work and servers typically arrive from the ven-
dor, installed with a multitude of development
tools and utilities, which although beneficial
to the user, also provide potential back-door
access to the systems.

Control of an operating system involves
the removal of all non essential tools, utilities
and other systems programmer options, any of
which could be used to ease a hacker’s path to
our systems.

The greatest difficulty in getting millions
of routers and computers to work on a brute-
force attack is convincing millions of computer
owners to participate around the globe. We
could ask politely, but that’s time consuming
and they might say no.

We could try breaking into their machines,
but that’s even more time consuming and we

---

**Figure 1. Diagram of Unix system (source: authors)**
Threats and Security Issues in Smart City Devices
www.igi-global.com/chapter/threats-and-security-issues-in-smart-city-devices/227776?camid=4v1a

Evaluating Security and Resilience of Critical Networked Infrastructures after Stuxnet
www.igi-global.com/chapter/evaluating-security-resilience-critical-networked/74634?camid=4v1a

GARCH Risk Assessment of Inflation and Industrial Production Factors on Pakistan Stocks
www.igi-global.com/article/garch-risk-assessment-inflation-industrial/74751?camid=4v1a