Chapter 22
Proposed Isomorphic Graph Model for Risk Assessment on a Unix Operating System

Prashant Kumar Patra
College of Engineering & Technology, India

Padma Lochan Pradhan
Sikha 'O' Anusandhan University, 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). 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.

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

DOI: 10.4018/978-1-4666-8473-7.ch022

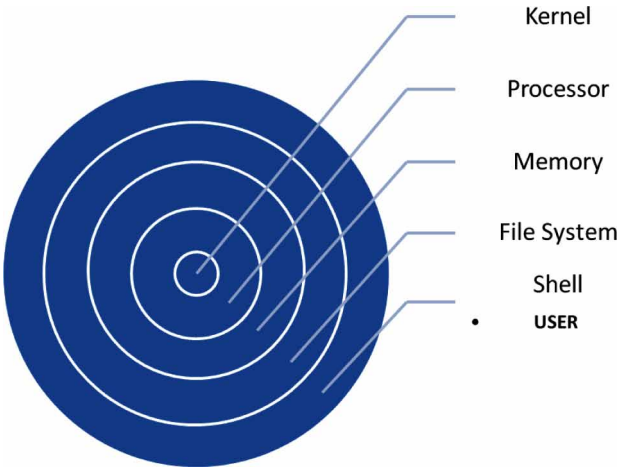
and control is probably the most important aspect of communications security for preventive control. Therefore, the top management has to decide whether to accept expected losses or to invest into technical security mechanisms in order to optimize the frequency of attacks and system down time.

There are various kinds of controls available and implemented on operating systems to protect our information technology (IT) assets against external & internal hackers. The operating 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 working 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.

Figure 1. Diagram of Unix system (source: authors)



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; network and servers typically arrive from the vendor, 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 might get arrested, we could also use a computer virus and other hacking tools & scripts to spread the cracking program more efficiently over many computers as possible at a time. Therefore, we need pre-planned prevention to safe guard the critical IT Infrastructure.

The primary purpose of security policy is to inform those responsible for protecting assets such as hardware, software, and data of their obligations. Management establishes a security policy based on the risks it is willing to tolerate. The policy itself does not set goals, but serves as a bridge between management's goals and the technical implementation.

Security is a process, not a result. It is a process which is difficult to adopt under normal condi-