Dynamic Semi-Group CIA Pattern Optimizing the Risk on RTS

Padma Lochan Pradhan, Gokul Institute of Technology & Science, Bobbili, VZM, AP, India

ABSTRACT

The preventive control is one of the best well advance control for recent complex IS Security Application to protect the data and services from the uncertainty, hacker, and unauthorized users. Now, increasing the demand and importance of business, information & communication system & growing the external risks is a very common phenomenon for everywhere. The RTS security put forward to the management focus on IT infrastructure. This work contributes to the development of an optimization pattern that aims to determine the optimal cost to be apply into security mechanisms deciding on the measure components of system security and resources. The author's mechanism should be design in such way, the Confidentiality, Integrity, Availability, Authenticity and Accountability are automatically PDC for all the time. The author has to optimize the system attacks and down time by implementing semi-group structure CIA pattern, mean while improving the throughput of the Business, Resources & Technology. Finally, the author has to maximize the protection of IT resources & Services for all the time and every time. This proposed CIA Pattern is the part of protection, detection, benchmarking, fault analysis and risk assessment of real time operating system and applicable to efficient resource management on web application.

KEYWORD

Access Control Mechanism, Authentication, Confidentiality, Detective & Corrective Control, Integrity, Preventive Access Control Mechanism, Preventive, Return on Investment, Risk Mitigation, Total Cost Ownership, Unix File System

1. INTRODUCTION

Nowadays, increasing the demands and importance of business, computer & communications system by complex IT industries has increased the risk on the IT infrastructure for all the time and every times in around the globe. The real time operating system functions, control & audit is a primary method of protecting system resources along with business, resources & technology for all the time and every times. The system control is probably the most important aspect of RT security. The PC is inversely proportional to the Risk and mean while control is directly proportional to the QoS (S). The system control provides accountability for individuals who are accessing sensitive information on application, system software, server and network. We have to develop the CIA model for risk mitigation on real time Unix operating system based on available technology, business & resources (Thomas, 1998).

The real time operating system is a collection of hardware, software & application that manages system resources and provides common services for resources, program, application & users. The operating system is an essential component of the system software (shell, file & kernel) in computer system. The high level language (application programs) usually requires an operating system to function. The time-sharing operating systems schedule & reschedule tasks for efficient use of the internal utilities that may also include auditing system software for resource & cost allocation of

DOI: 10.4018/IJDCF.2017010104

processor and memory time, mass storage, printing and other resources (Das, 2009; Kai, 2008; O' Reilly,1995; Sun-Microsystem, 2002).

The Real time operating system is a multitasking, time sharing & distributed operating system that executing real-time applications. The real-time operating systems often use specialized scheduling algorithms so that they can achieve a deterministic nature of behavior. The main objective of real-time operating systems is their quick and predictable response to events. They have an event-driven or time-sharing design and often aspects of both. An event-driven system switches between tasks based on their priorities or external (resources) events while time-sharing operating systems switch tasks based on clock interrupts(Das, 2009; Kai, 2008; O' Reilly,1995; Sun-Microsystem, 2002).

There are many more system control available and applied on real time operating system to protect our valuable IT assets for external & internal hacker. The PDC-CIA model & Mechanism traditionally prevent the core components of RTOS (Julie, 2000). The processor & memory is the core components of any types operating system. The processors 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 (Das, 2009; Kai, 2008; O' Reilly,1995; Sun-Microsystem, 2002).

1.1. Architecture of the Real Time Operating System:

The real time operating System control is a step by step process of securely configuring a system to protect it against unauthorized access, mean while taking steps to make the system more reliable. Generally anything that is done in the name of system. Preventive control ensures the system is secure, reliable and high available for high IT culture. Operating system control is the process to address security weaknesses in operation systems by implementing the latest OS patches, hot fixes and updates and following procedures and policies to reduce attacks and system down time men while increase the throughput of the system. Preventive control of the operating systems is the first step towards safeguarding systems from intrusion. The 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(Bruce, 1996; Harish, 2002; Ron, 2002).

2. SYSTEM SECURITY

The Security is a process, not a result. It is a process which is difficult to adopt under normal conditions; the problem is compounded when it spans several multiple jobs and multiple application running simultaneously under complex based web infrastructure which using millions of users accessing the same piece of devices and information around the globe in a multiple location and multiple business & resources. All the system level security in the world is rendered useless by insecure web-applications. The converse is also true—programming best practices, such as always verifying user input, are useless when the code is running on a server which hasn't been properly system programmed. (Bruce, 1996; Harish, 2002; Ron, 2002; Stalling, 2006).

The security is the ability of a system to protect, detect & correct information and system resources with respect to confidentiality, integrity and availability (CIA). The scope of this second definition includes system resources, which include Memory, CPUs, disks and programs, in addition to system information.

2.1. Existing Information System Security Mechanism & Services

Computer security is frequently associated with three core areas, which can be conveniently summarized by IS security & Audit the acronym "CIA" as per ISACA standard. (Stalling, 2006)