International Journal of Digital Crime and Forensics
Volume 9 • Issue 1 • January-March 2017

Proposed Round Robin CIA Pattern on RTS for Risk Assessment

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

ABSTRACT

The preventive, detective and corrective control is well advanced automated control in order to attain the maximum objectives of preserving the CIA mechanism on RTS. The risk analysis is the process of identifying the risk on RTS to achieving business objectives and deciding the measure components of RTOS on optimizing the lowest level of risk. This proposed round robin mechanism is going to be implemented on RTOS and mean while providing actionable, accountable & measurable for individuals who are accessing sensitive information on multiple relation functions, operation and services (RFOS) on multiple resources of RTS. We have to develop the RRP for risk assessment on MIMD. This research work going to be applied into security pattern on the measure component of the system security as well as RTOS. Furthermore, this RRP optimize the cost, time & resources is supposed to optimize the system risks and maximize the performance of business, resource & technology all the time & every time.

KEYWORDS

Advance Encryption Standard, Confidentiality, Integrity and Authentication (CIA), Preventive Detective Corrective Control, Processor Memory Encryption, Real Time Operating System, Risk Mitigation, Round Robin Pattern

1. INTRODUCTION

The increased applications of business, technology, resources & communications system by IT industries has increased the risk of theft of proprietary information. The real time operating system control & audit is a primary method of protecting system resources (Processor, Memory & Encryption Key). The system control is probably the most important aspect of communications security and becoming increasingly important as basic building block for information security. The control is inversely proportional to the Risk & mean while control is directly proportional to the quality of standard(S) (Gupta, 2012). The control provides accountability for individuals who are accessing sensitive information on application, system software, server and network. We have to develop the anti-symmetric model for risk mitigation on large scale Unix operating system based on available product, business & resources (Das, 2009; O'Reilly, 1995; Kai, 2008; Sun-Microsystem, 2002; Tanenbaum,2010).

The real operating system (server system) in large scale has even greater responsibilities and powers for large scale business like web based and mobile computing. It is just like a traffic management system and makes sure that different programs and software packages the users and clients running at the same time do not interfere with each other. The operating system is also responsible for risk and security ensuring that unauthorized users do not access the system (Das, 2009; O'Reilly, 1995; Kai, 2008; Sun-Microsystem, 2002; Tanenbaum,2010).

DOI: 10.4018/IJDCF.2017010105

1.1. Information Security

To assess effectively the security needs of an organization to evaluate and choose various security products and policies, the authority is responsible for security needs some systematic way of defining the requirements for security and characterizing the approaches to satisfying those requirements. This is difficult enough in a centralized data processing environment; with the use of local and wide area networks, the problems are compounded. The OSI security architecture focuses on security attacks, mechanisms, and services. These can be defined briefly as Security attacks: any action that compromises the security of information owned by an organization. Security mechanism: A process that is designed to detect, prevent, or correct from any security attack. Security services: A processing or communication services that enhances the security of the data processing systems and the information transfer of an organization. The services are intended to encounter security attacks and they make use of one or more security mechanisms to provide the services (Ron, 2002; Stalling, 2006; Schneier, 1996)

1.2. Information Security on PDC

We have to prevent, detect & correct the operating system resources all the time (Data & Services). This PME model & mechanism protecting & providing high level data & services on any type of organization in around the clock (7 x 24 x 52). The graphical PME model maximizes the utilities of processor, memory & high utilization of encryption key at optimal cost. The processor, memory & encryption key always prevention, detection & correction at minimal cost with high availability of data & services as per business & resource requirement. Therefore, the stronger security on PME always depends on the PDC or verse versa.

The preventive, detective, corrective control and high availability (HA) preventing the data & services around the clock. The data & services are the measure components of the shell, file, memory, processor & kernel of the operating system. Therefore, the preventive control is very much essential for betterment of multi-tier IT infrastructure.

These additional elements don’t neatly integrate into a singular definition. From one perspective, the concepts of privacy, confidentiality, and security are quite distinct and possess different attributes. The privacy is a property of individuals; confidentiality is a property of data; and security is a property assigned to computer hardware and software systems & resources. There is some practical perspective, the concepts are inter woven. A system that does not maintain data confidentiality and individual privacy could be theoretically or even mathematically secure, but it probably wouldn’t be wise to deploy anywhere in the real world in around the globe (24 x 7 x 52) (Ron, 2002; Stalling, 2006; Schneier,1996)

1.3. Information Security Requirement on CIA

The Security is the ability of a system to protect, detect & correct information and system resources with respect to confidentiality, integrity and availability (CIA). Note that the scope of this second definition includes system resources, which include Memory, CPUs, disks and programs, in addition to system information (Ron, 2002; Stalling, 2006; Schneier, 1996)

C**onfidentiality:** Preserving authorized restrictions access and disclosure, including mean for protecting personal privacy and proprietary information. A loss of confidentiality is the unauthorized disclosure of information.

Integrity: Guarding against improper information modification or destruction, including ensuring information non-repudiation and authenticity. A loss of integrity is the unauthorized modification or destruction of information.

Availability: Ensuring timely and reliable access to and use of information. A loss of availability is the disruption of access to or use of information or an information system.