Proposed Heuristics Model
Optimizing the Risk on RTS

PL Pradhan, Computer Science & Engineering, GITAS Gokul Grp, VZM, AP, India

ABSTRACT

The author’s objective is resolve the unstable, uncertainty problems of complex technology on right time and right place of ever where & every time in around the globe. It should be more accountable for performance, fault tolerance, throughput, bench marking and risk assessment on any application on any time. This work would optimize the technology & resource cost and maximizes the business (throughput) based on dynamic heuristics model over a multiple business and location. The subject and object can able to integrate, synchronize, communicate and optimize through RTOS and optimizing them step by step of heuristic function, that have been highlighted in proposed pattern for development and production purpose. This work has to define, design, development and deployment this mechanism to prevent the data & services on RTOS from external hackers, theft, uncertainty, un-order, un-setup and unsafe environment. Therefore, this proposed dynamic heuristics pattern for risk optimization on RTOS based on available technology, business & resources for anti-fragile technology.

KEYWORDS
Access Control Mechanism, Prevent Detect & Correct, Processor, Memory & File, Real Time Operating System, Relation Function Operation and Service, Risk Assessment

1. INTRODUCTION

Now a day increasing the use of clients, business and computer & communications system by IT industries has increased the risk of theft of proprietary information. The 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 computer security. The preventive control is inversely proportional to the Risk & mean while control is directly proportional to the quality of standard(S).

There are various kinds of controls mechanism available and implemented on operating system to protect our IT assets for external & internal hacker. The operating system consists of three main components such as, file, shell & kernel. The processor & memory is the core component of any type 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 (O’ Reilly, 1995) (see Figure 1).

The operating system (server system) is a large scale has even greater responsibilities and powers for large scale multiple business for multiple products & clients like web based and mobile computing. It is just like a traffic management system, it makes sure that different tools, application, programs and software packages, the users and clients running at the same time do not interfere with each other (Coriolis,2002; Kai, 2008; Stalling, 2006).
The multi programming, time shearing, parallel programming is solving our objective in right time and right way over a multiple Relation, Function, Operation & Services on heterogeneous complex infrastructure. The complex operating system is also responsible for risk and security ensuring that unauthorized users do not access the system (Kai, 2008).

All major computer platforms (hardware and software) require and sometimes include an operating system. HP_UX, Sun solaria, AIX, LINUX, WINDOW, NT, WIN2000, VME, OS/400, z/OS and VMware all examples of large scale operating systems.

1.1. Internal Structure of the Operating System

We have to prevent, detect and correct these internal components of RTOS (O’ Reilly, 1995) (Figure 2).

The machine consists of millions of chips, each capable of testing a million keys per second, such machine could be test up to 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 depends on Memory, Control, Arithmetic unit, Processor etc. to perform the functionality of the operating system. The processor & instruction level parallelism (SISD, SIMD, MISD, MIMD), Memory and Encryption key are the major role to optimize the risk on multi-tire high end computing. The operating system control is the process to address security weaknesses in operation systems by implementing the encryption key, latest OS patches, hot fixes, updates and the procedures and policies to reduce system attacks and down time, meanwhile increase the throughput of the system (Schneier, 1996).

The preventive control provides accountability for individuals who are accessing sensitive information on application, system & resources. This accountability is accomplished through access control mechanisms (UFS ACM) that require identification, authentication & authorization through the audit functions. These controls must be in accordance with and accurately represent the organization’s security policy. The assurance procedures ensure that the control mechanisms correctly create, manage, measure and control (CMMC) the security policy for the entire life cycle of an
19 more pages are available in the full version of this document, which may be purchased using the "Add to Cart" button on the product's webpage:

www.igi-global.com/article/proposed-heuristics-model-optimizing-the-risk-on-rts/176381?camid=4v1


Recommend this product to your librarian:

www.igi-global.com/e-resources/library-recommendation/?id=2

Related Content

What Issues of Literary Analysis Can Differential Equations Clarify?
www.igi-global.com/article/what-issues-of-literary-analysis-can-differential-equations-clarify/136069?camid=4v1a

E-Waste Recycling System in Closed Loop Supply Chain
www.igi-global.com/article/e-waste-recycling-system-in-closed-loop-supply-chain/202400?camid=4v1a

Designing Optimal Aviation Baggage Screening Strategies Using Evolutionary Algorithms
www.igi-global.com/article/designing-optimal-aviation-baggage-screening/75822?camid=4v1a