An Unordered ACM MODEL
Optimizing the Risk on RTOS:
ACM on RTS

Padma Pradhan, Gokul College of Engineering, Bobbili, VZM, AP, India & Central Institute of Technology, New Raipur, India

ABSTRACT

In the recent computing age, there are frequent change of climate on business, resources and technology to co-op with the sophisticated society in around the globe. At the same time increasing the uncertainty, un order, un safe and un setup due to hacker and down time of communication system is a great obstacle on one’s day to day business. The author’s objective is to resolve these uncertainty problems to develop the un order ACM to optimize the resources and technology and maximize the business, quality of services for all the time and every time which is applicable to pervasive and ubiquitous technology. The relation, function, operation and services is the vital role for all aspect of multiples business and technologies in around the cloud services. Meanwhile, it will be more accountable for performance, fault tolerance, throughput, benchmarking and risk optimization on any web services for all the time. One has to make more simplification, normalization, unification by applying un order ACM mechanism based on distributed object oriented system on multi-dimensional work culture.

Keywords: Access Control Mechanism (ACM), Business Resource Technology (BRT), Distributed Object Oriented System (DOOS), Prevent Detect Correct (PDC), Processor Memory File Systems, Real Time Operating System (RTOS), Relation Function Operation and Services (RFOS)

1. INTRODUCTION

The preventive control ACM model provides accountability for individuals who are accessing sensitive information on application, system software, server and network. We have to develop the multi-dimensional un order ACM model for risk mitigation on large scale UNIX real time operating system based on available technology, business and resources. We have to prevent our data and service from public resources and unauthorized user over a complex parallel & distributed operating system (Schneier, 1996; Weber, 2002). Now a day, increasing the complex business, applications, client, users, and resources over a heterogeneous business domain of the multiple location of WAN, LAN, IT Infrastructure, computer & communications system by IT industries has increased the uncertainty, un order, risk of theft to proprietary information. The

DOI: 10.4018/IJAPUC.2015100104
operating system control & audit is a primary method of protecting system resources (Processor, Memory, Kernel & File system).

1.1. Real Time Operating System

The most fundamental system program is the operating system, whose job is to control all the resources of the computer and provide a base upon which is the application program can be written. The concept of the operating system as primarily providing its users with a convenient interface is a top-down view. The modern computer system consists of professors, memories, times, firmware, disk, network interfaces, printer and associates with a wide variety of other devices. When a computer or a network has multiple users, the need for managing and protecting the memory, I/O devices and other resources is even greater, since the users might otherwise interface with one another. In addition, users often need to share not only hardware, but information (files, databases, etc.) as well. In short, this view of the operating system holds that its primary task is to keep track of who is using which resources, to grant resource requests, to account for usage, and to mediate conflicting requests from different programs and users (Tanenbaum, 2010). The resource management including multiplexing (sharing), time sharing resources in two ways: in time and in space. When resource is time multiplexed, different programs or users take turns using it. First one of them gets to use the resources, then another, and so on. To determining how the resource is time multiplexed – who goes next and for how long- is the task of the RTOS (Tanenbaum. (2010).

2. ATTRIBUTE-BASED ACCESS CONTROL (RWX)

The rights (RWX) and permissions are implemented differently in systems based on discretionary access control (DAC) and mandatory access control (MAC). In any ACM, the entities that can perform actions on the system are called subjects, and the entities representing resources to which access may need to be controlled are called objects (Access Control Matrix: data collection). The subjects and objects should both be considered as software entities, rather than as human users: any human user can only have an effect on the system via the software entities that they control. The authorization involves the act of defining access-rights for subjects. The authorization policy specifies the operations that subjects are allowed to execute within a system. The most modern operating systems implement authorization policies as formal sets of permissions that are variations or extensions of three basic types of access: (RWX).

- **Read (R):** The subject can (R), Read file contents, List directory contents
- **Write (W):** The subject can change (update) the contents of a file or directory with the following tasks: Update (Add Update Delete Rename)
- **Execute (X):** If the file is a program, the subject can cause the program to be run. (In Unix-style systems, the “execute” permission doubles as a traverse directory permission when granted for a directory.)

2.2. Access Control List and Limitations

The ACL is an example of a policy concept that is frequently implemented directly or as an approximation in real time operating systems. An ACL associates the permitted operation to an object and specifies all the subjects that can access the object, along with their rights or role to the object. That is, each entry in the list is a pair (subject, set of rights or role). From another
Privacy Control Requirements for Context-Aware Mobile Services

Effortless Data Capture for Ambient E-Services with Digital Pen and Paper Technology

The Applications of Automata in Game Theory
Sally Almanasra, Khaled Suwais and Muhammad Rafie (2013). *Intelligent Technologies and Techniques for Pervasive Computing* (pp. 204-217). www.igi-global.com/chapter/applications-automata-game-theory/76789?camid=4v1a