TELKOMNIKA Indonesian Journal of Electrical Engineering
Vol. 13, No. 2, February 2015, pp. 387 ~ 398
DOI: 10.11591/telkomnika.v13i2.7059

Dynamic RWX ACM Model Optimizing the Risk on Real Time Unix File System

P. K. Patra, P. L. Pradhan*
Dept. of CSE Central Institute of Technology, CSVTU, Raipur, CG, India
*Corresponding author, e-mail: citrprcs@rediffmail.com.

Abstract

The preventive control is one of the well advance controls for recent security for protection of data and services from the uncertainty. Because, increasing the importance of business, communication technologies and growing the external risk is a very common phenomenon now-a-days. The system security risks put forward to the management focus on IT infrastructure (OS). The top management has to decide whether to accept expected losses or to invest into technical security mechanisms in order to minimize the frequency of attacks, thefts as well as uncertainty. This work contributes to the development of an optimization model that aims to determine the optimal cost to be invested into security mechanisms deciding on the measure component of UFS attribute. Our model should be design in such way, the Read, Write & Execute automatically Protected, Detected and Corrected on RTOS. We have to optimize the system attacks and down time by implementing RWX ACM mechanism based on semi-group structure, mean while improving the throughput of the Business, Resources & Technology.

Keyword: *read write execute, Unix file system, access control mechanism, preventive detect corrective control, risk mitigation, real time operating system*

1. Introduction

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 processor and memory time, mass storage, printing and other resources [4-5].

There are various kinds of preventive control available and implemented on operating system to protect our IT assets for external & internal hacker. The PDC model & Mechanism traditionally prevent the core components of OS. The processor & memory is the core component of any type's operating system. The processor and kernel is fully functional dependency on each others, 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 [6-7].

Architecture of the Operating System:

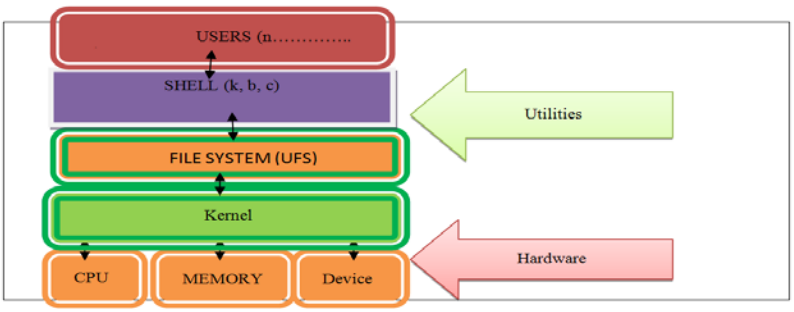


Figure 1. Internal Structure of RTOS

Received November 19, 2014; Revised January 5, 2015; Accepted January 23, 2015

The 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 required management procedures and policies are apply 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 [8-10].

2. Existing Control for the Risk Optimization

2.1. Preventive Controls [6-7], [10]

Preventive controls are implemented to stop the loss related to a risk from occurring when the risk situation presents itself, the preventive control kicks in and prevent the loss. Preventive techniques are the most complete form of stop loss control, because the loss is prevented by their nature. There are costs associated with preventive control that must be considered to get the full picture of the impact to the business. Prevention can mean the continuous close examination of each case, performing on analysis for the risk condition and stopping the risk whenever it is identified. This can be more expensive way to control than simply enabling the process to perform, identifying errant exceptions after they have occurred and taking them out of the process stream for corrective action in due course of time. While attempting to prevent errors whenever it is cost effective to do so, many production lines in the manufacturing sector also use detective technique to weed out errors, which is a more cost effective way of dealing with all of the possible permutations of error conditions that may exist in the process. The alternative of building preventative controls for each scenario would be cost prohibitive. The monitoring & management of the preventive controls also will need to be considered when determining what is best for the business.

2.2. Detective Controls [6-7], [10]

Detective controls are used in situations where it is more important to understand that some things have happened that it was to prevent from happening. In some cases, a detective control will ensure that a desirable event did indeed occur, providing feedback that the process is working as intended. Evaluation of the detective controls require proving that the detection occurs with a high degree of accuracy and reliability. When it is important to detect that an action has occurred, it will be equally important to rely on the control to not miss any valid occurrences where that detection should be taking place and to flag only those valid occurrences of predefined interest. To assess these controls, we will need to understand the trigger event and the mechanism used to identify it. The risks associated with detective control are the risk of not knowing a situation or event has occurred .If this failure to detect happens regularly, the control cannot be assessed as defective. When evaluating the cost-benefit for this control type, we must review what happens to the process if the events or situation is not detected and then assess the costs of this scenario against the cost of developing, implementing and maintaining the control. All system based logs automated generate on the development & production server.

2.3. Corrective Controls [6-7], [10]

A corrective control fixes errant situations or events as they are identified. It assumes some amount of detection is inherent in its mission of fixing out-of-bonds conditions. These controls are useful when simple corrections are easily found and fixed a process without lot of risk and complexity. The risk of not finding and fixing these items must be considered when assessing the total cost and benefit of such a control. It will need to be determined that corrective actions are possible and performed accurately to the satisfaction of the process in order to draw conclusions that these kinds of controls are effective. Determining what is acceptable in terms of corrective actions will be part of this process. Those situations that are not caught and fixed that do not require attention will need to be identified and examined for

false positive and false negative implications. Comparing this control to one that prevented the need for correction in the first place may be valid assessment when evaluating whether the right kinds of controls are employed to mitigate risk in a process. The cost to fix along with cost to identified or cost to prevent all will now need to be part of the cost benefit analysis. The PC, DC, CC & High Availability are a great services to data & services all the time in around the globe.

Figure 2. PDC Preventing Data & Services

3. Data Collection Based on Existing Control (RTOS DATA)

There are number of preventive control methods design and developed as per requirement of the secure computing to achieve the desired level of organization objective. There are few methods developed based on UNIX server and system programming. The preventive control is inversely proportional to the Risk [4-5], [8-9].

Table 1. Sample of RTOS UFS Data Collection

SN	SYSTEM FILES	ACTION PLAN	REMARKS
1	/etc/system	Can be update the kernel & n-bit processor	**Can be improve the system performance KERNEL**
2	/etc/hosts	Develop the scripts: allow/disallow as per policy, chimed 000= /etc/nnn-mark disallow	**Preventative control [H, M, L]**
3	/etc/services	Disable the third parties services. Remove the ftp, http, telnet, port no, printer, IP services. Those services are not required.	**Can be improve the system security preventative control [H, M, L] Can be improve the system security**
4	/use/bin/rash, etc/pam.conf	Disable all remote services: chmod 000 /usr/bin/rsh, rksh, rcp, ipcs, ruser, rlogin, uptime.	**Preventative control SHELL**
5	/vary/dam/message	Date & time stamp (DC: event mgmt)	**Internal audit purpose Detective control**
6	/etc/rc.conf script	Run level script Run level script have to develop as per requirement. /etc/init.conf,rc2.d example: httpd_flags="NO"	**preventative control [H, M, L]**
7	/etc/init.conf	OS services, run level	**Preventative control**
8	**etc/ssh/sshd_config CKM file system Automated Control**	**Cryptography enable through ssh implementation AES: 256 bits chipper aes256-chr.ssh-key gen -b 1024 -f /etc/ssh_host_key -n '' chmod - - - /etc/ssh/ssh_config**	**preventative control n=1024, 2048, 4096 chimed r w x (i. e. 4 2 1) – blank is nothing [H, M, L]**

4. Existing in UFS Problem

As per above data collection, the automated control (PDC) is not available of the recent RTOS. There is great risk on the corrective action & reaction on file system, application & resources on this current security age. The multiple Relation, Function, Operation and Services is happening over a multiple clients, business, application and resources on a complex heterogeneous IT infrastructure for all the time & every time. Therefore, resource conflicts are the biggest issue over a complex network, platform and user application.

5. Proposed Dynamic RWX ACM Model for Risk Optimization

This paper contributes to the define and development of an optimal model that our objective to determine the minimal cost, quality & time to be invested into the risk assessment and management on the measure components of Unix file system attributes (Read, Write & Execute). That's why we are calling as it RWX model for system based risk analysis. Furthermore, this mechanism optimize the cost, time & resources is supposed to reduce the system attack, down time and vulnerabilities. We have to optimize the technology & resource cost and maximizes the business (throughput). We have to protect our data and services to over a multiple business, resources & technology on all the time (24 x 7 x 52).

Figure 3. Technology, Business & Resources Preventing Data & Services

We have to implement our idea based on the SEMIGROUP (isomorphism graph) theory, how the operating system optimizing as per our business requirement. Our objective is that maximize our business (throughput) and minimizes our technology & resources cost and time.

5.1. Define

We have to design & develop this optimization method based on Semi group. Like a semi group is a set with a binary operation but there is no requirement for an inverse function or an identity elements. In order to be a semi group, a set of objects plus an operation, must obey the following axioms. A semi group is important when we are looking at cosets.For all r, w, x € S, the equation (r. w) . x = r . (w. x) holds. For all p, d, c € S, the equation (p . d) . c = p . (d . c) holds [1-3].

PDC:

Associative Low: (P U D) U C = P U (D U C), (P ∩ D) ∩ C = P ∩ (D ∩ C)

Distributive Low: P U (D ∩ C) = (P U D) ∩ (P U C), P ∩ (D U C) = (P ∩ D) U (P ∩ C)

RWX:

Associative Low: (R U W) U X = R U (W U X) , (R ∩ W) ∩ X = R ∩ (W ∩ X)

Distributive Low: R U (W ∩ X) = (R U W) ∩ (R U X), R ∩ (W U X) = (R ∩ W) U (R ∩ X)

Let us consider R={P, D, C} & M={R, W, X). It is easy to verify that the following operation tables give Semi Group Structures for R & M respectively.

We have to maintain the sequence as follows: 1st we have take care of the Prevent, 2nd Detect, then Correct. These three parameters should be satisfied according to our data & services for better performance & high security.

The High Availability is Risk Mitigation. [K=PC+DC+CC]. We can optimize the risk factor by help of these six elements. All these sixe elements depend on each others. Availabilities is the main concern among the all of them.

As per business & resource management the PDC & RWX Model and Mechanism are very well suited for multiple RFOS & Technology in around the globe on 24 x 7 x 52 pattern.

5.2. Design

This isomorphism sets of elements are equally satisfying to the transitive, union of, associative, distributive & composition and Sum of all for the Risk Mitigation. We are proposing this idea based on directed graph theory as follows. We have to design and develop the security & reliability policy for our complex IT infrastructure. We have to find out the best solution to applying step by step of algorithm, method, model & mechanism. We have to draw two identical directed graph one for PDC & another for RWX. The both of these two directed graph working for high availability on 24 x 7 x 52 pattern in around the security world as follows [1-3].

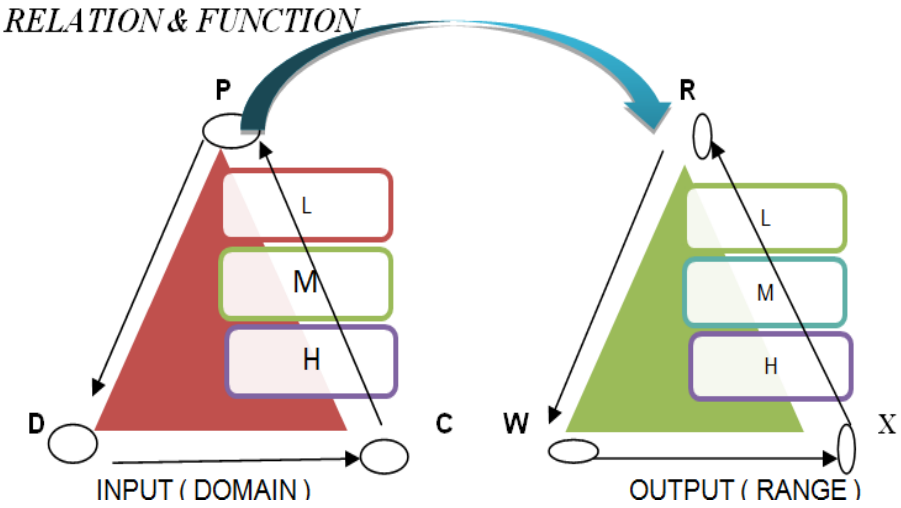


Figure 4. (a) [PDC] Figure 4. (b) [RWX]

We can find the composition of the table as follow:

Table 2. (a) [PDCA]

X	P	C	D	A
P	P	C	D	A
C	C	P	A	D
D	D	A	P	C
A	A	D	C	P

Table 2. (b) [RWXA]

X	R	W	X	H
R	R	W	X	H
W	W	R	H	X
X	X	H	R	W
H	H	X	W	R

Associative law: Multiplication is associative in G, since associative law holds in case of matrix multiplication: (PC) D = P (CD) Where A= Availability, H= High Availability. Let us onsider R={P,D,C} & M={R, W, X). It is easy to verify that the following operation table gives Semi Group Structures for R & M respectively. AN ISOMORPHISM GRAPH in Between M & R, f(p) = 1, f(d) = 6, f(c) = 8,f(a) = 3, f(c) = 5, f(i) = 2, f(a.t) = 4, f(h) =7.

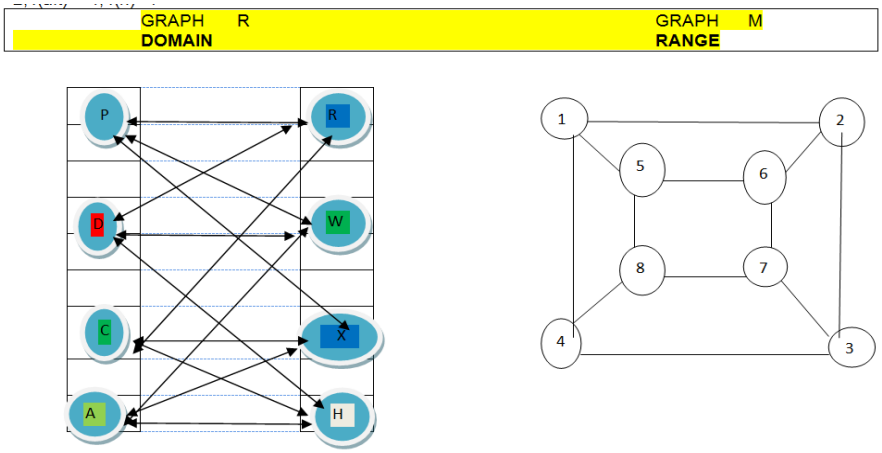
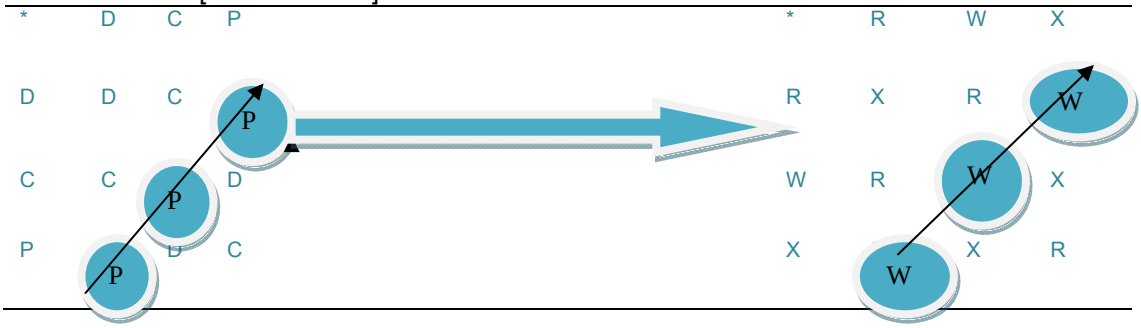


Figure 5(a) Figure 5(b)

5.3. Development (Function)

We have to move forward to finding alternate solution and algorithm for risk optimization on semi-group method. This scalable complex semi group method definitely will be solve our risk and security issue on complex real time system for multiple client application, business and resources available for multi- location on any time around the clock. We have to optimize the RTOS step by step as follows:

Table 3. [DPC ->RWX] Model-1.a Prevention on Write Access DCP Verses RWX

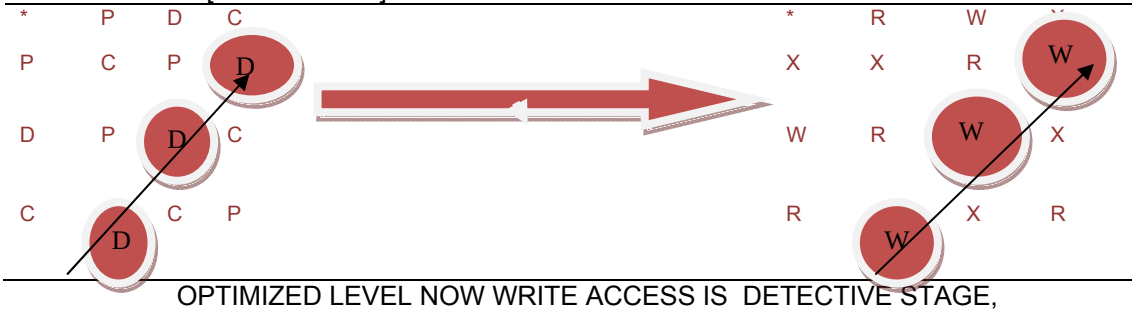


Now write access is preventive stage. Prevention is better than cure.

Diagonal view (P-P-P=W-W-W) BUSINESS OWNER et us consider that: f(D)=W, f(C)=R, f(P)=X.

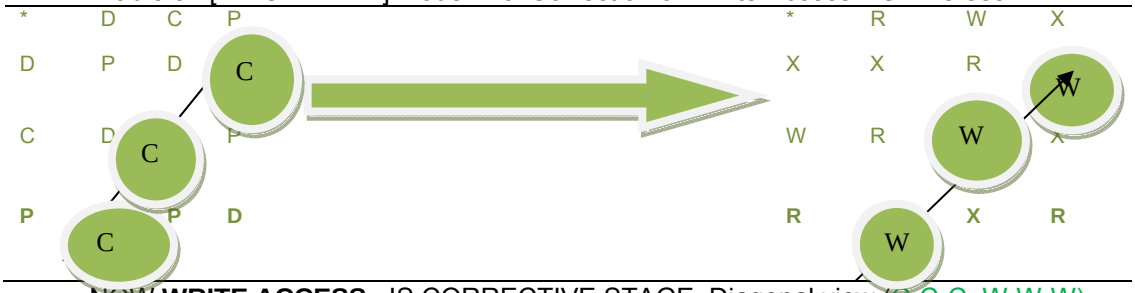
Now, replacing the function in R by their images and rearranging the tables, we obtain exactly the table for M. Thus R & M are Isomorphic. Therefore, this model is called“ SEMI-GROUP as well as ISOMORPHIC MODEL ON SYSTEM SECURITY FOR RISK OPTIMIZATION”. Then we can move forwards to the NEXT OPTIMIZED LEVEL as follows.

Table 4. [PDC ->RWX] Model-1.b Detection on Write Access PDC Verses RWX



OPTIMIZED LEVEL NOW WRITE ACCESS IS DETECTIVE STAGE,
Diagonal view (D-D-D=W-W-W) BUSINESS OWNER

Table 5. [DPC ->RWX] Model-1.c Correction on Write Access DCP Verses RWX



NOW **WRITE ACCESS** IS CORRECTIVE STAGE. Diagonal view (C-C-C=W-W-W)
BUSINESS OWNER

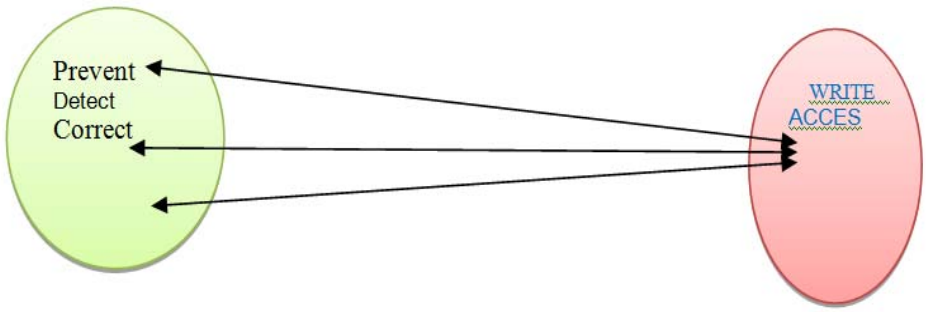
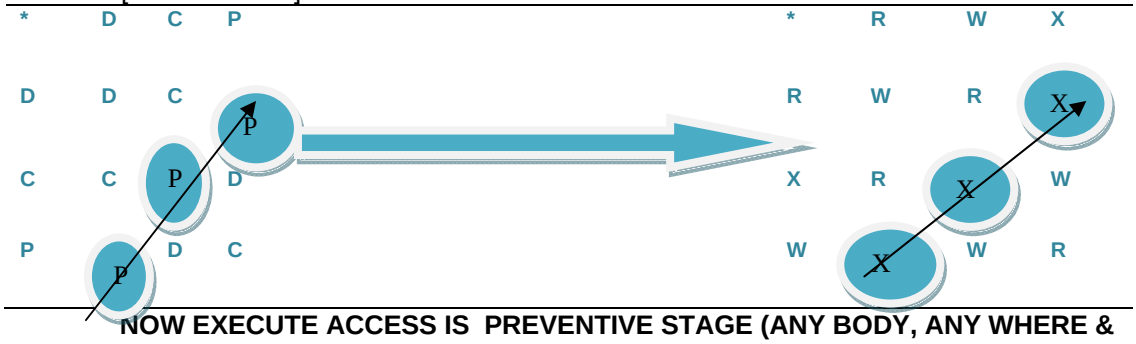


Figure 6. Write Activities

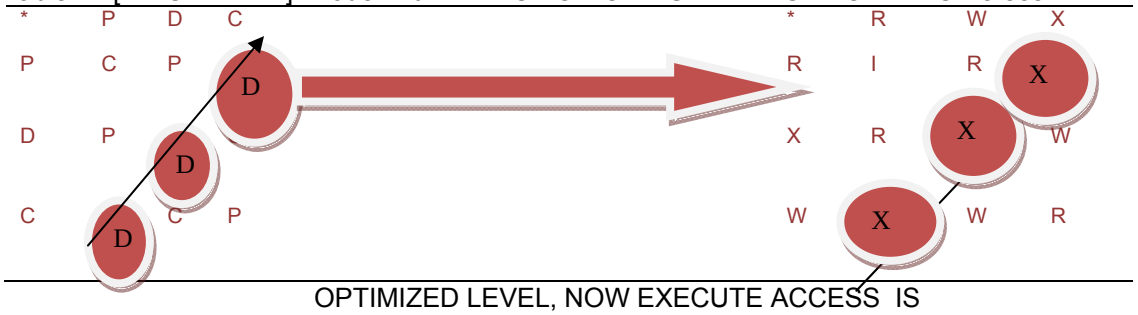
This graphical representation show that, WRITE **ACCESS** is prevented, detected and corrected automatically.

Table 6. [DCP ->RXW] Model 2.a PREVENTION ON EXECUTE ACCESS DCP Verses RXW



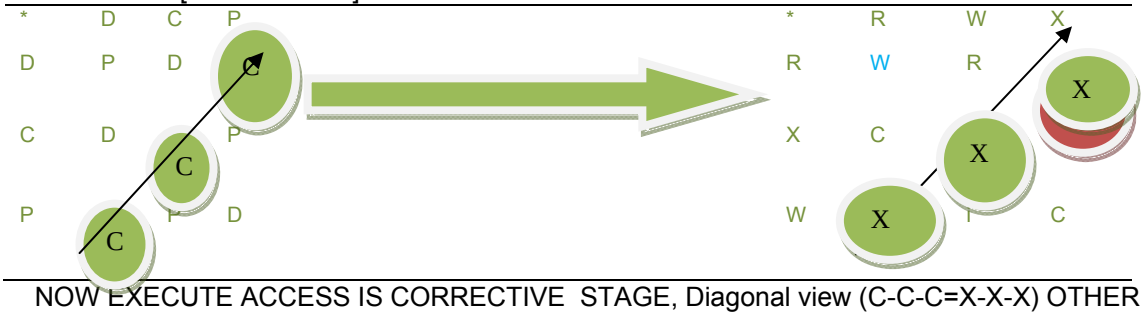
NOW EXECUTE ACCESS IS PREVENTIVE STAGE (ANY BODY, ANY WHERE & ANY TIME
PREVENTION IS BETTER THAN CURE. Diagonal view (P-P-P=X-X-X) OTHER.

Table 7. [PDC ->RXW] Model:2.b DETECTION ON AUTHENTICATION PDC Verses RXW



OPTIMIZED LEVEL, NOW EXECUTE ACCESS IS
DETECTIVE STAGE. Diagonal view (D-D-D=X-X-X) OTHER.

Table 8. [DCP ->RXW] Model: 2.c CORRECTION ON AILABILITY DCP verses RXW



NOW EXECUTE ACCESS IS CORRECTIVE STAGE, Diagonal view (C-C-C=X-X-X) OTHER

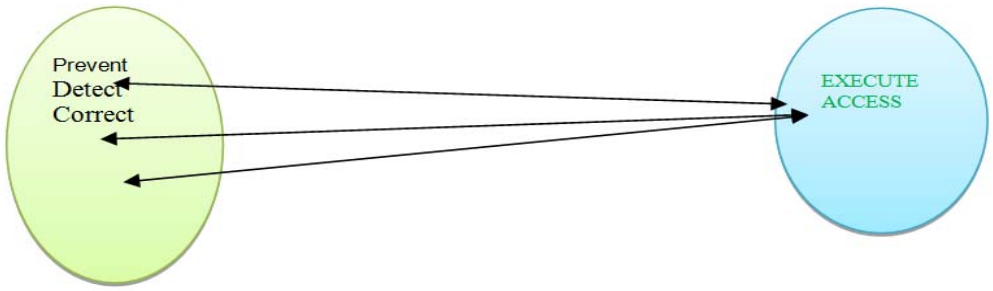
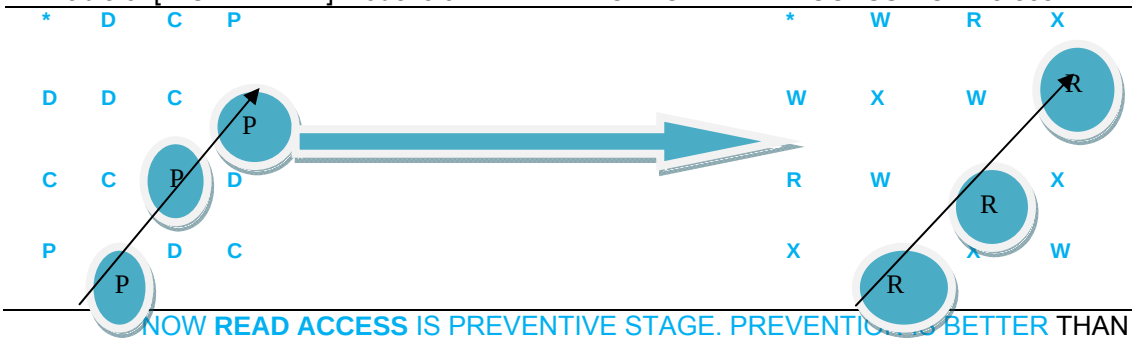


Figure 7. Execute Activities

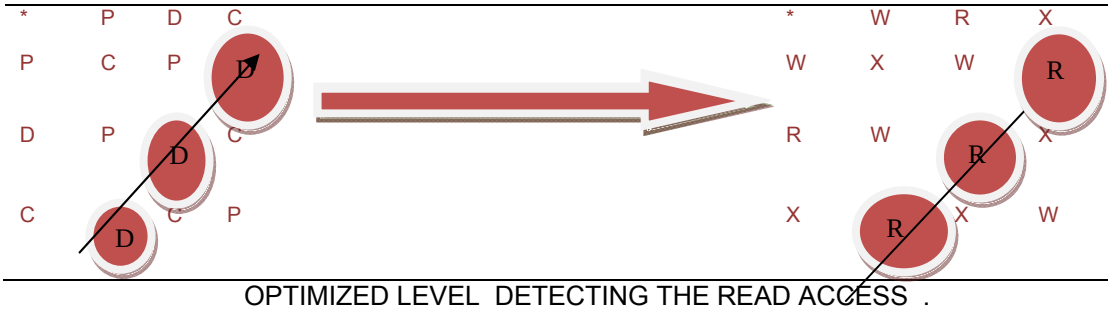
This graphical representation show that, **EXECUTE ACCESS** is prevented, detected and corrected on the objects in automated way.

Table 9. [DCP ->WRX] Model:3.a PREVENTION ON READ ACCESS DCP Verses WRX



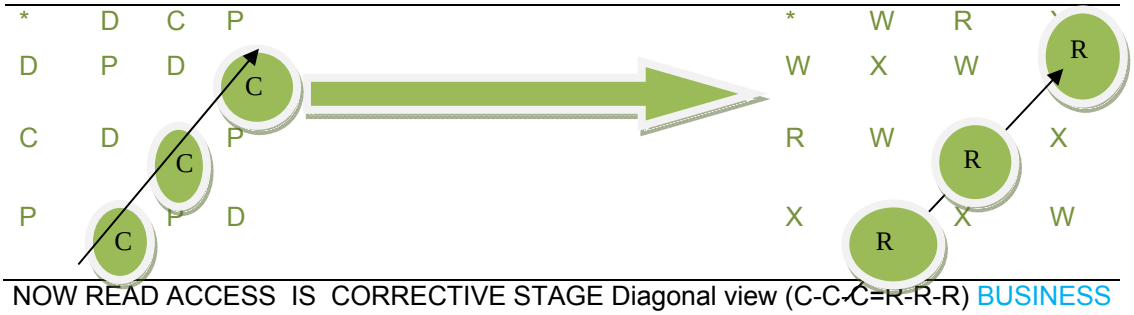
NOW **READ ACCESS** IS PREVENTIVE STAGE. PREVENTION IS BETTER THAN CURE.
Diagonal view (P-P-P=R-R-R) BUSINESS OWNER

Table 10. [PDC ->WRX] Model:3.b DETECTION MATRIX ON READ ACCES PDC Verses WRX



OPTIMIZED LEVEL DETECTING THE READ ACCESS .
Diagonal view (D-D-D=R-R-R) BUSINESS OWNER

Table 11. [DCP->WRX] Model: 3.c CORRECTION THE CONFIDENTIALITY DCP Verses WRX



NOW READ ACCESS IS CORRECTIVE STAGE Diagonal view (C-C-C=R-R-R) BUSINESS OWNER

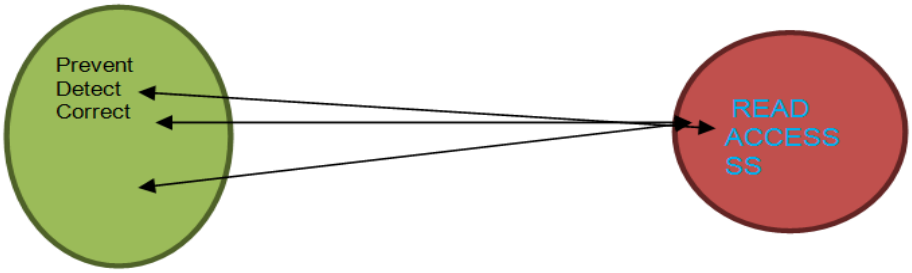


Figure 8. Read Activities

This graphical representation shows that, READ is prevented, detected and corrected automatically. This is the dynamic life cycle of PDC & RWX based on the semi-group, isomorphic & directed graph theory. When RWX optimization technique applied on OS, the space & time complexity of Processor, Memory and users details can be detected by OS system parameters is already defined in existing risk assessment method on file system (/var/adm/messages), then we can fix up the unix file system (UFS) as per availability of technology, resources and business requirement. In this way we can dynamically optimize our technology & business risk.

We can conclude that from the above optimization model the operating system components are the shell, file, processor, memory & encryption key have to take highest priorities of the Preventive, Detective and Corrective, action plan, which is shown in the model 1, 2 & 3 respectively. In this way, we can improve the performance & security of the high end READ, WRITE and EXECUTE attributes for the technology, business & resources. The preventive control will be facilitate and resolve the various issue when it spans several jobs and applications are running simultaneously under heterogeneous complex based web

infrastructure (B2B, B2C, P2P, G2G) in around the web world. These above optimization models will be very helpful for Instruction level parallelism for high end computing. We hope this theoretical and experimental idea will be very much help to the parallel computing environment to optimize the operating system software risk. We can improve our risk optimization model that, which will be help to the risk management on operating system.

5.4. Brief Summary of the Dynamic RWX ACM Model

Table 12. Life Cycle of PDC & RWX Operation

MODEL	STAGE	DESCRIPTION	ACTION PLAN
Model-1.a	1st Round: on Write Access	Diagonal view (P-P-P=W-W-W)	Preventive Control on Write Access Detective Control on Write Access
Model-1.b		Diagonal view (D-D-D=W-W-W)	Corrective control on Write Access
Model-1.c		Diagonal view (C-C-C=W-W-W)	
Model-2.a	2nd Round: Execute Access	Diagonal view (P-P-P-X-X-X)	Preventive Control on Execute Access Detective Control on Execute Access
Model-2.b		Diagonal view (D-D-D= X-X-X)	Corrective control on Execute Access
Model-2.c		Diagonal view (C-C-C= X-X-X)	
Model-3.a	3rd Round: Read Access	Diagonal view (P-P-P=R-R-R)	Preventive Control on Read Access Detective Control on Read Access Corrective
Model-3.b		Diagonal view(D-D-D=R-R-R))	Control on Read Access
Model-3.c		Diagonal view(C-C-C- R-R-R)	
Model-1.c	Automated Corrective Control	Diagonal view (C-C-C-W-W-W)	Corrective control on Write Access Corrective control on Executive Access
Model-2.c		Diagonal view (C-C-C-X-X-X)	Corrective control on Read Access
Model-3.c		Diagonal view(C-C-C-R-R-R)	

5.5. Deployment: (Test, Verification, Results & Services) Practical Implact Analysis on RWX ACM Model

We have to verify & validated the operating system integrity, high availability, reliability, scalability, reliability of Read, Write & Execute Access over a UFS on RTOS. We have to protect, Detect and Correct the UFS per business, resource requirement and availability of technology. We have to apply some review method on internal UNIX operating system on super user mode. This table(3) is the part of benchmarking, performance analysis and risk assessment of real time operating system over a complex web portal application on large scale RTOS.

Table 13. Verification of RTOS [8], [9]

SN	INPUT (Subject) How to do ?	DESCRIPTIONS ACTION PLAN What to do?	Risk Assessment OUTPUT (Object) What happen & When ??
01	/var/adm/message	System mesg (event mgmt) DC	Date & time stamp SECONDARY RISK ASSESSMENT
02	/var/adm/syslog	syslog system logs	Detective control, Accountability & Authentication
03	/var/adm/sulog	super user log	Detective control, Accountability & Authentication
04	/var/adm/loginlog	user login log	Detective control, Accountability & Authentication
05	etc/ssh/sshd_config	AES, CKM Key mgmt	Run the scripts: Preventive control

6. Results (Services) [Efficient Resource Management]

The subject and object can able to mapping, synchronize and optimize through real time operating system. This virtual programming utilities and application will be more measurable and accountable for performance, fault tolerance, throughput, bench marking and risk assessment on any application over a complex IT infrastructure. How is behaving the (MIMD) UNIX server along with its sub components, when we are running on the different processor, memory & encryption key on the same programming & application or reverse way? The iostat, vmstat and pmstat commands will be give the full detail output statistics of processor and memory on real time operating system. The primary risk can be analysis on right time and right way. The /var/adm/message scripts will be give the output statistics of hardware and software problem of real time event management system including date and time stamp on unix machine. We can verify and validate the access control mechanism (ACM) by help of these scripts, which is already mentioned on table 13. (/var/adm/sulog, syslog, login log).

a) How is the system behaving, when millions of users accessing the same piece of data & information in around the clock (high availability, scalability and reliability). In this ways, we can improve the ACM, performance, benchmarking, fault tolerance and risk assessment at a time to utilizing the above scripts and virtualization concept, which is help to our business, technology and society in around the globe.
b) Maximize the protection, detection & correction (PDC) at optimal cost and time.
c) Maximize the performance, reliability, high availability at optimal cost (TQM).
d) Maximum utilization of resources at minimal cost at right time in right way.

7. Conclusion

This dynamic RWX is a one of the best preventive control, which is providing accountability for individuals who are accessing sensitive information on shell, file system & kernel. The accountabilities is accomplished through access control mechanisms (ACM) that require identification, authentication, authorization, accountability, non-repudiation, availability, reliability & integrity through the audit function on various file system. The large scale optimization can be done in this way to protect, detect & correct the RWX model for efficient resource management in a dynamic way of the web application over a RTOS. A sound information security policy identifies prevention, detection, and response measures on various components of system security. This above model provides more details on risk assessment tools and practices that may be used to improve information security programs. The preventive measures may include regularly using vulnerability assessment tools and conducting periodic penetration analyses. Intrusion detection tools can be effective in detecting potential intrusions or system misuse. Our research & development should also develop a response. By reading through this paper and utilizing the model & mechanism for preventive, detective and corrective action plan of the organization is a great benefits. The security programmer & administrator now have a base knowledge of security, server hardening, intrusion detection, auditing and security tools. This knowledge can be directly applied to their servers and many vulnerable holes will now be filled. Therefore, it is critical that every unix security-minded programmer maintains their knowledge of security by researching and referring to the Internet resources that have been mentioned in survey data collection. If there is ever a question about updating & implementation of any of the suggested features, refer to the OS server security manuals that were designated with the specified feature (all features have been research, design, developed & documented).

References

[1] Bernard, Kolman. *Discrete Mathematical Structures*. New Delhi, India: Person Education India (PHI). 2007.
[2] Edgar G. *Discrete Mathematics with Graph Theory*. New Delhi, India: Person India (PHI). 2007.
[3] Joe L Matt. *Discrete Mathematics for Scientist and Mathematician*. New Delhi, India: Person Education India (PHI). 2008.
[4] Hwang, Kai. *Advance Computer Architecture*. New Delhi, India: Tata McGraw Hill. 2008
[5] O' Reilly. *Essential of System Administration*. O' Reilly Media: USA. 1995.
[6] Shon, Harrish. *CISSP Exam study guide*, New Delhi, India: Dreamtech. 2002
[7] Shon, Harrish. *Security Management Practices*. New Delhi, India : Wiley Publishing Inc. 2002

[8] Sumitabh Das. *UNIX System V UNIX Concept & Application*. Delhi, India: Tata McGraw Hill.2009.
[9] Sun-Microsystem. *UNIX Sun Solaris system administration*. USA. 2002.
[10] Weber, Ron. *Information System Control & Audit.* New Delhi, India: Person Education India (PHI). 2002.