A Literature Survey on Risk Assessment for Unix Operating System:
Risk Assessment on UNIX OS

Padma Lochan Pradhan, Sritech New Raipur, Raipur, India

https://orcid.org/0000-0003-2284-6819

ABSTRACT

This proposed literature survey provides basic data regarding the first step of risk identification and analysis to achieve a secured infrastructure. The demand and risk are two parts of the same coin. The demand is directly proportional to the risk, but preventive control is inversely proportional to risk. The necessity of preventive control in any organization has increased because of the changes in logic, structure, and the type of technology applied to services that generate risks. Finally, the business increases along with technology, which creates risks and spreads over its infrastructure. We have to focus on protecting, detecting, correcting, verifying and validating the Unix file system. This survey article proposes and resolves the Unix file system by applying a hardening, re-configuration and access control mechanism up to the highest level of preventive control.

KEYWORDS

Access Control Mechanism, Defective and Corrective Control, High Medium and Low, Preventive, Real-Time Operating System, Real-Time Unix Operating System, Unix File System

1. INTRODUCTION

Every organization grows with the demand of business, technology, and resources. Now a day, Information security and services is a top priority for each and every organization. The risk analysis is the most important and helpful scenario to any Information Technology organization (Devis, 2011). The risk consists of a set of the possible threat, that may be hardware, software and human error, failure, defect, uncertainty, unordered, unsafe and the probabilities of them occur at any time. It is defined as the prevention, detection, verification, validation, correction, and recovery from undesirable destruction, modification, the disclosure of information and resources (Ron, 2002). The information security is a set of process, procedures, policy, personnel, business, and technology applied to the characteristics of the assets (technology), that creates risk (Charles, Shari, & Deven, 2007).

The necessity of information security in any organization has increased because of the changes in design, logic, structure, programming, coding, and type of technology applied into services that create risk, spread over the business, technology, and resources (Ron, 2002). We are more emphasized

on protecting, detecting, correcting, verification and validation of the Unix File System. We are proposing and resolving the Unix file system by applying hardening, re-configuration and access control mechanism. We are focused and taking care of UFS ACM, scripting and system programming on Unix operating system all the time and every time for web services, ubiquitous, pervasive and self-autonomy system (Stalling, 2006, 2009; Sumitabh, 2009; Sun-Microsystem, 2002).

2. GOAL OF LITERATURE SURVEY

There is a thorough review of the literature was conducted with the primary goal of determining the risk assessment on the Unix operating system for IT infrastructure on the large electronic workplace. This research has been conducted on real-time Unix file systems applying hardening, re-configuration, access control mechanism and system programming as per the demand of complex Business, Technology & Resources (Dario, 2009; Denis, 2003; Debi, 2008).

Now a day, Information security and services is the most important and well advanced to any Information Technology organization. The literature defines information security as a set of process, procedures, policy, personnel, business and technology charged with property on organization into assets (technology) (Dieter, 2008). It is also can be defined as the prevention, detection, correction, and recovery from unauthorized or undesirable destruction, modification, disclosure or use of information and resources (Ron, 2002). The necessity of information security in any organization has increased because of the enormous changes in structure and type of information technology applied to information creates risks. Finally, the business increases along with technology, which generates risks as well as vulnerabilities (Schofield, 2005).

The risk of assets is identified in terms of non-identity, integrity, non-repudiation, high availability, authentication, accountability, scalability, and reliability. The critical of each and every risk as rated accuracy of potential impact likelihood of occurrences (Forouzan, 2008; Stalling, 2006).

Therefore, the risk consists of the set of a possible threat, that may be hardware, software and human error, failure, defect uncertainty, unorder, unsafe and the probability of them occurring on any time. The exposure of an asset to a particular threat generally referred to as the vulnerability of assets (Susan & Davis, 2003).

The risk is happening, in the course of system operation, maintenance and services. As a result of internal strategies, system processes, policy, procedures, and information used by the organization (Stalling, 2006).

Risk analysis is the study of potential threats, vulnerabilities, and impacts in order to identify and assess the extent and potential severity (Thomas Finne, 2000) of the risks to which the organization and its assets are exposed (Ron, 2002). The risk assessment is closely associated with risk analysis.

The risk management (identifying, analysis and mitigation) is a process to optimizing the risks to acceptable levels (HTML) by the application of various control strategies of prevention, detection, correction, verification and validation (Ron, 20020). The risk analysis, assessment, and management are the integrated process for business, technology, and resources for all the time and every time. Assessing the risks and needs of business, resources and technology have become standard practice in many more IT organization. The understanding of the concepts of risk and need is essential factors for important of decisions involving business, resources, and technology. The risk is created due to a dynamic decision over a business, and technology. The risk is propagated over vendor, order, and customers across the all related sub-systems (Turban, Aronson, Liang, & Shard, 2009).

3. REAL TIME UNIX OPERATING SYSTEM

In a large scale real-time operating system, the multitasking, multiuser, time-sharing operating system where multiple programs can be running at the same time, the operating system determines which applications should run in what order and how much time should be allowed for each application

Related Content

Conversational System, Intelligent Virtual Assistant (IVA) Named DIVA Using Raspberry Pi
Divij Bajajand Dhanya Pramod (2020). *International Journal of Security and Privacy in Pervasive Computing (pp. 38-52).*
www.irma-international.org/article/conversational-system-intelligent-virtual-assistant-iva-named-diva-using-raspberry-pi/264449

CADEAU: Supporting Autonomic and User-Controlled Application Composition in Ubiquitous Environments
Oleg Davidyuk, Iván Sánchez Milaraand Jukka Riekki (2011). *Pervasive Computing and Communications Design and Deployment: Technologies, Trends and Applications (pp. 74-102).*
www.irma-international.org/chapter/cadeau-supporting-autonomic-user-controlled/53785

Cooperative Cache Replacement Policy for MANETs
Prashant Kumar, Naveen Chauhan, LK Awasthiand Narottam Chand (2014). *International Journal of Advanced Pervasive and Ubiquitous Computing (pp. 36-47).*
www.irma-international.org/article/cooperative-cache-replacement-policy-for-manets/116034

Research on Underground Personnel Positioning Method Based on PSO-GSA Optimization
Ye Liu, Tianze Li, Tao Gao, Yuhan Wangand JiaHui Chen (2016). *International Journal of Advanced Pervasive and Ubiquitous Computing (pp. 21-74).*
www.irma-international.org/article/research-on-underground-personnel-positioning-method-based-on-pso-gsa-optimization/179236

Opportunistic Detection Methods for Emotion-Aware Smartphone Applications
Igor Bisio, Alessandro Delfino, Fabio Lavagettoand Mario Marchese (2014). *Creating Personal, Social, and Urban Awareness through Pervasive Computing (pp. 53-85).*
www.irma-international.org/chapter/opportunistic-detection-methods-for-emotion-aware-smartphone-applications/88797