TCM: Transactional Completeness Measure based vulnerability analysis for Business Intelligence Support

S. Senthil Kumar[1], Dr.M.Prabakaran[2]
[1]Research Scholar, Department of Computer Science, Karpagam University, Tamil Nadu, India
[2]Assistant Professor, Department of Computer Science, Government Arts College, Tamil Nadu, India

Abstract: Real world business applications completely lie on the top of internet technology where the faces of user are unknown at most cases. The user may be a registered or trusted one; the behavior of them cannot be predicted. In any transactional platform the vulnerability arises depend on the security measures enforced in the underlying platform. To enhance the security measures and to support the business intelligence we propose a transactional completeness measures to gauge the genuiness of the transactions. The TCM is measured using the logs of the server and how the transactions started and the completeness status and etc… Based on the computed TCM a vulnerability measure will be computed to propose the vulnerability assessment report to the administering group.

Index Terms: Business intelligence, vulnerability, decision support

1. Introduction

In the organization the growing concern about potential costal risk associated with neural phenomena such as erosion and human activities along the cast have created increasing interest in costal risk assessment which a critical and essential part of any decision is making process. It present fundamental information for managing and ranking possible action and strategies within any integrated coastal zone management plan treating environmental and social and economical aspects. Estimating risk involves identifying Hazard the event produces risk target element at risk and Vulnerability of element at risk the degree of intrinsic susceptibility of the features. Daude risk assessment techniques require integrating a great amount of data from several sources to provide a coherent vision of potential risk regarding mentioned components. Moreover coastal regions are under authority of different organizations in local provincial and federal governments.

As the technology grows, there is an increased growth of vulnerabilities towards the business solutions. The web logs are the most important source for the analysis of vulnerabilities in order to provide a secure and reliable solution. Using web logs the business solution can analyze and understand the nature and pattern of vulnerabilities and how it focuses towards the intelligence. Also the web logs are most dominant source for the development of business using which the business people could make decisions.

Configuration is major important to any business system. Due to the reason that we will be able to predict what is the effect to the system, when they are most likely to occur and where is the most severe impact on the link. This is the basic information to form the road network vulnerability analysis. Then after that we need to identify the possible solutions to prevent recover from disturbances. We also have to mind about cost that will happen during the process due to the resource allocation or various actions required as well. For example, in planning development and maintenance of road network, the decision makers make their choice base on some key factors or criteria such as traffic volume, average speed and travel time, in terms of congestion and delay, and economic issues.

However the risk assessment process is not as straightforward as one might imagine. Dealing such analysis is the main challenge of decision makers who are involved in any step of plan by allowing fast synthesis fast summarizing easy comparisons and multi level querying for efficient decision making purposes. In this regard the main objective of this research is in to develop an integrated multidimensional tool to improve risk assessment and representation.

2. Background

The supporting factors and solutions for the business intelligence get new dimensions at all the times. We explore those dimensions with metrics of business intelligence here. A new vulnerability analysis method based on software oriented architecture for business processes is proposed in [1]. The method is focused towards vulnerability identification on SOA objects and works based on the predefined vulnerability pattern. According to the pattern provided the proposed method search for the SOA business process and generates alerts if any of the patterns gets matched.

Risk and vulnerability analysis of power systems including extraordinary events [2], proposes a framework which identifies threats based on events generated and structures. This method maintains event pattern and structures for variety of vulnerabilities. The probability of identifying the threat is lower because the frequency of event generation is low. The challenge of identifying vulnerable states and events are explored here.

Vulnerability analysis on power systems based on maximum-flow is presented in [7]. They compute a centrality measure and index which represent possible transmission capacity of the link selected. The traversal path for the communication is selected based on the centrality index which shows the channel capacity between a source and destination. The capacity of the link is evaluated using the maximum flow and minimum cut theorems.

Vulnerability Analysis of Wide Area Measurement System in the Smart Grid [9], performs a comprehensive analysis of security issues with a wide area measurement system is presented and the research efforts required to be taken are identified. Moreover, the effect of communication failure on a PMU installed system has been presented using integer linear programming.

Vulnerability analysis for cost effective resource allocation of power systems is discussed, where the resources are allocated based on the policies enforced. In [10], a power allocation scheme is presented which uses reliability, RT and flexibility of rules. A quantitative analysis is performed about reliability for power distribution systems using possible states of the power systems.

A Framework of Business Intelligence-Driven Data Mining for E-business [11], has been proposed which combines knowledge and data driven approaches. The vulnerability of the transaction can be computed using both knowledge which represents the proactive patterns and also with the data driven which show the data or reactive information.

A Distributed Approach to Business Intelligence Systems Synchronization [12], presents set of network services for distributed synchronization of Business Intelligence. The solution is focused towards dynamic deployment of services of business intelligence in distributed environment which could be accessed through internet. The proposed work beats the challenge of synchronization of architecture where business intelligence applications can be installed and moved over different servers of distributed environment.

We propose a vulnerability analysis framework based on completeness measure of transaction on any business solution.

3. Proposed Method

The proposed method has five different phase preprocessing, transition graph generation, Transactional complete score computation, vulnerability score computation, Intelligent result generation.

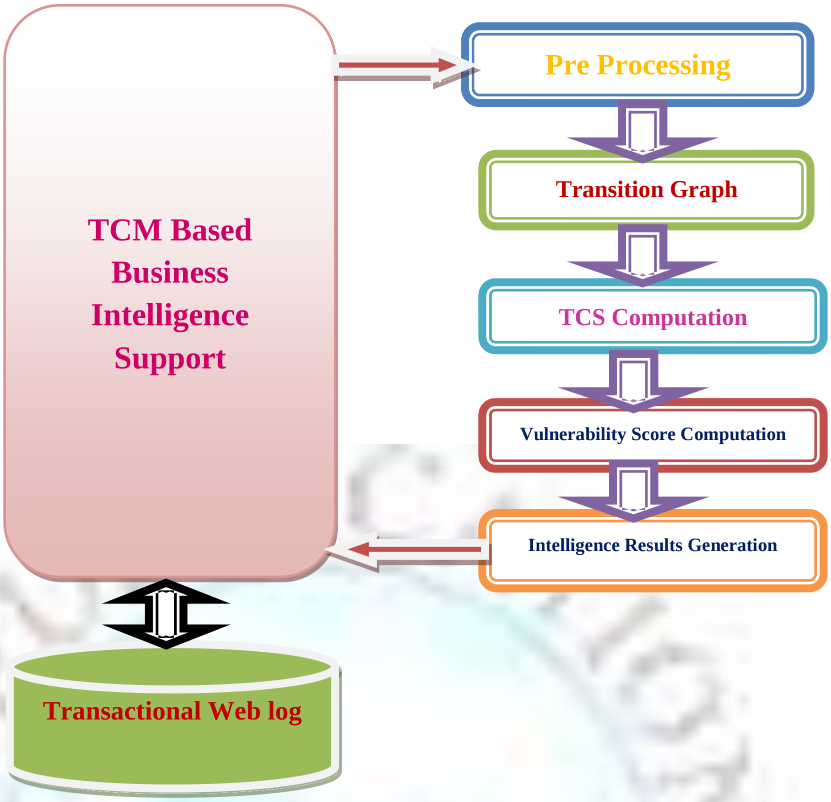


Figure 1: Proposed system architecture

3.1 Preprocessing:

At the preprocessing stage the web log is cleaned by identifying incomplete and noisy logs and converted into the form of computational script. The every access they get in which important piece of information about the accessing the recorded from the URL requested the IP address which the request invents and timestamp, service accessed and status of the service and etc…

Algorithm:

```
Step1: start
Step2: read web log Wl.
Step3: for each log l from wl
                Check for the feature and noise.
                If incomplete then
                        Remove record from log.
                        $Wl = Ø (l \times Wl)$.
                End
Step4: stop.
```

3.2 Transition Graph Generation

Transition graph is one which represents the traversal path of the user request. In a banking application the user will login first, then he may tends to transfer the money to some other account and to transfer the money to other account he has to provide valid account number and have sufficient balance in his account. The transaction will succeed only if he provide proper transaction password and security key generated at the runtime. So the transaction has various steps and each has to be completed accordingly. Each stage of the transaction is considered as a vertex and each transition is marked as edge. Each user log will be generated as a graph at one session and will be used for analysis.

3.3 Transaction Completeness Score

The TCS is computed using generated transaction or transition graph as follows: for each request received by the server the services which are completed successfully will be calculated and the number of services which are not completed successfully is also computed also the reason for the incompleteness is identified.

The vulnerability score is computed using the values of the TCS by computing the frequency of incomplete service access for each service. Also for each vulnerable pattern we compute the frequency and based on that the patterns are suggested for the admin peoples for further development of the solution.

Algorithm:

```
Step1: start
Step2: read service details (Sd) from data base.
Step3: Initialize vulnerability pattern vp, No of transaction Tn, no of completion Ct.
Step3: read preprocessed log Wl.
Step4: for each transaction $T_i$ from Wl
    Identify service name Sn.
    Identify number of internal Isn services of Sn.
    Initialize transaction id Tid.
    Track the service id and service invocation and status.
    If the service status== ok then
Cn= cn+1;
Else
    Identify user, status, pattern.
Add pattern to Vulnerable Pattern vp.
                                   End
            End.
Step5: compute Tcs = tn-cn;
Step6: compute vulnerability score vs =( Tcs/Tn)×100.
Step7: stop.
```

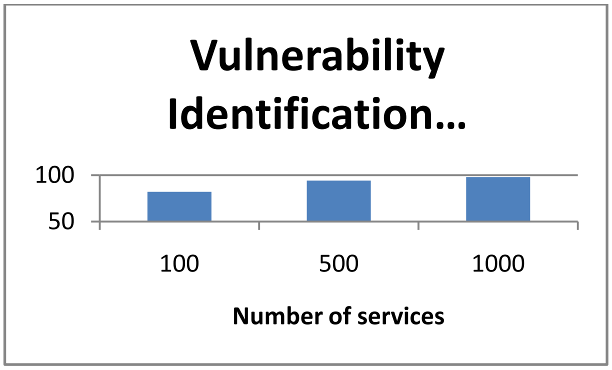
3.4 Intelligence Results Generation:

The vulnerability intelligence will be generated from the identified patterns. From the patterns identified from analysis we select the unique patterns of vulnerability and prepare a set of reports which shows the time, date and frequency of pattern appears in the web log.

4. Result and Discussion

The proposed TCM based vulnerability analysis framework has produced better results in identifying the malicious threats and network threats which happens in different business environment also in other transactional fields.

Table1: shows the frequency of identifying vulnerability.



Conclusion

We proposed a vulnerability analysis framework which uses the web log traces to preprocess and extracted the necessary features to generate the transaction graph using which we have computed the transactional completeness and vulnerability score to identify the vulnerability and propose set of patterns how the malicious user generates vulnerabilities to the business solutions.

References

[1]. Lowis L, Vulnerability Analysis in SOA-Based Business Processes, Ieee transaction on service computing, volume 4 issue 3 pp 230-242, 2011.

[2]. Gjerde o, Risk and vulnerability analysis of power systems including extraordinary events.

[3]. Unclassified Statement for the Record on the World wide Threat Assessment of the US Intelligence Community for the Senate Select Committee on Intelligence James R. Clapper Director of National Intelligence January 31, 2012.

[4]. “Towards a new stage in the bi-regional partnership: innovation and technology for sustainable development and social inclusion” MADRID ACTION PLAN 2010-2012.

[5]. Web Security Log Server Troubleshooting Guide Topic 50300 | Web sense Web Security Solutions | Version 7.7 | Updated 29-Jun-2012.

[6]. Decision-making under uncertainty: an assessment of adaptation strategies and scenario development for resource managers a white paper from the California energy commission’s California climate change center July 2012 cec-500-2012-027.

[7]. Dwivedi A, A Maximum-Flow-Based Complex Network Approach for Power System Vulnerability Analysis, Ieee Transaction on industrial informatics volume 9, issue 1, pp 81-88, 2013.

[8]. Jenelius, E. 2007. Incorporating dynamic and information in consequence model for road network vulnerability analysis. INSTR 2007.

[9]. M. Rihan, M. Ahmad and M. Beg, "Vulnerability Analysis of Wide Area Measurement System in the Smart Grid," Smart Grid and Renewable Energy, Vol. 4 No. 6A, 2013, pp. 1-7.

[10]. Walnerstrom c.j., Vulnerability Analysis of Power Distribution Systems for Cost-Effective Resource Allocation, ieee transactions on power systems , vol 27, issue 1, pp 224-232, 2012.

[11]. Yang hang, A Framework of Business Intelligence-Driven Data Mining for E-business, NCM, pp 1964-1970,2009.

[12]. Ciabanu V, A Distributed Approach to Business Intelligence Systems Synchronization, Symbolic and Numeric Algorithms for Scientific Computing (SYNASC),pp 581-595, 2010.