# 정성적 위험 분석을 위한 버디 시스템의 구조 분석

o
윤 정 원* 김 홍 근*

한국 전산원*
전산망 보안실

# The Architectural Analysis of the Buddy System for Qualitative Risk Analysis

o
Jeongwon Yoon* Hong-Keun Kim*

Information Systems Safety and Security Center
Korean National Computerization Agency*

***Abstract*** The importance of the risk analysis tool has been recognized and its use also has been emphasized by a number of researchers recently. The methodology were examined but neither algorithms nor practical applications have been implemented or practiced in Korea. In this paper, the architecture of the Buddy System, one of the automated risk assessment tools, is analyzed in depth to provide the algorithmic understanding and to promote the development of the risk analysis methodology. The Buddy System mainly uses three main factors of vulnerability, threat and countermeasures as a nucleus of the qualatative analysis with the modified loss expectancy value. These factors are identified and assessed by the separation of duties between the end user and security analyst. The Buddy System uses five axioms as its bases of assessment algorithm and the assessed vulnerability level is strictly within these axioms. Since the In-place countermeasures reduce the vulnerability level up to a certain level, the security analyst may use "what if " model to examine the impact of additional countermeasures by proposing each to reduce the vulnerability level further to within the acceptable range. The emphasis on the qualitative approach on vulnerability leveling is very well balanced with the quantitative analysis that the system performance is prominent.

## 1. Introduction

The risk assessment methodologies have been widely used in both industry and government organizations. Since there are so many different techniques available, it is more than simple to judge which methodology is more appropriate than the others. Many developers and vendors claim that their assessment tools and services are better but , for users, the performance of the risk analysis is very hard to determine because of diversity of methodology.

However, by analyzing the automated risk assessment systems, a relative comparison with other systems could be possible and the overall structure and algorithm could also be evaluated in depth. The automated risk assessment systems have been evaluated before by NIST(National Institute of Standards and Technology) of U.S., many other security related institutions and researchers. However many algorithms adopted by the risk assessment system haven't been justified their accuracy and efficiency due to its diversity. Each algorithms are method-oriented and environment-dependent that the parameters are too various to be used for comparative analysis. Therefore, the analysis of each algorithm needs to be done by varifying the nucleus of risk factors and their interplay based on the ISO(International Organisation for Standardisation)'s definition as the baseline.

In this paper, the analysis of the Buddy System was performed. The Buddy System has very unique algorithm which is simple and efficient than the other competitors. The main analysis module of the Buddy System concentrates on the vulnerability, countermeasure, threat, assets and data. And the interplay and relationship between these factors are following the algorithm's five axioms that mostly meet the ISO's guidelines. The most important features of the Buddy System's algorithm is that it allows the coustomization to fit the system to the target environment for accurate analysis. The Buddy System has been simulated and tested by chainging target system's parameters and the result verifies the accuracy and efficiency of the algorithm. However, the comparitive testings of the other risk assessment tools are in progress.

## 2. Overall System Architecture

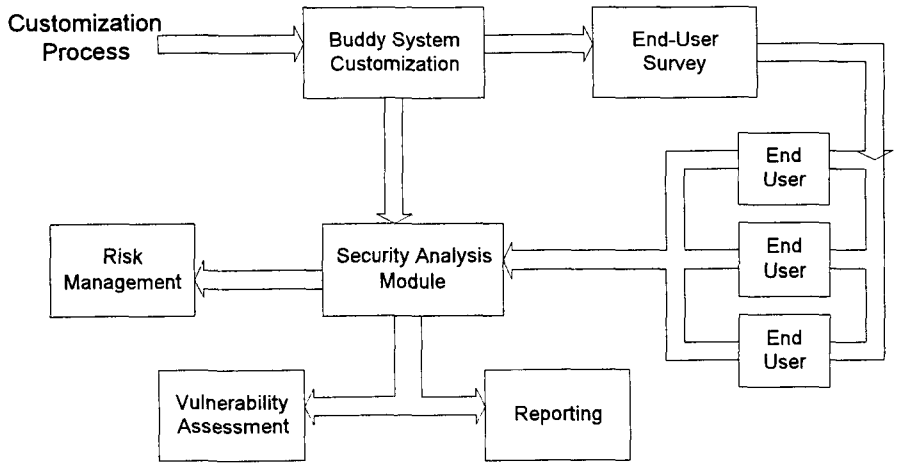


*Fig. 1. Buddy System Architecture*

The overall structure of the Buddy System consists of three main parts; security analysis module, maintenance module and end-user survey module. Security analysis module processes the analysis algorithm to produce the results of vulnerability assessment, threat and countermeasure identification and loss expectancy value. Maintenance module controls the most of the risk management process which maintain tracking and assigning actions. The historic analysis logs in the module are maintained for a future assessment and the decision made by the risk manager is also recorded for compliance evaluation. Moreover, the maintenance module also supports the customization process, that the analyst could edit the parameter of weights corresponding to each threat sources and countermeasure, to adjust the Buddy System to the target system environment. The end user surveys is very user friendly and can be done by each system user or administrator depending upon the system type such as microcomputer or mainframe. To comply with strict regulation of performing analysis which is proposed by the risk manager, the surveys could be done with regularity throughout the network and converge to the security analyst for collection. Then, these surveyed datum could be imported to the analysis module. Throughout the reporting process, there are seven major reports produced, which are risk analysis report, end used system information summary, vulnerability summary, compliance/audit measurement, multiple system vulnerability analysis, risk management report and in-place countermeasures report. Finally, upon the results, the risk manager assigns proper actions to each responsible personnel of the target system with the compliance requirements, countermeasure implementation and redoing of user survey.

## 3. Qualitative Approach

The architecture of the Buddy System provides both quantitative and qualitative analysis. The Buddy System carefully measures the vulnerability level by accessing the In-place countermeasures with the defined threat sources and computed loss expectancy values. The Buddy System is guided by the 5 axioms which is the fundemental baseline of leveling system vulnerability. These axioms always apply whenever the threats, vulnerabilities and/or countermeasures defined, paired, accessed or used throughout the entire analysis process. Any given countermeasures may be paired with more than one vulnerability and may be assigned a different weight for each pairing.

### 3.1 Five Axioms

The five axioms are fundamentally corresponded to the definitions of ISO's suggested guidelines[6]. These axioms are bases of the Buddy System as mentioned before.

T : Threats(Population of)
Ft: Frequency of Threat Occurrence
V : Vulnerability
C: Countermeasures
A: Assets

Axiom #1: The same population of threats exist for all systems[4].

$T = \{ T1, T2, T3, .... \}$

For any arbitrary Target Systems Sx and Sy,

Sx = { Vx, Cx, Tx, Ftx, Ax } and Sy ={Vy, Cy, Ty, Fty, Ax}
then, Tx = Ty always regardless of any other parameters.

Axiom #2: The frequency of occurrence of a threat cannot be altered[4].

$Ft = \{ Ft1, Ft2, Ft3, ..... \}$ where each $0 < Ftn < \infty$
When certain time interval is defined, say t(n), t(n+1) then,

$$Ft = \sum_{n=1}^{n=\infty} Ftn(Tn)$$ where Ftn = Frequency of Threat Occurrence
when $t(n) \leq Ftn \leq t(n+1)$, and Ftn can not be predicted.

There is no parameter exist to alter the Ftn by any means such as V, C, or A except T. However, the population of threats are infinite and the frequency of the threats(Ft) is uncontrollable by nature under any circumstances. Therefore, application of the countermeasures only reduces the level of the vulnerability to the manifested threat but not the frequency of the threat. This axiom corresponds to the following ISO's definition of threats[6]; a cloud of threats, constantly changing and only partially known. The definition implies that the population of threat is unpredictable( could be zero or infinite) and the frequency of threat groups are incident-dependent that means no alteration is allowed.

Axiom #3: Vulnerability decreases as countermeasures increase[4].

$V \propto 1/C$ where $C < \infty$, therefore $V > 0$
also $C = \{ V \}$ and $V \notin \varnothing$

Countermeasures could never be infinite since they have inherent vulnerabilities that creates another risk requiring countermeasures.

Axiom #4: All countermeasures have inherent vulnerabilities[4].

Any countermeasures have their own inherent vulnerabilities that a level of vulnerability can never be achieved to zero. According to the ISO's definition, safeguards(countermeasures in the Buddy System) may have some internal vulnerability, or not be totally effective, that lead to residual risk after implemetation[6]. Conclusively, the axiom #3 and #4 are inter-dependent.

Axiom #5:An acceptable level of vulnerability can be obtained through the implemetation of countermeasures[4].

Axiom #5 gives many possible solution to reduce the level of risks, by adopting the customization, "what if" scenario, to an acceptable level. The followings states the ISO's definitions; sometimes, several safeguards are necessary to reduce the residual risk associated with a threat to an acceptable level; sometimes, no safeguards are needed, despite the possibility of a threat because the risk is acceptable.

### 3.2 Vulnerability Level

The computation of the vulnerability level depends on the In-place countermeasures and the customized setup that provides interplay of each primal sources, such as threat, assets, countermeasures and data sensitivity, which are preloaded and paired with each vulnerability by the security analyst. The types of vulnerability, which are eighteen in total, are defined by the Buddy System and the analyst may edit these for customization by adding, deleting, or even pairing with other primal sources. Since each vulnerability must be paired with one or more countermeasures, threats and asset groups, the analyst should investigate their target systems and their environment before starting the customization process. The details are discussed in the next section.

After the customization process, the analysis module is ready to run by first computing the level of vulnerability. The main formula is the following.

$$Vlevel = ( \Sigma Wcmi ) - ( \Sigma Wcmp)[4]$$

Where, Vlevel : Vulnerability level, in any area of vulnerability,
Wcmi : The total weight of countermeasures that are currently In-place for the system,
Wcmp: The computed value assigned to each area of vulnerability. It is the sum of all positive weights of countermeasures that are paired with the specific vulnerability area.

Wcmp is always bigger than Wcmi due to the axiom #4 states that all countermeasures have inherent vulnerabilities. Therefore, even all the countermeasures are implemented, the best vulnerability level that can be achieved is 2.0 but never 0.0. By default, the acceptable range of the vulnerability level lies between 2.0 and 12.0. The worst level is 18.0.

## 4. Customization

The customization process, which is the qualitative approach of the Buddy System, is the key to efficient and accurate analysis. Even the computation of the Annual Loss Expectancy(ALE) values is partially embedded in the idea of the qualitative approach of the customization process. Each asset group of hardware, software, data, tangible/intangible assets is evaluated for ALE after paring, weighting, editing of vulnerability, threat, asset and countermeasures.

Vlevel × Tfact × Av = SLE[4] then, SLE × Tf = ALE[4]

where: Vlevel = Target system's vulnerability level in each applicable area

Tfact = The degree of exposure to the paired vulnerability area (high, medium, or low).
High Constant = 0.05555, Medium Contant = 0.005555,
Low Constant = 0.0005555

Av = Asset value expressed as dollar
SLE = Single Loss Expectancy, means dollar amount that will be lost with each occurrence of the paired threat.
Tf = The projected number of times the threat will occur in a given year.
ALE = Annual Loss Expectancy, or the amount that may be lost over the period of one year due to threat occurrence.

Threat customizations are determined by four major factors such as destruction, modification, denial of service and disclosure. Each factor has its own weight value and the sum of all values must be equal to 1.0 or 100%. The total impact value of 1.0 means that a single threat occurrence can never cause a loss greater than an asset's total value. Through the process, the appropriate paring with vulnerability is done by deciding exposure factor which determines the High, Medium or Low as mentioned in ALE computation. More complex customization process is the vulenrability pairing with assets. Whenever threat occurs by the associated vulnerabilities, a negative impact to the asset groups occurs. The pairing process must be done by the "what if" scenario that carefully examine the possible scenario of security holes and its impacts. All possible countermeasures against vulnerabilities must be considered to be paired during the customization process accordng to the "what if" scenario. The risk analyst could embed all possible scenarios into the customization process. The scenario could be laid down using many available identification methodology of risk management. For instance, the delphi technique could be used if the security experts and analyst from each department/division can analyze the current scenario or plan the new one. Figure 2. shows the overall flows of the algorithm.

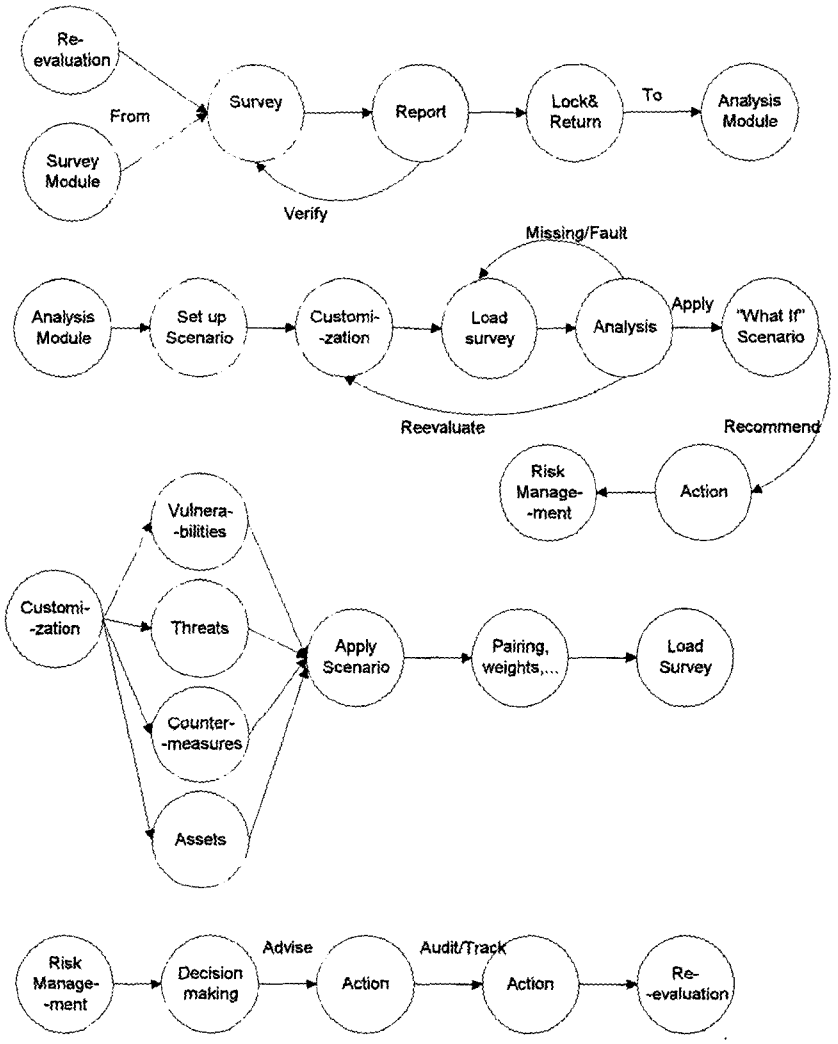


Fig. 2. The Flow of Analysis Process

## 5. Conclusion

Since the accuracy of the risk analysis is heavily depended on the scenario, it has to be carefully examined before actual application. Throughout the analysis of the Buddy System, the application of the simple scenario, which was designed by us for the purpose of the test, was done and the result of the vulnerability assessment, ALE computation

and the threat identification were turned out to be satifying. Even the Survey Module is relatively user-friendly, the survey of the target system done by the end user needs to be verified by the risk analyst to avoid the tendency of faulty identification, cover-ups, and misunderstanding. Comparing with the other risk analysis tools such as Riskpac, BDSS, or CRAMM, the cost-benefit ratio of the Buddy System shows relative superiority because of the low maintenance cost. However the customization, which is too dependent on the scenario designed by the security analyst, needs to adopt dynamic approach such as the knowledge-based system that actually helps the analyst to set the appropriate scenario by just adjusting parameters of the target system environment. In this way, the top-to-bottom design of the scenario is unnecessary. Therefore the possibility of the fallacy existing in the customized design could be eliminated and the result could be more credible.

## 6. References

[1] Jackson K. M., Hruska J. and Parker, D.B., Computer Security Reference Book, CRC Press, 1992.

[2] Ozier, Will, "Issues in Quantitative Versus Qualitative Risk Analysis", Datapro, McGraw-Hill, Vol. 1, No. IS20-25, January, 1994

[3] Perry, William E. and Kuong, Javier F., EDP Risk Analysis and Control Justification, Management Advisory Publications, 1981

[4] Zenkins, Budddy, Security Analysis and Management Manual, Countermeasures Inc, 1994

[5] Description of Automated Risk Management Packages, NIST/NCSC Risk Management Research Laboratory, March 1991

[6] Guidelines for the Management of IT Security, ISO(International Organisation for Standardisation)/IEC(International Electrotechnical Commission) JTC 1 / SC27 / WG1(Work Group Meeting) N391, October 1993