Security Evaluation of IT Products: Bridging the Gap between Common Criteria (CC) and Real Option Thinking

Haider Abbas, Louise Yngström, Ahmed Hemani

Abstract—**Information security has long been considered as a key concern for organizations benefiting from the electronic era. Rapid technological developments have been observed in the last decade which has given rise to novel security threats, making IT, an uncertain infrastructure. For this reason, the business organizations have an acute need to evaluate the security aspects of their IT infrastructure. Since many years, CC (Common Criteria) has been widely used and accepted for evaluating the security of IT products. It does not impose predefined security rules that a product should exhibit but a language for security evaluation. CC has certain advantages over ITSEC[1], CTCPEC[2] and TCSEC[3] due to its ability to address all the three dimensions: a) it provides opportunity for users to specify their security requirements, b) an implementation guide for the developers and c) provides comprehensive criteria to evaluate the security requirements. Among the few notable shortcomings of CC is the amount of resources and a lot of time consumption. Another drawback of CC is that the security requirements in this uncertain IT environment must be defined before the project starts. ROA is a well known modern methodology used to make investment decisions for the projects under uncertainty. It is based on options theory that provides not only strategic flexibility but also helps to consider hidden options during uncertainty. ROA comes in two flavors: first for the financial option pricing and second for the more uncertain real world problems where the end results are not deterministic. Information security is one of the core areas under consideration where researchers are employing ROA to take security investment decisions. In this paper, we give a brief introduction of ROA and its use in various domains. We will evaluate the use of Real options based methods to enhance the Common Criteria evaluation methodology to manage the dynamic security requirement specification and reducing required time and resources. We will analyze the possibilities to overcome CC limitations from the perspective of the end user, developer and evaluator. We believe that with the ROA enhanced capabilities will potentially be able to stop and possibly reverse this trend and strengthen the CC usage with a more effective and responsive evaluation methodology.**

***Index Terms*— Common Criteria (CC), IT Security Evaluation, Real Option Analysis (ROA), Return on security Investments (ROSI)**

H. Abbas is with the Royal Institute of Technology, Sweden (email: haidera@kth.se)
L. Yngström is with the Royal Institute of Technology, Sweden (email: louise@dsv.su.se)
A. Hemani is with the Royal Institute of Technology, Sweden (email: hemani@kth.se)

I. Introduction

Real option analysis is considered a sophisticated methodology for making decisions under uncertainty mainly in corporate finance. It enables, making investment decisions efficiently and choose from a range of possible options for investing in the future market. ROA perceives an option as a "right" and not as an obligation, thus opening grounds for investor to opt from various alternatives. Another advantage of ROA is the provision of providing opportunities for making different investments in parallel for a specified period of time. Moreover the decision can be altered based on the outcomes that have been achieved during that period. ROA is widely used and accepted by the economists, business community and the venture capitalists as an assistive tool for decision making. Its significant success and popularity in corporate finance has inspired software engineers to use Real options theory in software engineering processes [1] i.e. eXtreme Programming (XP), project investment analysis and many more.
IT infrastructure revolves around uncertainty due to rapid technological innovation and novel threats eruptions caused by development. This requires acute need for the authenticity of the IT products and hence a comprehensive methodology is inevitable. CC (common criteria) for this purpose is widely used and accepted for the evaluation of the security of IT products since many years. The main focus of CC as shown in Fig 1 is to address the three main dimensions i.e., it provides opportunity for users to specify their security requirements, an implementation guidance for the developers, and the evaluation strategy for the laboratories to justify if the requirements are fulfilled [2].

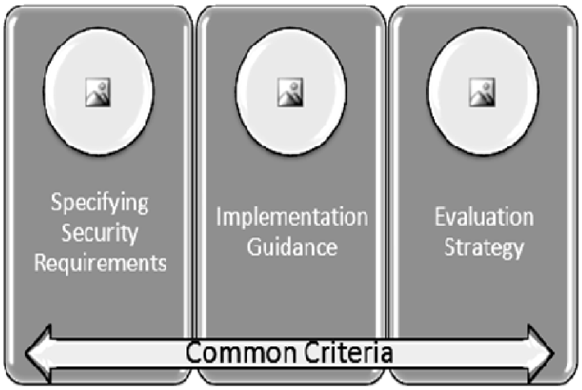

Figure1. Three Dimensions of Common Criteria

[1] Information Technology Security Evaluation Criteria
[2] Canadian Trusted Computer Product Evaluation Criteria
[3] Trusted Computer System Evaluation Criteria

Last but not the least it provides a standard for the evaluation with different assurance levels (EALs) that are well accepted under CCRA (Common Criteria Recognition Arrangement) by contracting countries [3]. The assurance levels may base on the organizations different opinion of their security requirements but having the same objective of the authenticity for the IT product.

Along with the advantages of a technique there are always some shortcomings associated same is the case with CC, as it requires considerable resources in terms of amount and time. Therefore it has always been criticized [4] [5] [6] by the practitioners and security professionals and considered as cumbersome procedure. In this paper we aim to analyze the possibility of applying real options theory to cope the uncertainty issues in security evaluation. We will explore the possibility that how ROA methodology can be used to boost the existing CC infrastructure in order to make it a complete and efficient solution for any IT system's security evaluation. The rest of the paper is divided into four sections, first section elaborates the ROA advantage over other methods like NPV and DCF, second section analyzes the ROA use in various domains, third section analyzes the success stories of ROA use in IT and IT security decision makings. Employing ROA thinking on CC is twofold, one from the user aspect and other from the evaluator. In fourth section we will look into semantic and procedural aspects that if the ROA thinking can be used for refining CC infrastructure.

II. ROA VANTAGE

Real Option Analysis helps to take efficient investment decisions in a high risk area [7]. It provides investment opportunities in an uncertain environment and reveals the hidden options for investor. Practitioners in corporate finance grade ROA potentially advantageous over traditional approaches like NPA (net present value) and DCF (discounted cash flow) [8]. In a high risk area NPV and DCF may lead to under investment and impose higher discount rate in adjustment for higher risks, thus reducing the overall future income streams [8]. DCF targets one time valuation of the asset and makes decision accordingly for valuation of risk management. It neglects the exploratory phase of the investment having the objective to explore the opportunity for further investment into the project [9]. ROA considers the option approach and assigns positive value in high risk area. It spreads the investment into phases keeping the option for termination in case of failure and prolongation with further investment in case of success.

III. ROA AS A MULTIDIMENSIONAL PARADIGM

Real option was primarily formulated by Professor Stewart Myers at the MIT Sloan School of Management around 1977 [10] in a methodological way for making capital investment decisions in corporate investments. Michael J. Mauboussin popularized this concept by effectively using for stock market investments. This was the prime significant use of ROA in finance and provided new grounds for exploration to the business researchers. It soon acquired competitive advantage over other traditional investment valuation models. ROA gained popularity with the passage of time and attracted the researcher from various domains to use ROA as a tool for making investment decisions in their respective fields. We will analyze the use of ROA in various domains in the following sections.

A. ROA in Government sector

Government's policies and initiatives in R&D face uncertainty and thus require a specific time for maturity. The outcome for such projects become clear and can be measured when they are actually deployed. Certain initiatives have been taken to estimate the appropriateness of using ROA in order to make investment decisions for the governmental projects. An advice from the council of science and technology to the secretary of state says *"The Council for Science and Technology (CST) suggests that, in the context of the Ten Year Investment Framework which requires substantial growth in business R&D in the UK and where the Government is increasing its own funding of the science base, it is essential that Government draws on the best available information and techniques for taking decisions on which projects to support. We believe that ROA could play a valuable role here."*[11]. Some recommendations have been made by CST [11] to government for employing ROA for dividing investment decision into phases.

We assume that, ROA when used in public sector for the investments decision will give a broader concept of experiencing more opportunities. This model provides multidimensional view for utilizing an option along with the possibility to roll back or to continue a project. If properly used and researched this technique will lead any government to take better investment decisions even in more uncertain situations. It will thus improve the capacity of the government to consider much more R&D projects and for taking the appropriate investment decisions.

B. ROA in Technological Innovation

Rapid technological innovation in information technology has lead to uncertainty and caused novel threats. Most of the businesses today are relying on technology (software and hardware) and it serves as a backbone for the entire business system. There is a careful analysis needed regarding how much to invest in each stage of implementation phase in this uncertain environment of emerging technology. Dhiman Chitterjee and VC Ramesh present a model for risk management of software project using option valuation techniques [12]. Their model recommend at early stage of software development to analyze technology identification and take managerial decision regarding adoption for the project. Different alternatives of the innovative technology should also be considered at this stage. Next step is to determine the existing position of the organization including employee's expertise and its financial ability to adopt the identified technology. Having all these issues identified, Real options then can be employed to view the opportunities for investment in a particular project.

C. ROA in IT Security Decisions

Information security has become critically important for any organization competing in electronic commerce. Investment decisions evolve around uncertainty due to the emerging technology topped with novel attacks and vulnerabilities. Every organization has to face the challenge for determining the appropriate security area and to take the appropriate counter measures. A survey report published by CS/FBI computer crime and security survey 2005, describes that many organizations have started using economic models like NPV, ROSI and IIR (Internal Rate of Return) for security investments to assign economic values to their investments [13]. As we have previously discussed that these traditional approaches do not consider the managerial flexibility for altering investment decision when some uncertainty is known.

Jingyue Li and Xiaomeng Su have concluded in their paper [14] that managers prefer to have a mid course correction in decision or strategy during the project. This will add flexibility to adopt new changes that become unavoidable or to forgo for an option that becomes obsolete during the project. Real option provides the power to calculate value for a flexible solution under uncertainty. This fits more appropriately while considering security solutions due to the reason that today's businesses have uncertain security requirements. Business market is of divergent nature, sometime it requires to invest more to adapt novel technology to survive in a competitive environment or to roll back and consider to invest in some other market. If the current business relies on technology then security management can be considered as integral part of the business also.

IV. Discussion

In the above sections we have reviewed the Real option analysis and its different flavors for some uncertain environments. ROA provides strategic flexibility in decision making and benefits mainly in two domains. First for the financial option pricing where results are deterministic then Black Scholes equations and Binomial Lattice can be employed. Second for the more uncertain real world problems where mathematical calculations could not be implied then decision tree analysis or Monte Carlo simulations can be used as shown in figure 2.

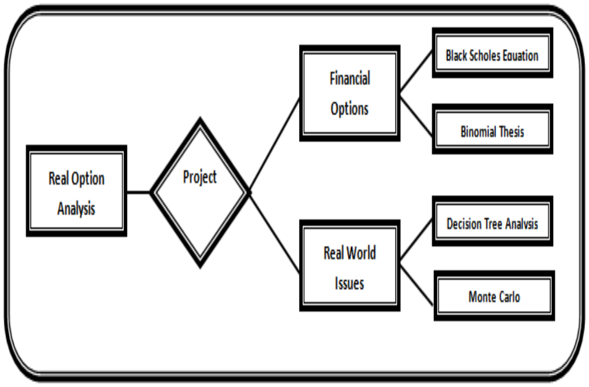

Figure 2: Applicability of various Real Option Techniques

Real options as its name implies use options theory to evaluate the assets with significant amount of a managerial flexibility under significant amount of uncertainty. It uses different options i.e. expansion, abandonment etc. that corresponds to the real world problems. The flexibility in real options framework inspired technocrats and researcher to use real options power to target uncertainty issues in their respective areas. We believe that a framework based on Real options theory will provide potential benefits in security evaluation of IT products.

V. Exploring Possibility To Model Common Criteria (CC) Evaluation Using Real Options Theory

The ever growing popularity of ROA and its advantageous solution to cope with uncertainty issues have lead us to explore it as a principal candidate to be used for Common Criteria methodology. Common Criteria is being criticized by the researchers due to a costly, time consuming and cumbersome procedure. The possibility to use ROA thinking in evaluation of IT systems will be analyzed based on ground realities for uncertainty and their correspondence to ROA vantages.

A. Analysis of CC shortcomings and ROA Vantages:

The theme of the real option theory aims to uncover the hidden possibilities of using options that are considered as “right” not the “obligation”. On the other hand Common Criteria is used for specification, implementation and evaluation of IT security. CC recommends a requirement specification process using PP (protection Profiles) before the project starts and it only evaluates the product according to the protection profile (PP) requirements. Using real options enhanced methodology, for example the critical security feature or the standards imposed by the government or law enforcing authorities can be executed and the uncertain requirements could be specified later when they become clear. This will enable to manage changing requirements due to uncertain IT environment with novel attacks and vulnerabilities. For example an IT product has the security requirement of strong authentication then its implementation has the options embedded using passwords, biometrics, smart cards etc. If product is in evolution phase the passwords mechanism could be used for the time being and can be continued or replaced with biometrics or smart cards in case of failure.

Evaluation process of CC in real option thinking could be of twofold one way would be the customer side to apply ROA and the other side will be from the prospect of evaluation laboratory. The customer can apply ROA to decide the current evaluation options and to defer its dependent evaluation. The evaluation laboratory may employ ROA for various evaluation decisions. The evaluation of a component can be divided into phases considering uncertainty involved due to technology innovation or the evaluation cost in terms of personnel efforts.

Common Criteria is also criticized due to an expensive method. It requires an extensive amount of resources for the evaluation process to get a product CC certified and when the product is evaluated it does not guarantee that the product is secure. Because the evaluation is done according to the requirements that CC requires to be specified before development. Using real option thinking the requirement specification and evaluation strategy will be enhanced and it will work in an iterative manner to adopt novel threats and manage changing requirements. Real option theory can also be employed in this scenario of the CC requirement specification and implementation to take advantageous investment decisions.

In a volatile IT environment security evaluation involves heedful consideration of the vulnerabilities and security breaches occurred recently. Also it can happen that these threats may go away and new threats or breaches may appear in due time. So the researcher believe to opt the strategy of wait –and-see, Gordon et al.[15] suggest to spend on security at actual breach. While CC believes to provide details of security requirement of the product under consideration in protection profile (PP) in the early stage and PP is created by the user community. CC is inspired by the waterfall model and works in a sequential fashion but it has the potential to opt any other strategy. Deploying ROA with CC infrastructure will require working in an iterative fashion based on the following ground (i) uncertainty in backbone technology's innovation (ii) novel threats and vulnerabilities bundled with the new technology (iii) obsolescence of existing security measures.

B. *Proposed Strategy*

ROA is widely used for investment decisions; our task of using Real options theory for evaluation of security systems will open new challenges. In this paper we have done an analysis for using CC as a principle candidate when used with ROA. The two models are independent of each other and have their own advantages and disadvantages therefore we propose a bridging metrics model that will overcome the shortcomings of these two models and provide a flexible structure to the future users for IT security evaluation. This metrics model is based on Real Options theory that will be used to address the critical issues faced by IT security product evaluation. This metrics will bridge two domains as shown in figure 3.

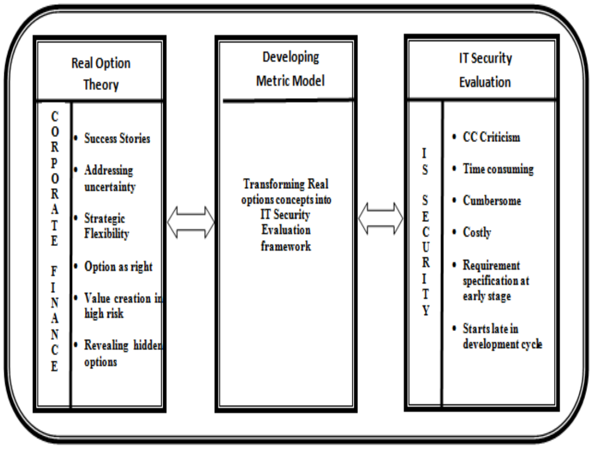

Figure 3: Metrics model approach for bridging gap between ROA and IT Security Evaluation

This metrics model will help to set basic rules for security evaluation using real option theory. Our analysis in this paper shows that root cause for most of the criticism of CC is uncertain infrastructure and Real option theory provides significant results for such environment. Defining security requirements for a rapidly changing environment based on option theory will benefit to manage complex requirements that become known during development or evaluation. Evaluation strategy is also based on requirement specifications, employing options theory here and working in an iterative way, will help to reduce time and resource consumption.

VI. Conclusion

In this paper we have reviewed in depth ROA, its origin, popularity and vantage over other traditional financial methods. We highlighted some domains where ROA is successfully employed to cope with uncertainty in investment decisions. ROA success stories influenced us to analyze the possibility to use real options theory for the evaluation of IT security products. We have given a preliminary idea for exploring ROA thinking in semantic and procedural aspects. We assume that there will be a metrics model based on Real options thinking for this process to be accomplished. At this point in time we can conclude that for the employment of ROA in CC requires working in an iterative way to achieve significant results. We believe that employing ROA thinking in CC seems semantically and procedurally valid and this fuel up our enthusiasm to explore further to develop a model based on ROA that will address CC criticism. As a future work we intend to continue our research to enhance IT security evaluation process using ROA thinking and build an infrastructure that could be used for taking efficient security evaluation decisions. We will come up with a detailed methodology and implementation details followed by some case studies in future.

References

[1] B. Tansey and E. Stroulia, Valuating Software Service Development: Integrating COCOMO II and Real Options Theory

[2] Common Criteria for Information Technology Security Evaluation, Version 3.1 Revision 1, September 2006 http://www.commoncriteriaportal.org/

[3] Arrangement on the Recognition of Common Criteria Certificates In the field of Information Technology Security, May 2000

[4] J. Jackson , Symantec: Common Criteria is bad for you, March 2006 http://www.gcn.com/online/vol1_no1/44205-1.html?page=2

[5] GAO United States Government Accountability Office, Information Assurance National Partnership Offers Benefits, but Faces Considerable Challenges, March 2006 http://www.gao.gov/new.items/d06392.pdf

[6] W. Jackson, under attack Common Criteria has loads of critics, but is it getting a bum rap? : http://www.gcn.com/print/26_21/44857-1.html

[7] J. Mun, Real Options Analysis - Tools and Techniques for Valuing Strategic Investments and decisions, Wiley Finance

[8] F.J. Faboozi, published Jul 29, 2007 Comparison between Real Option Valuation & Discounted Cash Flow Valuation : http://www.associatedcontent.com/article/327842/comparison_between_real_option_valuation.html

[9] B. R. Cobb, John M. Charnes , Real Options Valuation Proceedings of the 2007 Winter Simulation Conference

[10] Real options analysis: http://en.wikipedia.org/wiki/Real_options_analysis

[11] Council for Science and Technology, Real Options Analysis – a tool to help make decisions about investments, 18th May 2005 http://www.cst.gov.uk/cst/business/files/real-options.doc

[12] D. Chitterjee , V. Ramesh ,Real Options for Risk Management in Information Technology Projects, Proceedings of the Thirty-second Annual Hawaii International Conference on System Sciences-Volume 7, 1999

[13] L. A. Gordon, M. P. Loeb, W. Lucyshyn, and R. Rochardson, "2005 CSI/FBI computer crime and security survey", Technical Report, Computer Security Institute, 2005.

[14] J. Li, X. Su, Making Cost Effective Security Decision with Real Option Thinking, ICSEA '07: Proceedings of the International Conference on Software Engineering Advances (ICSEA 2007) - Volume 00, August 2007

[15] L.A.Gordon, L. Loeb, L. Lycysshin, Information Security and Real Options: a Wait-and-See Approach, Computer Security Journal, 19(3), 2003, pp. 1-8.