Abstract

Reliability of IT systems and infrastructure is a critical need for organizations to trust their business processes. This makes security evaluation of IT systems a prime concern for these organizations. Common Criteria is an elaborate, globally accepted security evaluation process that fulfills this need. However, CC rigidly follows the initial specification and security threats and takes too long to evaluate and as such is also very expensive. Rapid development in technology and with it the new security threats further aggravates the long evaluation time problem of CC to the extent that by the time a CC evaluation is done, it may no longer be valid because new security threats have emerged that have not been factored in. To address these problems, we propose a novel Option Based Evaluation methodology for security of IT systems that can also be considered as an enhancement to the CC process. The objective is to address uncertainty issues in IT environment and speed up the slow CC based evaluation processes. OBE will follow incremental evaluation model and address the following main concerns based on options theory i.e. i) managing dynamic security requirement with mid-course decision management ii) devising evaluation as an improvement process iii) reducing cost and time for evaluation of an IT product.

1. Introduction

In today’s world, a secure IT infrastructure is a must for any business organization, making the security evaluation a critical step. Rapid technological development that also results in equally rapid change in novel security threats has made the IT infrastructure vulnerable and requires agile and adaptive security evaluation process. Common Criteria [1] is a well-known security evaluation methodology that has been standardized and has been adopted by many countries [2] for security evaluation of their IT products. In spite of its wide-spread adoption, the limitations of CC as a slow, expensive and rigid process is well known[3][8]. In CC, the security threat is identified at the beginning of the process and rigidly followed during the course of the long evaluation process. This rigidity of CC and its inability to deal with changes during the evaluation process and the need for incremental evaluation during the lifetime of the IT product/infrastructure is what we address in this paper with an Options Based evaluation methodology.

Real options analysis [4][6] is a corporate finance method used for uncertainty analysis and has proved effective for uncertain investments in various domains. It provided strategic guidance in Govt. projects in Oil & Gas industry and also in IT security investments [14]. We have used the power of options theory to target uncertainty issues in IT security. Firstly, we will present the short description of adaptability model (needed to bridge IT security and real options theory) and then proceed to describing Options Based Evaluation (OBE) its prerequisites, dynamic security requirement management infrastructure and various phases to evaluate an IT product. SHS1 a Swedish government network infrastructure [7] developed by VERVA2 is referred as example for more precise illustrations.

2. Related work

Options theory to manage uncertainty issues and dynamically changing security requirements for IT security provides significant results. But there are several other areas of predictive analysis. Namely, Architecture Trade-Off Assessment Method

---

1 Sprednings- och Hämtningssystem
2 Swedish Administrative Development Agency
(Statskontoret as top level authority, VERVA no longer exists)
(ATAM) [5], Attribute Based Architecture Styles (ABAS) [19] and Architecture-Based Analysis of Complex Systems (ABACUS) [20]. Maxwell et al [17] and Parakhine et al [18] also present useful methods for analyzing architectures for non-functional requirements using predictive techniques. Options theory emphasizes on multiple architecture evolutions from non-functional requirements to functional requirements (for security) with different predictive techniques for each proposed solution and therefore done in a deterministic way with high confidence.

3. Adaptability Model

Information security and corporate finance are two diverse domains with their own work processes. Options theory follows mathematical models i.e. binomial model and various techniques i.e. Monte-Carlo simulation and Black-Scholes [4] for stimulating thinking about possible action/ options. Security evaluation process is carried out against some security criteria following security engineering methods [22] (model based testing, risk analysis etc) to provide assurance for the IT products and systems. It can’t be addressed directly using mathematical models. The commonality between these two domains is uncertainty resulting from changing evaluation basis. A middleware infrastructure was required to streamline both the processes and make them coherent. We developed an adaptability model that defines the basic rule of thumb and provides guidelines for uncertainty analysis in requirement specification and evaluation process for OBE.

4. Option Based Evaluation Methodology (OBE)

OBE mainly targets the dynamic security requirement management, evaluation as an improvement process and addresses some weaknesses of CC i.e. i) time span for evaluation ii) resource hungry evaluation procedures. OBE defines complete methodology for evaluation but it can also serve as a plug-in for Common Criteria, ATAM [21] etc. to deal with uncertainty issues. Based on uncertainty analysis in IT and novel threat eruptions which leads to the dynamic change in security requirements, we believe that the evaluation of IT products should be deployed as part of development cycle. OBE recommends a continuous process and addresses the complete development cycle for managing software evaluation and adjusting dynamic security requirements using options theory at various levels. It aligns very well with organizational objectives and can also be deployed into their existing setup. SHS is a network infrastructure used by Swedish Governmental organizations for their secure IT communication needs. We demonstrate the efficacy of OBE by evaluating the security aspects of SHS.

OBE is an iterative methodology and comprises of three phases as shown in Figure 1.

![Figure 1. Three Phases of OBE](image)

Phase 2 and phase 3 work closely in an iterative manner to adjust changing requirements during development or evaluation.

Identification of evaluation team is a prerequisite for OBE and its description and alternative solutions are as follows.

**Evaluation Team (Facilitator Group):** A group of persons with the responsibilities like requirement identification, evaluation, supervising the development process etc. Composition of the evaluation team is done before the OBE can be deployed. There are two alternatives depending on the product category and resources available:

- **Hire a team of experts (research labs) / University researchers.**
  
  This solution is appropriate if the IT product has to be delivered without the source code/ development details. Examples are IT devices or standardized IT software.

- **Build a team of internal employees from the organization.**
  
  This solution is appropriate if the product is going to be used internally or controlled by the developing organization. It helps to adjust changing requirements as they arise. For example SHS, developed and controlled by VERVA, Swedish Govt. agency for IT infrastructure, and VERVA is responsible for its smooth functioning. Any changes in security requirements can easily be addressed by VERA using OBE.

In OBE, the evaluation team is called “The Facilitator Group” and it consists of personnel having diverse expertise, i.e. information security specialists, real options expert, business analyst and test case experts. Their roles and responsibilities according to each phase are described in identification phase (stakeholders section).
Phase 1. Identification

This phase specifies the targets by identifying different aspects in the following three categories.

i) **Stakeholders**: Specifying which employees from the organization, developers and management are required to act as facilitator group. List of some possible stakeholders and their roles are as follows:

- **OBE Leader**: An expert responsible for the overall progress, coordination and decision making.
- **CIO (Chief information officer)**: Anchor person having the knowledge of the organization and its work processes.
- **Security Personnel**: Group of information security experts having knowledge of organization security requirements and capabilities to deal with security tradeoffs and test cases.
- **Business Analyst**: One or more resource persons with the knowledge of the business goals, Real options and dynamic decision making expertise.
- **Development Coordinator**: Representative from the developers to coordinate changes and manage iterations with the developers and evaluators.
- **Evaluators**: Group of evaluation experts consisting of test manager, test analysts and test case developers.

OBE roles could be varied according to the nature of the evaluation and product itself. One person can perform more than one roles and new role can also be defined if required.

ii) **Organization goals that specify their security requirements**: OBE identifies the security targets into two categories:

- **Internal Business policies**: Organizations, based on their business domain, model and management policy have specific security targets that need to be considered.
- **External Sources**: Countries and specific business segments, like banking, defense etc., might have their own set of security requirements and recommendations that needs to be considered. For example, minimum security requirement for federal information and information system by NIST [12] or FRA [13] in Sweden.

SHS was intended to provide secure communication channels between Swedish Governmental Organizations and later it was further extended for communication between Governmental and private organizations. SHS follows the Swedish government security requirement recommendations [13] with its own value added security features. SHS leaves the space for organization to adjust their specific security requirements as last mile connectivity for their internal system.

iii) **Candidate system and its boundaries**:

Specification of the target system or product and boundaries of the system to be evaluated. This also ensures the evaluation context i.e.

- **Product only**: The boundary in this case is restricted to evaluating the product as a stand-alone system. Neither the documentation, nor the context in which the product functions is part of evaluation.
- **Documentation and products**: When a product is a component of a larger system, its documentation is also a part of security evaluation, because the way the third party might integrate it relies on the quality of the documentation.
- **System evaluation**: This is the broadest category where, the product, its documentation and the context together with interacting applications and OS are also the subject of evaluation.

Identification phase gives a concise view of the target system, stakeholders and security requirements. It also reveals the opportunities, identifies constraints and tradeoffs in the system.

Phase 2. Options Based Formulation

After identification, the second phase is options based problem formulation and consists of following sections.

1. **Security requirement elicitation**: We use the system holistic approach [11] to get a concise overview of the system for specifying security requirements. There are two factors that specify organization’s security requirements as mentioned in the identification phase. Formulation phase divides these security requirements into two categories i.e.

- **Generic**: Security requirements for confidentiality, integrity and availability based on standard available technology and methods. Generic requirements also include any external enforcing authority’s requirements. For example, bank’s requirement to provide secure web transactions using SSL to its customers.
- **Specific**: Special security requirements except from standard requirements using customized methods and technology. For example, security client application from a bank for its customers storing certificates and their private keys.

Security requirements once specified by the organization are transformed into functional requirements and analyzed for alternative available solutions for their implementation. Options theory recommends to decompose technology (or available solution) and consider each part individually. This
helps to have a deep insight into the technology available, changing environment and the upcoming versions. Exploring alternatives for a requirement also provides the facility to specify appropriate solution. Options theory provides various options (shown in table 1) to manage uncertainty and mid course decision management. OBE executes appropriate option (from table 1) according to current state to manage uncertainty and changing requirements.

<table>
<thead>
<tr>
<th>Option</th>
<th>Description in OBE context</th>
</tr>
</thead>
<tbody>
<tr>
<td>Expansion option</td>
<td>Provides ability to expand the current security operations and choose among several strategies under the appropriate existing conditions.</td>
</tr>
<tr>
<td>Compound Option</td>
<td>Compound option refers to the case when the value of a strategic option depends on other option.</td>
</tr>
<tr>
<td>Sequential option</td>
<td>Continuation of the next available option depends on the results of the currently executing option and its result in a sequence.</td>
</tr>
<tr>
<td>Switching option</td>
<td>Providing rights and abilities to switch among various technologies, products, infrastructures or methods.</td>
</tr>
<tr>
<td>Abandonment Option</td>
<td>Exiting from the development cycle or leaving the current option, bearing penalties for the short period when the technology is under consideration.</td>
</tr>
<tr>
<td>Barrier option</td>
<td>Breaching artificial barrier, some parts of the technology could be refused at the beginning while other could be opted in.</td>
</tr>
<tr>
<td>Compound Expansion Options</td>
<td>Expanding services by branching out into relevant technologies, applications, or expanding vertically to opt for sub technologies.</td>
</tr>
<tr>
<td>Re-formulation option</td>
<td>If the certain option could not succeed, then it can be reformulated and considered again.</td>
</tr>
</tbody>
</table>

Table 1. Various Options and their description aligned to OBE context

For example, SHS system has some generic security requirements for example, secure end-to-end transmission, use established standards with industry acceptance and transport security using SSL at HTTP level among SHS nodes. SHS also emphasizes on adoption of evolving standards, therefore Governmental policies, technology advancements and new security measure could be treated as dynamically changing requirements for SHS infrastructure. OBE performs decision tree analysis for specifying security requirements and exploring their associated options. Referring to SHS generic requirement of end-to-end security, we name this requirement as R1. Exploring the options for R1, there could be two alternatives, (op1) Installing SSL-offloading devices in a PCI-card format [9] and (op2) Windows Integrated Security on IIS with Implementing Brokered Authentication [10]. Here Op2 has the compound expansion option with op2.1 and op2.2 as described below.

i) Option 1(op1) Installing SSL-offloading devices in a PCI-card format

ii) Option 2 (op2) Windows Integrated Security on IIS with Implementing Brokered Authentication

Option 2.1 (op2.1). Transport layer data confidentiality using HTTPS

Option 2.2. X.509 certificates and HTTPS

This particular scenario is depicted in figure 2 using decision tree.

![Decision tree representation for End to End Security requirements of SHS](image)

When some option is selected i.e. op1 and op2 in above mentioned example, it will be measured based on quality, appropriateness and security goals of the organization. Op1 failed or didn’t match with security objectives, it provided two alternatives either to reformulate it and consider this option again with new features or abandon it. Reformulation for op1 can also consider various other options from Table1. Op2 in the above example successfully met the requirement then the sub options op2.1 and op2.2 are executed in the same fashion and found as an appropriate solution. In figure 2, op2 provides abandonment option at each level. This indicates that OBE is ready to adjust novel technology or solution for end to end security requirement at any implementation level. Considering many alternative solutions for a requirement and choosing the appropriate one, helps to make evaluation as an improvement process.

OBE maintains an option card as a tool to keep track of each requirement and its associated options for future reevaluation to adjust uncertainty. Figure 3 shows option card for R1.
### Available Options

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
<th>Result</th>
<th>Comments</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Option 1</strong>&lt;br&gt;(op1)</td>
<td>SSL-offloading devices in a PCI-card format</td>
<td>Abandoned</td>
<td>Learning Logs</td>
</tr>
<tr>
<td><strong>Option 2</strong>&lt;br&gt;(op2)</td>
<td>Windows Integrated Security on IIS with Implementing Brokered Authentication</td>
<td>Executed</td>
<td>Met the requirements</td>
</tr>
<tr>
<td><strong>Option 2.1</strong>&lt;br&gt;(op2.1)</td>
<td>Transport layer data confidentiality using HTTPS</td>
<td>Compound expansion</td>
<td>Continued to the sub options</td>
</tr>
<tr>
<td><strong>Option 2.2</strong>&lt;br&gt;(op2.2)</td>
<td>X.509 certificates and HTTPS</td>
<td>Executed</td>
<td>Continue</td>
</tr>
</tbody>
</table>

### Requirement (R1)
End-to-end security for SHS web servers

### Description
SHS requirement for end to end security for their web servers are implemented by Windows Integrated Security on IIS with Implementing Brokered Authentication.

### Requirement Type & Stakeholder
Specific, Web Manager (This helps to keep track of change initiator)

### Date executed
18/03/2009

### Participants
OBE Leader, Requirement Engineer, Test Manager

### Corresponding section
Section (Module) name from the target of evaluation.

### Figure 3. Option card for requirement R1

2. **TOE Elicitation:** Target Of Evaluation is the system to be developed or evaluated. The boundaries of the TOE should be defined and agreed upon by the stakeholders from management, developers or evaluators. Once TOE (Whole-TOE) is specified OBE divides it into various sub systems (Sub-TOE) with respect to relevance, interdependency, service objectives etc. A Sub-TOE is further divided into sections where each section corresponds to one or more security requirement. The objective of dividing a large TOE into sub-TOE and sections is to employ options theory to their related requirement. It provides opportunity to precisely analyze each requirement and its alternatives as was explained in the case of end to end security requirement.

The complete system in notation can be expressed as follows. Whole-TOE = Sub-TOE1 + Sub-TOE2 + .......... Sub-TOEn

And a sub system as

Sub-TOE1 = Section1 + Section 2 ..... Section n

Completed sections can be considered for early evaluation and this helps to speed up the evaluation procedure. Referring to SHS example, the whole SHS system can be divided into sub-TOEs according to four perspectives, i.e., service, protocol, network and security. Considering SHS protocol perspective [15] the application layer has dependency on SHS layer and transport layer. It can be considered as one Sub-TOE with different sections based on application security requirements. Each section of SHS protocol perspective will be evaluated as an independent module. Whole-TOE, sub-TOEs and each section are described with the help of option card used to maintain the information about each level of the system. Figure 4 describes Whole-TOE of SHS Architecture.

### Option Card for W-TOE.

<table>
<thead>
<tr>
<th>Description</th>
<th>Sections</th>
<th>Comments</th>
</tr>
</thead>
<tbody>
<tr>
<td>SHS Architecture (Name of the W-TOE)</td>
<td>Section 8, section 10</td>
<td>Sub system to address SHS services perspectives. Refer to option card Sub-TOE1</td>
</tr>
<tr>
<td>Sub-TOE2</td>
<td>Section7, section9</td>
<td>Sub system to address SHS protocol perspectives. Refer to option card Sub-TOE2</td>
</tr>
<tr>
<td>Sub-TOE3</td>
<td>Section3, section5</td>
<td>Sub system to address SHS Network perspectives. Refer to option card</td>
</tr>
</tbody>
</table>

The complete system in notation can be expressed as follows. Whole-TOE = Sub-TOE1 + Sub-TOE2 + .......... Sub-TOEn

And a sub system as

Sub-TOE1 = Section1 + Section 2 ..... Section n
Sub-TOE system to address SHS security perspectives. Refer to option card Sub-TOE4

Description: Whole SHS system is divided into four Sub-Toes and their corresponding sections. Each sub-TOE has its own option card with section details. Every section is described with its own option card.

Version: 1
Date: 28/01/2009

Additional Information: Contains additional information about the product or system under evaluation.

Figure 4. Option card of Whole-TOE of SHS Architecture

Phase 3. Evaluation and Analysis

The next phase is evaluation and analysis using options theory. OBE recommends incremental iterative model for development and this helps for facilitator group to ensure authenticity of the product at each step. OBE evaluation process categorizes security test cases in four groups i.e. criticality, interdependence, completion and urgency (can be defined more). This helps to classify and prioritize tests to deploy option theory. Table 2 provides an example of criticality test cases [16] classification.

Table 2. Criticality tests cases classification for specific section

<table>
<thead>
<tr>
<th>Criticality. Test Cases</th>
<th>Description</th>
<th>Test Category</th>
<th>Test 1 Build Test</th>
<th>Ensuring application was built and installed successfully.</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
<td>Sub Tests</td>
<td>Test1.1 Test1.2</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Test 2 Smoke Test</td>
<td>Testing major functionality at high level that determines if further testing is possible</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>Test2.1 Test2.2 Test2.3</td>
</tr>
</tbody>
</table>

Each section is evaluated based on the selected “test group” from test cases customized for its evaluation. Compared to CC infrastructure that follows a long testing process and generates results at the end, OBE categorizes and prioritizes tests by providing flexibility to bypass unnecessary tests when a section doesn’t meet the basic test requirements. It helps to avoid unnecessary delays and proceed to other sections for evaluation. For example, Section 1 in Figure 5 is authorization of online users of SHS environment and it fails on criticality test. This brings in two options either to reformulate test and consider again or abandon it and submit logs to developers. OBE will provide option to bypass interdependency tests (Test 2 and test 2.1) if the abandon option is executed for test 1. This helps to avoid unnecessary evaluations and consider the other sections in the meantime.

Figure 5 depicts the option tree analysis of test cases for section 1.

Figure 5. Option Tree analysis of Section 1 for evaluation

It has been observed during SHS evaluation that some components of the system are readily available or have less interaction with the development environment i.e. users, various specification documents and sometime hardware. OBE emphasizes on working closely with developers and evaluators to speed up evaluation by considering those components as early evaluation. IT Product evaluation is performed normally which has less
impact on the product improvement [8]. OBE emphasizes on making evaluation as an improvement process and this could be achieved by taking evaluation iteratively side by side with the development process and as maintenance after development. OBE recommends evaluation as an ongoing task to adjust uncertainty issues in IT infrastructure. There could be two alternatives to achieve this goal i.e.

i) If the product is delivered where the customer is not authorized to alter the product. Dynamic requirement management and reevaluation is done when needed by the vendor as maintenance task.

ii) If the product is developed and delivered to customer and the facilitator group is deployed into the organization the product is evaluated periodically to streamline the changing requirements.

5. OBE Analysis with SHS Example

SHS architecture is developed and mainly controlled by VERVA to keep track its work processes. It has a continuous process of upgrading and open to new technologies that appears with due time. One time evaluation of such a system would not be very useful as it is continuously being updated and prone to new threats and vulnerabilities. OBE’s power of continuous evaluation for SHS architecture was beneficial. Various stakeholders for SHS include, VERVA as controlling authority, development team from VERVA, evaluation team from KTH3 and governmental organizations as end users. Stakeholders are further classified into various roles and SHS security requirements are streamlined with sections where each section exhibits one or more stakeholder requirements and vice versa. OBE maintains SHS’s already evaluated components using options card. For newer component or technology, the only needed evaluation will be the new technology or the interacting ends of these (already evaluated) components.

Governmental organizations using SHS as a communication medium are able to adjust dynamically changing security requirement that can be analyzed using OBE. This provides flexibility to SHS architecture to explore and execute appropriate options more confidently. Ordinarily technology is adopted and then explored for vulnerability in a particular system. OBE provides the opportunity to evaluate the technology prior to its adoption.

6. Conclusion & Future Work

Security evaluation of IT products is considered significantly important for the organizations relying on IT infrastructure. Novel threats are continuously appearing and making IT an uncertain infrastructure. Careful evaluation of such infrastructure is inevitable. CC is an established Method for evaluation of IT products but it is considered as cumbersome and resource hungry procedure. Moreover CC evaluated products become obsolete due to dynamically changing security requirement of the organization due to uncertain IT infrastructure. There is a need for an infrastructure that could cope with dynamically changing security requirement and make IT products more reliable for an organization. We have introduced a method Options Based Evaluation (OBE) to address uncertainty issues in IT, dynamic security requirement management and speed up the evaluation process. The method is derived from an established methodology options theory from corporate finance and has numerous success stories to deal uncertainty issues in various domains. Options theory provided strategic guidance to target uncertainty issues in IT infrastructure. OBE provides the flexibility to explore various alternatives for a solution and evaluate the technology prior to its adoption. It also provides guidance to indulge evaluation in development as an ongoing process for the organization to get efficient results. Evaluation can be performed within the organization or from external experts. In this paper, we presented OBE phases and steps to perform option based evaluation with some examples from the SHS system. We will come up with the study of detailed SHS analysis using OBE methodology in future.

7. References


[19] RICK KAZMAN, Mark Klein, Designing and Analyzing Software Architectures using ABASs , ICSE 2000 Limerick Ireland Copyright ACM 2000 1-58113-206-9/00/6

