Global Journal of Enterprise Information System

July 2010-Dec 2010

Volume-2 Issue-2

Security Threats in E-Business with Safety and Dependability

Narendra Kumar Tyagi

Asstt.Professor,DCE,Gurgaon,Haryana, India

narendratyagi21@gmail.com

ABSTRACT

Security is the main considerable part for any and every architectural quality. Critical software must be safe, secure, and dependable. Confidentiality and availability constitute part for measurement of quality consideration along with integrity. Security and most important dependability are particularly the essential part of qualities while dealing with threats in e-business. Architectural tactics, or architectural design decisions, that enhance one aspect of dependability can decrease security and vice versa. The quality attributes are measured on various scales of references. These scales are sometimes not quantitative. This makes it multi-scale problem. This paper proposes a qualitative approach to manage the transactions and exchange among the attributes used to define security threats in e-business.

KEYWORD

Durability	Confidentiality
Interoperability	System Quality
Soft Goals	Grap3

Preface

To support products security, addressing the functional and non-functional requirements of e-business, a well definition of system architecture is required. There is requirement for quality-driven techniques for explicitly considering non-functional quality attributes. Techniques described by **[Kazman[i], 2004]** are used to identify the desired quality attributes of a system. Designing the architecture with various quality attributes interacting with each other, is very hard. This is because an architecture decomposition that boosts one attribute may disgrace another. While managing the tradeoffs among qualities, it is hard for several reasons. The quality attributes involved in a particular system are not measured quantitatively, though others are quantitative. For example, security is not measured quantitatively in e-business. Many reasoning frameworks assist the architect in quantitatively analyzing the quality attributes like performance. Few techniques for qualitatively represented attribute reasoning like security are available. This paper presents a qualitative approach to reasoning about security at the architectural stage.

2. Traditional Approaches with Deficiencies to modern approaches

Producing correct software, according to **[Iwasaki,1997]**, needs three approaches process, product and testing. Process approach includes personnel certification with assessments of the software development process. Product approach includes going through the real software product and concerned artifacts by inspections, reviews, tracing, etc. Testing product is reviewed by working the software in its real platform. It is important as inspections and proofs make simple assumptions about the platform. For the correctness **[Kazman[ii], 2004]]** provides a good discussion of practical approaches. There are three more approaches: manage complexity, manage change, and manage rationale. Complexity has an inverse relationship to correctness. It is established that up to 90% of project effort goes into maintenance for corrections and enhancements. Heaping changes upon changes creates fragile software. Modifying a legacy system needs attest design rationale. In designing with safety the rationale behind design decisions becomes more important in case security, safety and dependability otherwise it may lead dangerous situations of maintenance of e-business. Zero defect approach is the critical applications **[John D. McGregor, 2007]**, against a reliability growth to eliminate faults in early stages maximization of process and product methods. There is a requirement for the defensive program to guide design of dependable software, abstraction hiding, fault tolerance and integrity. These may require formality and abstraction for creation of right things and recovery from wrong things.

2.1 Dependability is the trust justified on a computer system. It includes the qualities of safety, reliability, integrity, availability, confidentiality with maintainability **[Algirdas Avizienis, 2004]**. This paper , on designing dependable systems, identified four interactions among the qualities within dependability involving qualities related to security threats in E-Business, these are –

2.1.1 Safety vs. Confidentiality **[Schneier, B, 2003]**

2.1.2 Safety vs. Integrity **[Schneier, B, 2003]**

2.1.3 Availability vs. Confidentiality **[Warns, 2005]**

2.1.4 Availability vs. Integrity **[Warns, 2005]**

As shown in the Fig:2.1.1

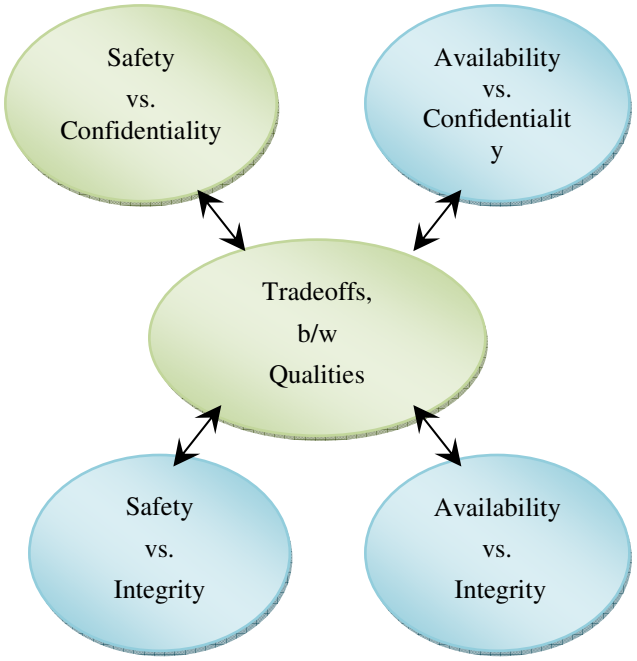

Fig: 2.1.1 Dependability involving qualities related to security threats in e-business

2.2 The tradeoffs, between qualities while designing a dependable system, must be evaluated as qualities are defined in terms of other qualities. These qualities are measured on different scales, some of which are not quantitative, are not readily handled by existing techniques. Security is not measured on a scale, a goal based scale is used to support design reasoning **[John D. McGregor, 2007]**. The goals are called softgoals because there is no precise, objective definition of the goal for satisfying them. A softgoal **[Chung, L.K. Nixon, B. and Yu, E, 2000]** will not capture the level of detail found in performance models but it will provide qualitative "indicators" to guide the architect.

3. Qualitative Reasoning for Security

3.1 Qualitative techniques adopt some type of ordinal scale because Qualitative reasoning **[Iwasaki, 1997]** provides a means of making decisions involving attributes that cannot be expressed quantitatively.

The reasoning rules use –

3.1.1 a current position on an ordinal scale

3.1.2 an indication of whether the attribute is changing its value .

3.2 Security attribute of a software might be rated on an ordinal scale as "very" secure. Qualitative reasoning supports building models to represent these relationships between qualitative values and support inferences about how the values change over time and how they cause other values to change. The model must consider the direction of change for each quality and the inequality relationship that exists among tactics tactic influencing the qualities comprising security. Many strategies are considered to improve confidentiality, integrity, security **[Steel, C. Nagappan, R. and Lai, 2005]** and availability etc. Net effect of these strategies can not be assessed on the degree to which the resulting system is secure since relative magnitudes of the "-"(weak satisfying) effect of replication and the "+" (weak) effect of a validator can not be compared.

3.3 The complexity in reasoning about these strategies is present partially because these attributes are not quantitative and partially because the measures are on different scales. It can be overwhelming to keep track of how each strategy influences each sub-quality of security threats and how each strategy relates to other strategies. For this reason, we are developing a modeling technique to assist the architect in reasoning about security threats in E-Business.

4. Satisfying security requirements: An Example

4.1 The qualities that are of most important to web-service are the following:

4.1.1 Confidentiality
4.1.2 Integrity
4.1.3 Reliability
4.1.4 Availability

Fig: 4.2 Software Qualities in E-Business

4.2 This paper chooses two strategies the first one implementing security and the second one introducing replication. Figure 4.2 describes influence of above said strategies on confidentiality and integrity in different directions. Any how the confidentiality and integrity of the overall system would have decreased after the application of both the strategies, it is due to an inequality relationship between the strategies (it was determined that "replicated elements %" has a greater impact on confidentiality and integrity than "security %").

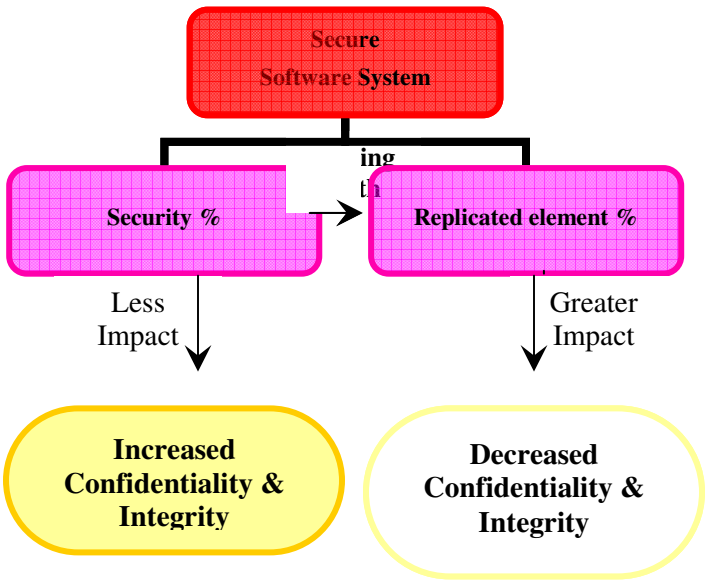

Fig: 4.2.3

4.3 The software architect is intended to take a decision on the inequality relationships between strategies which change

depending on the method of application. Garp3 is a workbench for building, simulating, and inspecting qualitative models. Garp3 is implemented in SWI-Prolog and seamlessly integrates three previously developed software components, including: Garp2 for simulating models, Homer for building models, and VisiGarp for inspecting simulation results. Integrating these tools has led to one new tool that incorporates all of the original functionalities, and thus incorporates the advantages of each tool, but also adds interoperability and an easy to use uniform user interface. Garp3 uses a diagrammatic approach for representing model content, and graphical buttons to communicate the available user options and manipulations. Garp3 can be freely downloaded and used. This paper uses Garp3 tool for generating all possible cases if no inequality is specified. To facilitate the application of qualitative reasoning to security a qualitative model of security is needed which describes the influences of strategies to the quality standards of the security. It will provide a knowledge base for qualitatively reasoning about security threats in e-business and also contain the necessary data for reasoning about security in a broader context like dependability and availability.

5. Conclusion

This paper is the hard work in the direction of establishment that simple models are always superior and supporting in decision making and for prediction purposes. The research **[Hastie, R. and Dawes, 2001]** shows that qualitative research methods reasoning for security threats in e-business are not accurate and simple though they appear so in comparison of simple modeling **[simulation model, 2005]**. This research paper presented the influence of dependability on security architectural strategies and influence of security architectural strategies on dependability. This paper elaborates a reasoning methodology of selecting architectural strategies for the software architect to get quality of system. This is also established that some security strategies register resistances against dependability targets of system. Through this paper it is proved that Garp3 tool incorporates all of the original functionalities, and thus incorporates the advantages of each goal, but also adds interoperability **[Narendra Kumar Tyagi , 2009]** and an easy to use uniform user interface.

References

i. Kazman, R. Klein, M. and Clements, P. *"ATAM: Method for Architecture Evaluation"*. CMU/SEI-2000-TR-2004.
ii. Algirdas Avizienis, Jean-Claude Laprie, and Brian Randell. Fundamental Concepts of Dependability.IEEE-CSP-2004
iii. Chung, L.K. Nixon, B. and Yu, E. "Non-functional Requirements in Software Engineering", Kluwer Academic Publishers, 2000.
iv. Hastie, R. and Dawes, RM. "Rational Choice in an Uncertain World: The Psychology of Judgment and Decision Making", Sage Publications Inc , 2001 Thousand Oaks CA.
v. Iwasaki, Y. Real-world applications of qualitative reasoning, Expert, IEEE, 1997, pp. 16—21.
vi. John D. McGregor and Tacksoo Im. A Qualitative Approach to Dependability Engineering, Proceedings of Dahstuhl Seminar #07031, January 2007.
vii. Schneier, B. Beyond Fear: Thinking Sensibly About Security in an Uncertain World, Copernicus Books, 2003.
viii. Warns, Timo Engineering Intrusion-Tolerant Software Systems. In: Dagstuhl Workshop, 22 25 May 2005, Dagstuhl, Germany.
ix. Steel, C. Nagappan, R. and Lai, R. Core Security Patterns: Best Practices and Strategies for J2EE(TM), Web Services, and Identity Management, Prentice Hall, 2005.
x. http://metacourses.org/simulationmodeling/glossary/
xi. Narendra Kumar Tyagi, research paper "**e-Bus : web services"** in International Conference **"icsci-2009"** held in Hyderabad on 7,8,9,10 Jan 2009