Journal of Theoretical and Applied Information Technology
10th May 2015. Vol.75. No.1

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

# EVALUATION OF SECURITY IN SOFTWARE ARCHITECTURE USING COMBINATION OF ATAM AND STRIDE

**PRAJNA DESHANTA IBNUGRAHA*, RIDI FERDIANA, SUHARYANTO, PAULUS INSAP SANTOSA**

Engineering and Information Technology Department, Gadjah Mada University ,Yogyakarta, Indonesia
Email : prajna.deshanta.i@mail.ugm.ac.id

* Applied Science Department of Telkom University, Bandung, Indonesia

**ABSTRACT**

In this time, security is important thing that must be included when develop software because it has large effect on continuity of software and business. Therefore, security evaluation is required as a phase in software architecture development. Security evaluation is useful to minimize future problems about security. The objective of this study is to simplify evaluation security attribute using ATAM and STRIDE. ATAM is used to analysis and evaluate security of software architecture. The output of ATAM is scenarios of quality attribute. Classification of security threat can be used to simplify scenarios building and test the scenarios. The result of experiment in case study show that security problems can be discovered using analysis and evaluation phase.
**Keywords:** *evaluation, ATAM, STRIDE*

## 1. INTRODUCTION

Software build to help human to finish the job easily. To build good software, developer needs to think about norms of Software Life Cycle in software architecture [1].

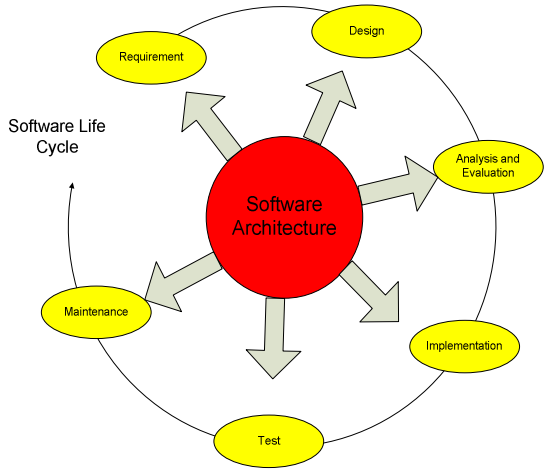


*Figure 1. Software Life Cycle in Software Architecture*

However, developers often overlook norms of Software Life Cycle. The process of software building often ignore the analysis and evaluation phase. Whereas it is very important because in that phase quality of software architecture can be seen based on Quality Attribute (QA) [2]. Some Quality Attributes defined in the standard ISO 9126 [3]. An good software architecture is not only able to function properly but also consider security elements like confidentiality, integrity, and availability[4].

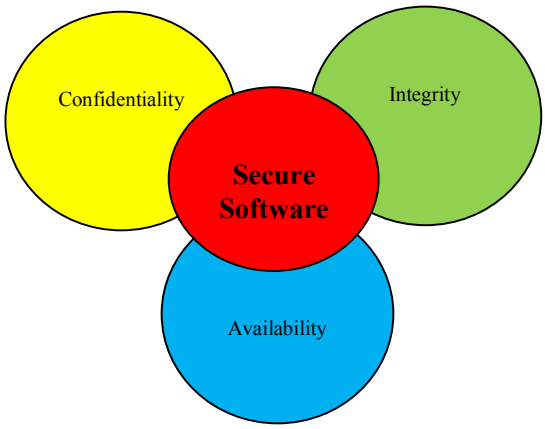


*Figure 2. Elements of secure software*

Security evaluation of software architecture becomes important because continuity of the software and business depend on it. Analysis and evaluation phase of software architecture can be done using methods below [1]:

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

- SAAM (Scenario-based Architecture Analysis Method, or called Software Architecture Analysis Method)
- ATAM (Architecture Trade-off Analysis Method)
- ALPSM (Architecture Level Prediction of Software Maintenance)
- SAEM (Software Architecture Evaluation Model)
- PASA (Performance Assessment of Software Architecture)
- ARID (Active Reviews for Intermediate Designs)
- CBAM (Cost-Benefit Analysis Method)

This study focuses in security attribute and uses ATAM as evaluation method because ATAM has capabilities to :

- assess the consequences of architectural decisions based on quality attribute to business goals
- discover risks created by architectural decisions in the system

STRIDE is method to clasify security threat that required by this study to assess quality of security in software. STRIDE consists of : Spoofing, Tampering, Repudiation, Information disclosure, Denial of service, Elevation of priviledge

In previous research, the evaluation of the security attribute to use ATAM focus on developing Quality Attribute Utility Tree and Quality Attribute Scenarios by involving elements of security (confidentiality, integrity and availability) [5] [6]. The problem of ATAM is lack of testing method for Quality Attribute Scenarios. Therefore, this study involves STRIDE method to test security scenarios from ATAM output.

## 2. METHODS

In ATAM, investigation and analysis phase consists of steps below :

1) Indentify Quality Attribute Utility Tree (QAUT)
Security attribute is compiled by two security elements, namely confidentiality and integrity.

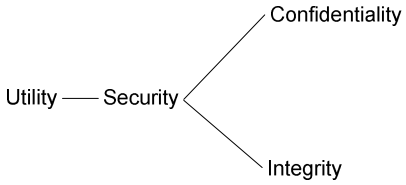


*Figure 3. Utility Tree of Security Attribute*

2) Identify Quality Attribute Scenarios (QAS)
The simple form of Quality Attribute Scenarios consists of stimulus, environment and response [7][8]. Quality Attribute Scenarios can be formed as Use Case Scenario, Growth Scenario or Exploratory Scenario [9]. Scenarios used in this study are shown below :

- Under normal condition, when user accesses information in the application control panel, it should be authenticated.
  - Stimulus : user accesses information in the application control panel
  - Environment : normal condition
  - Response : it should be authenticated

- Under normal operation, when invalid user accesses database information, it should be denied
  - Stimulus : invalid user accesses database information
  - Environment : normal operation
  - Response : it should be denied

- Under normal operation, only legal administrator can change information and application grants access to legal administrator.
  - Stimulus : only legal administrator can change information
  - Environment : normal operation
  - Response : application grants access to legal administrator.

- Under normal operation, only legal administrator can change indentity of registered user and application grants access to legal administrator.
  - Stimulus : only legal administrator can change indentity of registered user.
  - Environment : normal operation.

Journal of Theoretical and Applied Information Technology
10th May 2015. Vol.75. No.1

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

- Response : application grants access to legal administrator.

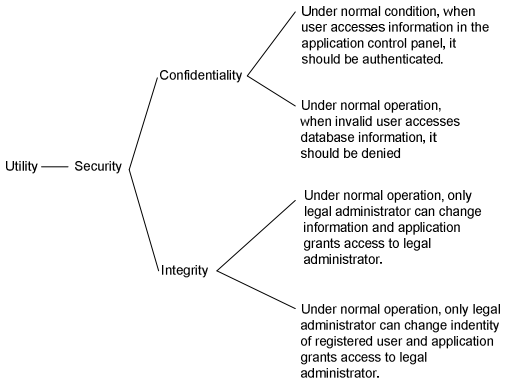


*Figure 4. Security Attribute Scenarios*

3) Analysis of Quality Attribute Scenarios based on priority.
Priority of utility tree consists of 2 dimensions that describe condition below [8]:

*Table 1. Grade description of utility tree dimensions*

| Dimension | Grade | Description |
|---|---|---|
| Importance for the success of system | High (H) | If the scenario can't be complete, the system will be useless |
| | Medium (M) | Completing the scenario will be highly desirable for the system. |
| | Low (L) | Completing the scenario will be nice feature for the system |
| Difficulty to achieve | High (H) | The developers have no idea to complete the scenario |
| | Medium (M) | It will be difficult and needs more time to complete the scenario, but develovers generally understand the method to solve the scenario |
| | Low (L) | easy to complete the scenario |

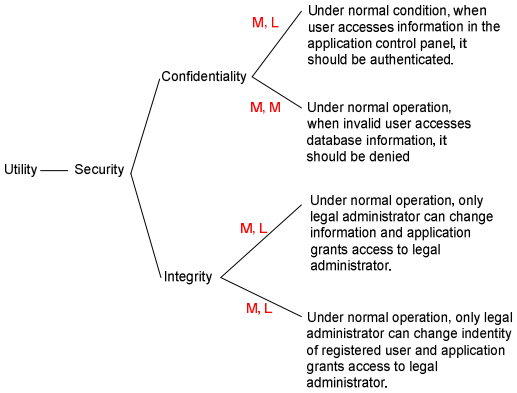


*Figure 5. Priority of security attribute scenarios*

After scenarios are created, then testing needs to be done. Spesific threat is used to simplify the testing. It is based on relation between type of threat in STRIDE and security control that can be shown below [10] :

*Table 2. Type of Threat vs Security Control*

| Type | Security Control |
|---|---|
| Spoofing | Authentication |
| Tampering | Integrity |
| Repudiation | Non-Repudiation |
| Information Disclosure | Confidentiality |
| Denial of Service | Availability |
| Elevation of privilege | Authorization |

## 3. EXPERIMENTAL DETAILS

Experiment is done to one of tourism website in Indonesia. Information Disclosure and Tampering are type of threat that used to test website security. It is based on ATAM scenarios above.

➢ Confidentiality
Type of threat : Information Disclosure
Result :
- Attacker can access information that stored in database through SQL injection bug [11].
- Attacker can find administrator account information

admin:
e10adc3949ba59abbe56e057f20f883e

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

- Integrity
  Type of threat : Tampering
  Result :
  - Attacker can crack administrator password using dictionary attack [12][13]

    e10adc3949ba59abbe56e057f20f883e:123456

  - Attacker can login to application control panel and has administrator authorization.

## 4. RESULT AND DISCUSSION

Result of experiment in case study can be shown below :

| Security Element | Confidentiality |
|---|---|
| Quality Attribute Scenarios | Under normal condition, when user accesses information in the application control panel, it should be authenticated |
| Scenario Testing Method | Information Disclosure |
| Result of case study | Invalid user can accesses information that stored in database throught SQL injection bug |

| Security Element | Integrity |
|---|---|
| Quality Attribute Scenarios | Under normal operation, only legal administrator can change information and application grants access to legal administrator. |
| Scenario Testing Method | Tampering Data |
| Result of case study | Attacker can decrypt administrator password and login to application control panel as administrator. So attacker can change information and content |

| Security Element | Confidentiality |
|---|---|
| Quality Attribute Scenarios | Under normal operation, when invalid user accesses database information, it should be denied |
| Scenario Testing Method | Information Disclosure |
| Result of case study | Invalid user can accesses database information throught SQL injection bug |

| Security Element | Integrity |
|---|---|
| Quality Attribute Scenarios | Under normal operation, only legal administrator can change indentity of registered user and application grants access to legal administrator. |
| Scenario Testing Method | Tampering Data |
| Result of case study | Attacker can decrypt administrator password and login to application control panel as administrator. So attacker can change indentity of registered user |

*Figure 6. Relation of elements*

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

Figure 6 shows relation between security element, quality attribute scenarios, scenario testing method and result of case study. ATAM and STRIDE have capability to discover future problems [14][15]. Threat classification of STRIDE can facilitate to find critical security. In case study, bug of SQL injection is found in application because security evaluation phase in software architecture was not done by developer. Whereas security has large effect on continuity of the software and business.

## 5. CONCLUSION

Norms of Software Life Cycle in software architecture is important to be considered as a guidance for developers to build good product. Analysis and evaluation phase needs to be done because it can help to minimize risks of future problems and keep continuity of the software and business. Security attribute must be included in analysis and evaluation phase to keep confidentiality and integrity of information in application. ATAM and STRIDE are complementary methods that can be used to simplify evaluation of software architecture. ATAM is used to make evaluation scenarios and STRIDE is used to validate the scenarios. Based on result experiment, security problems of website can be defined with ATAM and STRIDE.

## REFERENCES :

[1] Qin, Z., Xing, J., Zheng, X. "Advanced Topics In Science And Technology In China : Software Architecture". Springer, 2007.

[2] Lee, J., Kang, S., Kim, C. "Software architecture evaluation methods based on cost benefit analysis and quantitative decision making". Springer Science + Business Media, LLC, 2008.

[3] Välimäki, A., Vesiluoma, S., Koskimies, K. "Scenario-Based Assessment of Process Pattern Languages". Springer-Verlag Berlin Heidelberg pp. 248-249, 2009.

[4] Howard, M., LeBlanc, D. "Writing Secure Code Second Edition". Microsoft Press, 2003.

[5] Raza, A., Abbas, H., Yngström, L., Hemani, A. "Security Characterization for Evaluation of Software Architectures using ATAM". IEEE, 2009.

[6] Reza, H., Helps, W. "Security Trade-off Analysis of Service-oriented Software Architecture", World Journal of Computer Application and Technology pp. 110-120, 2013.

[7] Mälardalen University. "CDT413: Advanced Software Engineering Software Architecture Evaluation". Mälardalen University

[8] Kazman, R., Bass, L., Klein, M., Lattanze, T., Northrop, L. "A Basis for Analyzing Software Architecture Analysis Methods". Software Quality Journal, 13, pp. 329–355, Springer Science + Business Media, Inc. Manufactured in The Netherlands, pp. 337-338, 2005.

[9] Gagliardi, M., Wood, B. "Architecture Evaluation and Quality Attribute Specification for Software, Systems and SoS Architectures". Three Rivers Chapter of INCOSE, 2011.

[10] OWASP. "Application Threat Modeling". a Creative Commons 3.0 License. [Online:https://www.owasp.org/index.php/Application_Threat_Modeling]. [Accessed : 06-11-2014]

[11] Shar, L.K., Tan, H.B.K. "Defeating SQL Injection". IEEE Computer Society, pp. 69-77, 2013.

[12] Thangavel, T.S., Krishnan, A. "Provably Secured Two Server Hash Password Authentication". J Journal of Theoretical and Applied Information Technology, pp. 68-75, 2010.

[13] Jali, M.Z., Ismail, S., Abdullah, Z.H,. "An Assessment on The Password Practices Among Students". Journal of Theoretical and Applied Information Technology, pp. 840-848, 2014.

[14] Carnegie Mellon University Pittsburgh. "Architecture Tradeoff Analysis Method$^{SM}$(ATAM$^{SM}$)". Software Engineering Institute Carnegie Mellon University Pittsburgh, 2002.

[15] Koscho, J.W., Ries, W. "Identifying and Proactively Managing Architecture Risk". ICSE Workshop on Leadership and Management in Software Architecture (IEEE), 2009.