ISSN 1598-0170 (Print)
ISSN 2287-1136 (Online)
http://www.jksii.or.kr

기능주도개발 Agile 방법을 사용할 때의 안전한 소프트웨어 개발에 관한 문헌연구☆

A Systematic Literature Review on Secure Software Development using Feature Driven Development (FDD) Agile Model

아딜라 알바인[1] 임란 가니[1] 정 승 렬[2*]
Adila Firdaus Arbain Imran Ghani Seung Ryul Jeong

요 약

Agile 방법론은 시간적 제약하에서도 효율적인 개발 프로세스로 빠르게 제품을 완성할 수 있는 방법으로 알려져 있다. 하지만 scrum, XP, DSDM 등과 같은 여타 Agile 방법들처럼 기능주도개발 (FDD) Agile 방법도 보안요소의 불가용성으로 인해 비판을 받고 있다. 이러한 이슈를 보다 자세히 살펴보기 위해 본 연구는 2001년부터 2012년사이에 나타난 연구들에 대한 체계적인 문헌연구를 수행하였다. 본 연구 결과, 현재 FDD 방법은 안전한 소프트웨어 개발을 부분적으로 지원하고 있는 것으로 나타났다. 하지만 안전한 소프트웨어 사용에 관한 상세한 정보가 문헌에 거의 나타나고 있지 않은 것으로 보아 이 분야에 대한 연구 노력은 거의 없어 보인다. 따라서 현재의 5단계 FDD 방법은 안전한 소프트웨어 개발에 충분하지 않음을 알 수 있고 결국, 본 연구는 FDD 방법에서 보안에 기반을 둔 새로운 수행 단계와 프랙티스가 제안될 필요가 있음을 보여준다.

☞ 주제어 : Agile 방법론, 보안, 소프트웨어 공학, 기능주도개발

ABSTRACT

Agile methodologies have gained recognition as efficient development processes through their quick delivery of software, even under time constraints. However, like other agile methods such as Scrum, Extreme Programming (XP) and The Dynamic Systems Development Method (DSDM), Feature Driven Development (FDD) has been criticized due to the unavailability of security elements in its twelve practices. In order to examine this matter more closely, we conducted a systematic literature review (SLR) and studied literature for the years 2001-2012. Our findings highlight that, in its current form, the FDD model partially supports the development of secure software. However, there is little research on this topic, as detailed information about the usage of secure software is rarely published. Thus, we have been able to conclude that the existing five phases of FDD have not been enough to develop secure software until recently. For this reason, security-based phase and practices in FDD need to be proposed.

☞ Keyword : Agile Methodology, Security, Software Engineering, Feature Driven Development

1. Introduction

Agile methodologies have had an important impact on software development practices in recent years [1]. A significant amount of positive feedback has been noted from the organizations [2, 3] that practice agile methods. Their statements [4, 5] suggest that agile methods help during the software development process by emphasizing rapid development. This, along with an ability to quickly respond to changes in requirements, leads to a high degree of customer satisfaction. Agile methods are more flexible and help to reduce iterations. However, they need to follow several rules related to the agile manifesto, including those

1 Faculty of Computing, Dept. of Software Engineering, Universiti Teknologi Malaysia, Skudai, Malaysia
2 Graduate School of Business IT, Kookmin University, Seoul, Korea.
* Corresponding author (srjeong@kookmin.ac.kr)
[Received 28 October 2013, Reviewed 4 November 2013, Accepted 18 December 2013]
☆ This research was supported by a research grant from Ministry of Science, Technology and Innovation (MOSTI) at Vot: 4S028, at Universiti Teknologi Malaysia.
☆ A preliminary version of this paper appeared in APIC-IST 2013, Aug 12-14, Jeju Island, Korea. This version is improved considerably from the previous version by including new results and features.

concerning less documentation and team member interactions, which provide for appropriate communication with customers and other users.

On the other hand, some researchers and practitioners [4, 6, 7, 8] have noted that, in software development, rapid development and changing requirements are not the only issues. They highlighted another critical software problem – software security [9]. In other words, the rapid development of software that is secure. Unfortunately, agile methodologies such as Scrum, FDD, DSDM [96] and XP [97]do not suggest or include security elements in their models. In general, the exclusion of security elements from the agile development process creates vulnerable software. This leads to reiteration in order to make the software secure, which affectsthe project timeline, significantly raises costs, and negatively affects customer satisfaction, which ultimately diminishes the notion of such a methodology being "agile."

In this paper, we explore both points of view in detail. We also present our own point of view on the existing agile models, methods and systems that have integrated security into FDD.

The objectives of this paper are:

1. *To review the possible software security issues that are raised while using FDD practices.*
2. *To identify whether it is feasible to integrate security elements into FDD as a whole.*

The paper has been organized [10] asfollows: Section 2presents works relevant to the paper. Section 3covers how the SLR procedure has been used. Section 4is a report about the research results, while section 5 is a discussion of the research results. Finally, section 6 is the conclusion, and suggests possible future outcomes.

2. Related Works

As the paper focus on agile methodology, so it is appropriate to provide brief introduction about the existing FDD method.

2.1 Feature Driven Development (FDD)

FDD was initially devised by Jeff De Luca, to meet the specific needs of a 15-month, 50-person software development project at a large Singapore bank in 1997. Jeff De Luca delivereda set of five processes that covered the development of an overall model and the listing, planning, design and building of features (Fig. 1).

2.1.1 Develop overall model

The software project started with a high-level walkthrough of the scope of the system and its context. Next, detailed domain walkthroughs were held for each modeling area. Domain area models are merged into an overall model, and the overall model shape is adjusted along the way.

2.1.2 Build Feature List

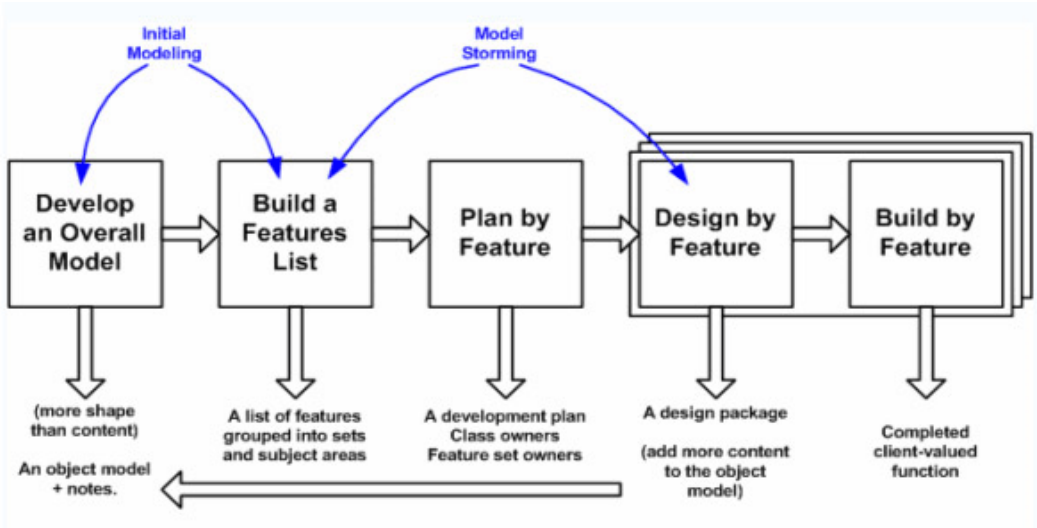
The knowledge that was gathered during the initial modeling was used to identify a list of features. This was done by functionally decomposing the domain into subject areas. Subject areas each contain business activities, the steps within each business activity formed the categorized feature list. Features in this respect were small pieces of client-valued functions expressed in the form "<action> <result> <object>", for example: 'Calculate the total of a sale' or 'Validate the password of a user'. Features should not take more than two weeks to complete, else they should be broken down into smaller pieces.

2.1.3 Plan by feature

After the feature list had been completed, the next step was to produce the development plan. Class ownership has been done by ordering and assigning features (or feature sets) as classes to chief programmers.

2.1.4 Design by feature

A design package was produced for each feature. A chief programmer selected a small group of features that are to be developed with in two weeks. Together with the corresponding class owners, the chief programmer worked out detailed sequence diagrams for each feature and refines the overall model. Next, the class and method prologues are written and finally a design inspection is held.



(Figure 1) Feature Driven Development Model (Source: Skillresouce [100])

2.1.5 Build by Feature

After a successful design inspection a per feature activity to produce a completed client-valued function (feature) is being produced. The class owners develop the actual code for their classes. After a unit test and a successful code inspection, the completed feature is promoted to the main build.

The first process is heavily influenced by Peter Coad's approach to object modelling [98]. The second process incorporates Peter Coad's ideas of using a feature list to manage functional requirements and development tasks. The other processes and the blending of the processes into a cohesive whole is a result of Jeff De Luca's experience. Since its successful use on the Singapore project, there have been several implementations of FDD. The description of FDD was first introduced to the world in the book Java Modeling in Color with UML[98] by Peter Coad, Eric Lefebvre and Jeff De Luca in 1999. Later, in Stephen Palmer and Mac Felsing's book A Practical Guide to Feature-Driven Development[99], a more general description of FDD was given, as decoupled from Java modeling.

However, the introduction of security in agile methods started a few years back, but in this paper, we would like to focus on security elements that could enhance security quality

after going through the FDD process. Agile methods such as Scrum [11] and XP have introduced new models that are equipped with security [12, 13] and security itself has its own model [14-18]. However, since there are only a few studies related to FDD, it seems that there is still much progress to be made in the development of a secure FDD model.

[19, 20] and [21] provided examples of SLR. However, unlike most of the previous work, this paper will cover how security can be embedded in Feature Driven Development and how it will be used in real world software development to produce more secure systems.

3. Review Process

SLR guidelines for SE proposed by [22] have been followed for this study. The definition of this process is to identify, assess and interpret all relevant and available research proofs in order to be able to provide answers to the research questions proposed.

3.1 Research Questions

Table I shows the criteria and scope of the research

questions structure, which is the *Population, Intervention, Comparison, Outcomes,* and *Context* [PICOC] structure.

(Table 1) Summary of PICOC

Criteria	Scope
Population	Papers proposing models or frameworks for FDD and Security
Intervention	Security, FDD
Comparison	Secure Agile Model
Outcomes	Suggest how security can be injected into the FDD model
Context	Secure FDD model

Based on Table 1, the research questions are:

[Q1] How many studies mentioned security in FDD and when were the initial and latest studies?

[Q2] Were any frameworks or models proposed for FDD and security?

[Q3] How is the integration between Security and FDD when it comes to a real life software development environment?

[Q4] How are we going to measure Security and FDD integration after the study?

3.2 Search Strategy

The strategy that was used to construct the search strings was based on [20], which is as follows: (1) Major terms are derived for use in the review questions [for example: it will be based on population, intervention, outcome and context] (2) Known keywords mentioned in the articles are listed(3) The use of Boolean OR to discover synonyms, alternative spellings or related keywords such as abbreviations (4) The use of Boolean AND in order to connect the main terms to the outcome, intervention and population.

Therefore, the complete search strings used for this paper are as follows:

[*Agile* OR *Agile Methodology*] AND [*Software Security* OR *Security*] AND [*Feature driven development* OR *FDD*].

Afterwards, in order to discover information regarding SE methodologies, the search strings above have been modified as follows:

[*Software Engineering* OR *SE*] AND [*Agile* OR *Agile Methodology*].

The research paper foundwere classified according to the publication type. Later, different search methods were employed by manually filtering the conferences, journals, books, and websites by checking each of the publications that were published in the year 2007 and later.

3.3 Selection Criteria

The inclusion criteria for this paper include studies that primarily target Software Engineering and focus on security aspects and the FDD methodology. The priority hierarchy from "most important" to "least important" in regards to publication type is as follows: Journals > Conference Proceedings > Books > Websites > White Papers

In addition, the research paper found must include the following criteria in order to be included in this paper

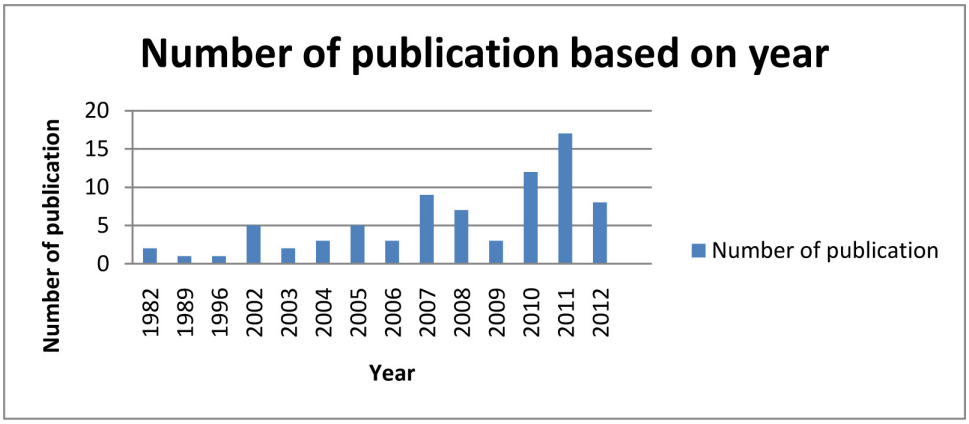
- Indexed by known databases such as IEEE Xplore, Springer, SpringSim, ACM, etc.
- Written in English
- Subjects covered must include Software Engineering, specifically in the Security or Computer Sciences field

3.4 Qualitative Analysis

To speed up the data extraction process, a form was designed. It was used to gather proof related to the research question and as a qualitative measurement for the study. Table 2 shows the questions that were asked after the keywords chosen for this study were analysed.

(Table 2) Questions

Question	Answer
Q1. Was the article about Agile and FDD specifically?	Yes/No
Q2. Was Security mentioned in the paper?	Yes/No
Q3. Did the paper make mention of a quantitative measurement regarding the effectiveness of the study?	Yes/No/Partial
Q4. Will the paper contribute to the research conducted?	Yes/No/Partial



(Figure 2) Number Of Publications

4. Results

4.1 Appendix A Finding

Appendix A shows the results of the search procedure. Initially, we identified 98 papers. However, after completing qualitative analysis, we only managed to identify 79 papers relevant to the study and SLR references.

Although some of the papers might propose a framework for security and the agile model, they were not selected. This is because they were either not meant for the security model [23-36], or not specifically about the Feature driven model [36], or were for learning purposes.

The papers in Appendix A were reviewed individually while data was extracted and questions proposed during the qualitative analysis were answered. The answers to the questions have been recorded.

Based on Fig 2, the selected papers were from the years 1982-2012. No papers from 2000 and 2001 were selected. One paper was selected each year for the years 1989, and 1996. Seventeen papers, the maximum number of papers selected in a year, were selected in 2011. According to Figure 1, the mode for the number of publications is set at seventeen papers. On average, 5.6 papers were found per year.

4.2 Sources of the Study

Based on table from Appendix A, the main sources for the papers were books focusing primarily on security software. Although the years of the books vary, thirteen publications came from such sources. Conference proceedings follow as a primary source, with most papers coming from IEEE, Springer, Spring Sim and ACM. There were also 26 journals, with the remainder coming from websites and white paper. Most of the sources are about security software and agile methodology. Table 3 below shows the sources of papers found and the amount of paper for each source.

(Table 3) Papers Found

Acronym	Type	Number of Publications
ISCI	Journal	1
BT	Journal	1
BPM	Journal	1
ISE	Journal	1
IJIS	Journal	2
Information and Software Technology	Journal	1
ISCA	Proceedings	1
ICAC3	Proceedings	1
MySec	Proceedings	1
JOSS	Journal	1
SERVICES 2010	Proceedings	1
Proceedings 8th International Conference XP	Proceedings	1
RSA	Proceedings	1
TDSC	Proceedings	3
ACMSE	Proceedings	1

Acronym	Type	Number of Publications
HealthSec	Proceedings	1
ACM SIGSOFT	Proceedings	2
SESS	Proceedings	2
LMSA	Proceedings	1
QoP	Proceedings	2
WOSP	Proceedings	1
ECSA	Proceedings	1
Springsim	Proceedings	6
Softw. Pract. Exper.	Proceedings	2
CODASPY	Proceedings	1
HICSS	Proceedings	1
IET	Proceedings	1
AICCSA	Proceedings	1
ICIMA	Proceedings	1
ICCST	Proceedings	1
ARES	Proceedings	1
ICSSP	Proceedings	1
APCC	Proceedings	1
ISOLA	Proceedings	1
TSE	Proceedings	3
WCS	Proceedings	1
SysCon	Proceedings	1
ICCSNT	Proceedings	1
ISSE	Proceedings	1
Proceedings of the Agile Development Conference	Proceedings	1
19th Australian Conference on Software Engineering	Proceedings	1
Fifth International Conference on Software Engineering Advances	Proceedings	1
21st Conference on Software Engineering Education and Training	Proceedings	1
Website		4
Book Review	Book	24
White Paper		3

5. Discussion

In this section, we discuss the answers to the study's proposed research questions.

Q1: *How many studies mentioned security in Agile and when were the initial and latest studies?*

Studies [37-47] mentioned both agile methods and security. [48-55] and some other papers talk about information security. [56] only mentioned agile methodology. The latest study that mentioned security and agile methodology was from 2011 and, according to this SLR, the initial study was from 2005.

Q2: *Were any frameworks or models proposed for FDD and security?*

This SLR did not show any papers that provided an existing framework or model for security and FDD combined, but there was one paper [57]that showed measurements for a matrix comparing compatible FDD elements and security elements. There were also many frameworks [58], architecture [59-63], models [64], and metrics [65] of security that were mentioned in related works.

Q3: *How is the integration between Security and FDD when it comes to a real life software development environment?*

FDD is well known for its structured management in software development and being people oriented [66]. However, a problem remains in that there are no security elements inside FDD. Additionally, there is no specific security role inside FDD [66-68]. Of course there are many security methods that been applied in the real world [69-80], especially in Malaysia [80] and India [81].There is also discussion and much awareness among IT organizations regarding software security practices[82] and the human factors that could attribute to software security[83].However, there is no specific research regarding the integration of security and FDD.

Q4: *How are we going to measure Security and FDD integration after the study?*

For this, we can use security testing papers [84-91], some of which concentrate specifically on data and applications [92]or the design stage [93, 94]. Additionally, there are papers that measure FDD quality and attempt to use those techniques, or combine them, to measure the security quality [95] in the FDD process.

6. Conclusion

There is no established study regarding security integrated with the FDD model because most of the papers found are about agile methodology and security, such as Scrum and XP. We conducted an extensive literature review using 7 journals, 56 conferences, 14 books, 4 website references and 3 white papers, with most of the material coming from 2011. Based on this review, we noted that there is extensive evidence that integration would definitively benefit IT organizations that use the FDD model in creating secure software. In the modern world, people wish to use software for many purposes, such as chatting with friends, navigating via GPS [Global Positioning System], sending e-mails, managing bank transactions, connecting to networking sites and delivering complicated or daily transactions that may involve valuable information. Without a proper software development process that can create secure software, dangerous and unexpected consequences may occur. For example:

- The system that was developed may not be equipped with security measures
- Software vulnerabilities may be created. These may then be able to be exploited by attackers. [9]
- There may be no demand for the system product
- The software developer and user[client] may have little awareness about software security Issues

Since today's software has a high degree of usability, it is not only exposed to threats such as viruses, worms and spyware, but other security threats such as SQL injections, etc. Therefore, it has become important for industries to not only make sure that they develop a fully functional software system, but to equip that system with proper security measurements to ensure that software's future viability.

7. Future Work

We will propose an extended FDD model that integrates security measurements into its structure.The enhanced security-based FDD model will then be applied and evaluated in controlled studies. The findings of the evaluation will be shared with the research community and body of knowledge.

Acknowledgement

We would like to express our gratitude to Ministry of Science, Technology and Innovation (MOSTI) and Universiti Teknologi Malaysia (UTM) for funding this research project under Vot: 4S028.

References

[1] Dyba, T., Dingsoyr, T., "Empirical studies of agile software development: A systematic review," *Information and Software Technology* , pg 833 – 859, 2008.

[2] Mchugh, O., Conboy, K., Lang, M., "Agile Practices: "The Impact on Trust in Software Project Teams, *"Articles on Computer Sciences* , 71-76, 2011.

[3] Slaten, K.M., Droujkova, M., Berenson, S.B., Williams, L., Layman, L., "Undergraduate Student Perceptions of Pair Programming and Agile Software Methodologies: Verifying a Model of Social Interaction," *Proceedings of the Agile Development Conference*, 2005.

[4] Azim, A.S., Amir, S.S., Shams, F., "Embedding Architectural Practices into Extreme Programming," *19th Australian Conference on Software Engineering* , 310-319, 2008.

[5] Breivold, H.P., Sundmark, D., Wallin, P., Larsson, S., "What Does Research Say About Agile and Architecture," *Fifth International Conference on Software Engineering Advances*, 32-37, 2011

[6] Wäyrynen, J., Bodén, M., Boström, G., "Security Engineering and eXtreme Programming: An Impossible Marriage?," *Forum on Stockholm University/Royal Institute of Technology*, 117-128, 2004.

[7] Richard G. Epstein., "Getting Students to Think About How Agile Processes Can Be Made More Secure," *21st Conference on Software Engineering Education and Training,* 2008.

[8] Azham, Z., Ghani, I., Ithnin, N., "Security Backlog in Scrum Security Practices," *5th MySEC (Malaysian*

Conference in Software Engineering), 2011.

[9] AAllen J. H., 2008] Allen J. H.,Software Security Engineering: A Guide for Project Manager, *In Addison Wesley Professional*, 2008.

[10] Sedek K. A., Sulaiman S., and Omar M. A., A systematic literature review of interoperable architecture for e-government portals, *Malaysian Conference in Software Engineering*, pp. 82-87, 2011.

[11] [Agile!=Security, 2012] Agile!=Security, 2012, http://www.rakkhis.com/2011/06/agile-security.html

[12] Spruit M. E. M. and Looijen M., IT security *in Dutch practice, Computers and Security*, vol. 15, No. 2, pp. 157-170, 1996.

[13] Bala Musa.S, Norita Md Norwawi, Mohd Hassan Selamat, Khaironi Yetim Sharif Improved Extreme Programming, *IEEE Symposium on Computers & Informatics*, 2011.

[14] Ryan Riley, Xuxian Jiang, Dongyan Xu., An Architectural Approach to Preventing Code Injection Attacks, *IEEE Transactions On Dependable And Secure Computing, Vol. 7*, No. 4, 2010.

[15] Jie Ren, Richard Taylor, Paul Dourish, David Redmiles., Towards An Architectural Treatment of Software Security: A Connector-Centric Approach. Software *Engineering for Secure Systems - Building Trustworthy Applications* , 2005.

[16] A Jones., A framework for the management of information security risks, *BT Technology* ,2007.

[17] Mohamed El-Attar.,A framework for improving quality in misuse case models, *Business Process Management Journal* Vol. 18 No. 2, 2012.

[18] Vibhu Saujanya Sharma, Kishor S. Trivedi.,Quantifying software performance, reliability and security:An architecture-based approach, *The Journal of Systems and Software* 80, p. 493-509, 2007.

[19] Dieste O., and Juristo N., Systematic review and aggregation of empirical studies on elicitation techniques., *IEEE Transactions on Software Engineering*, vol. 37, no. 2, pp. 283-304, 2011.

[20] Salleh N., Mendes E., and Grundy J.,Empirical Studies of Pair Programming for CS/SE Teaching in Higher Education: A Systematic Literature Review, *IEEE Transactions on Software Engineering*, vol. 37, no. 4, pp. 509-525, 2011.

[21] Kitchenham B., Pearl O. B., Budgen D., Turner M., Bailey J., and Linkman S.,Systematic literature reviews in software engineering - A systematic literature review, *Information and Software Technology*, vol. 51, no. 1, pp. 7-15, 2009

[22] B. A. Kitchenham et al..,Preliminary guidelines for empirical research in software engineering, *IEEE Transactions on Software Engineering*, vol. 28, no. 8, pp. 721-734, 2002.

[23] Jim Q. Chen, Dien Phan, B. Wang, Douglas R. Vogel., Light-Weight Development Method: a Case Study, *IEEE*,2007.

[24] Richard G. Epstein., Getting Students to Think About How Agile Processes Can Be Made More Secure,*21st Conference on Software Engineering Education and Training*, 2008.

[25] Ali Inan, Murat Kantarcioglu, Gabriel Ghinita, and Elisa Bertino.,A Hybrid Approach to Private Record Matching, *IEEE Transactions On Dependable And Secure Computing*, Vol. 9, No. 5, 2012.

[26] Bernhard Hämmerli., Financial Services Industry. Critical Information Infrastructure Protection, *LNCS* 7130, pp. 301-329, 2012.

[27] Amir Mohd Talib,Rodziah Atan, Rusli Abdullah, Masraf Azrifah Azmi Murad., Multi agent system architecture oriented Prometheus methodology design to facilitate security of cloud data storage, *Journal of Software Engineering* , vol. 5, no. 3, pp. 78-90, 2011.

[28] Lian Yu1, Shi-Zhong Wu, Tao Guo, Guo-Wei Dong,Cheng-Cheng Wan1, and Yin-Hang Jing., Ontology Model-Based Static Analysis of Security Vulnerabilities, *LNCS* 7043, pp. 330–344, 2011.

[29] Sam Weber Paul A. Karger Amit Paradkar., A Software Flaw Taxonomy: Aiming Tools *At Security.Software Engineering for Secure Systems, Building Trustworthy Applications*, 2005.

[30] GOETZ GRAEFE.,Query Evaluation Techniques for Large Databases, *ACM Computing Surveys*, Vol. 25, No. 2, 1993.

[31] Ross Hytnen and Mario Garcia., AN ANALYSIS OF WIRELESS SECURITY, Consortium for Computing Sciences in Colleges, 2006.

[32] Michael Kainerstorfer et al., 2011] Michael Kainerstorfer, Johannes Sametinger, Andreas Wiesauer., Software Security for Small Development Teams - A Case Study, WAS2011, 2011.

[33] Donald G. Firesmith, 2010] Donald G. Firesmith., Engineering Safety- and Security-Related Requirements for Software-Intensive Systems: Tutorial Summary, ICSE, 2010.

[34] Terrence August and Tunay I. Tuncay, 2011] Terrence August, Tunay I. Tuncay., Who Should be Responsible for Software Security? A Comparative Analysis of Liability Policies in Network Environments, Management Science Vol. 57, Issue. 5, INFORMS, pp. 934-959, 2011.

[35] Zhendong Ma, Christian Wagner, Thomas Bleier., Model-driven security for Web services in e-Government system: ideal and real, IEEE, 2011.

[36] Zahid Anwar and Roy Campbell., Automated Assessment Of Compliance With Security Best Practices, IFIP International Federation for Information Processing, Volume 290; *Critical Infrastructure Protection II*, eds. Papa, M., Shenoi, S., Boston, Springer, pp. 173-187, 2008.

[37] Nicolaysen T., Sassoon R., Line M. B, Jaatun M. G., Agile Software Development: The Straight and Narrow Path to Secure Software?, *International Journal of Secure Software Engineering*, Vol. 1, Issue 3, pp.71-85, 2010.

[38] Lane A.,Agile Development, Security Fail, *RSA Conference Europe*, 2011.

[39] Siponen M., Baskerville R. and Kuivalainen T., Integrating Security into Agile Development Methods, *Proceedings IEEE 38th Hawaii International Conference on System Sciences*, pp. 7695-2268, 2005.

[40] Dejan Baca, Bengt Carlsson.,Agile development with security engineering activities, *Proceeding, ICSSP '11 Proceedings of International Conference on Software and Systems Process*, 2011.

[41] Gencer Erdogan, Per Hakon Meland, and Derek Mathieson., Security Testing in Agile Web Application Development - A Case Study Using the East Methodology. XP, *LNBIP , Springer-Verlag Berlin Heidelberg* ,48, pp. 14-27, 2010.

[42] Neugent W.,Teaching Computer Securitv: A Course Outline, *Computers and Security*, vol. 1, pp. 152-163, 1982.

[43] Mikko Siponena, Richard Baskervilleb and Tapio Kuivalainena., Integrating Security into Agile Development Methods, *Proceedings of the 38th Hawaii International Conference on System Sciences* , 2005.

[44] Hossein Keramati, Seyed-Hassan Mirian-Hosseinabadi., Integrating Software Development Security Activities with Agile Methodologies, *IEEE*, 2008.

[45] Min, Liu Qiong-mei, Wang Cheng., Practices of Agile Manufacturing Enterprise Data Security and Software Protection, *2nd International Conference on Industrial Mechatronics and Automation*, 2010.

[46] Rick Dove., Pattern Qualifications And Examples Of Next-Generation Agile System-Security Strategies, *IEEE*, 2010.

[47] Steffen Bartsch., Practitioners' Perspectives on Security in Agile Development, *Sixth International Conference on Availability, Reliability and Security*, 2011.

[48] Highsmith J.,What Is Agile Software Development*?, Boston, Crosswalk*, 2002

[49] Shore J. andWarden S. 2007.," The Art Of Agile Development", *USA O'Reilly*, 2007.

[50] Gregorio D., How the Business Analyst Supports and Encourages Collaboration on Agile Projects, *Massachusetts*, 2012.

[51] Post g. v. and Karen-Ann K. "Accessibility vs.Security: A Look at the Demand for Computer Security," *Computers and Security*, vol.10,pp.331-344, 2007.

[52] John Steven.,"Security Testing of Internal Tools," *Basic Training*, 2007.

[53] Qiu-Hong Wang, Wei T. Yue, Kai-Lung Hui,"Do Hacker Forums Contribute to Security Attacks?," *WEB*, 2011.

[54] Spruit M. E. M. and Looijen M., "IT security in Dutch practice," *Computers and Security*, vol. 15, No. 2, pp. 157-170, 1996.

[55] Brian Chess, Brad Arkin.,Software Security in Practice, *Build in Security*, 2011.

[56] Richard Stanley., "Information Security. Cybercrimes: A Multidisciplinary Analysis," Berlin, Heidelberg: *Springer Berlin Heidelberg*, pp. 95 – 126, 2010.

[57] Siponen M., Baskerville R. and Kuivalainen T.:Integrating Security into Agile Development Methods, Proceedings IEEE 38th Hawaii International Conference on System Sciences, pp. 7695-2268, 2005.

[58] Valcke P. and Dumortier J., 2012] Valcke P. and Dumortier J.:Trust in the information society - In search of trust generating. Computer law and security review, vol. 28, pp. 504-512, 2012.

[59] Brian Chess, Brad Arkin.: Software Security in Practice, Build in Security, 2011.

[60] Gary McGraw," Software Security, Building Security In," *Addison-Wesley Professional*, 2006.

[61] Vibhu Saujanya Sharma, Kishor S. Trivedi," Architecture Based Analysis of Performance, Reliability and Security of Software Systems," *WOSP* , 2005.

[62] Michael Dalton, Hari Kannan, Christos Kozyrakis," Raksha: A Flexible Information Flow Architecture for Software Security," *ISCA*, 2007.

[63] Spyros T. Halkidis, Nikolaos Tsantalis, Alexander Chatzigeorgiou,George Stephanides," Architectural Risk Analysis of Software Systems Based on Security Patterns." *IEEE Transactions On Dependable And Secure Computing*, Vol. 5, No. 3, 2008.

[64] Jay-Evan J. Tevis, John A. Hamilton, Jr,"A Security-centric Ring-based Software Architecture." *SpringSim* , Vol. 2, 2007

[65] Pratyusa K. Manadhata, Jeannette M. Wing,"An Attack Surface Metric." *IEEE Transactions On Software Engineering*, Vol. 37, No. 3, 2011.

[66] Rhoden E., "People and processes – The Key Elements to Information Security,"*Computer Fraud and Security, Volume*,Issue: 6, pp. 14-15, 2002.

[67] Ashraf Ferdouse Chowdhury, Mohammad Nazmul Huda, "Comparison between Adaptive Software Development andFeature Driven Development" *International Conference on Computer Science and Network Technology*, 2011.

[68] Stephen.R.Palm,"Feature-Driven Development－Practices," *A Practical Guide to Feature-Driven Development*, Chap.3, pp. 35-54, 2002

[69] Konstantin Beznosov,Brian Chess,"An Industry Perspective on the Secure-Software Challenge, " *Security for the Rest of Us*,2008.

[70] Davide Balzarotti, Greg Banks, Marco Cova, Viktoria Felmetsger, Richard A. Kemmerer, William Robertson ,Fredrik Valeur, and Giovanni Vigna," An Experience in Testing the Security of Real-World Electronic Voting Systems," *IEEE Transactions On Software Engineering*, vol. 36, no. 4, pp. 453–473, 2010.

[71] Scott Knight , Scott Buffett, Patrick C. K. Hung," The International Journal of Information Security Special Issue on privacy, security and trust technologies and E-business services," *International Journal of Information Security*, vol. 6, no. 5, pp. 285-286, Jul. 2007.

[72] Carlos Becker Westphall, Peter Mueller,"Management of Security and Security for Management Systems, " *Guest Editorial*, 2010.

[73] Yves Le Roux,"Information Security Governance for Executive Management, "*Securing Electronic Business Processes*, 2007.

[74] Frank Innerhofer-Oberperfler ,Markus Mitterer, Michael Hafner and Ruth Breu,"A methodical Approach and case study," 2010.

[75] Scott Knight, Scott Buffett,Patrick C. K. Hung," The International Journal of Information Security Special Issue on privacy, security and trust technologies and E-business services, " *Guest Editors'Introduction,*2007.

[76] Dejan Baca, Bengt Carlsson, Kai Petersen and Lars Lundberg," Improving software security with static automated code analysis in an industry setting, " *Software Practice And Experience*, 2012.

[77] Leach J," TBSE and engineering approach to the design of accurate and reliable security systems, " *Computers and Security*, vol. 23, pp. 22-28, 2004.

[78] John B. Dickson,"Software Security: Is OK Good Enough?, " *CODASPY*,2011.

[79] Ann E.K. Sobel, Gary McGraw," Interview:Software Security In The Real World, " *Software Assurance*, 2010.

[80] W. AI-Salihy, Jannet Ann, R. Sures," Effectivess of Information Systems Security in IT Organizations" *in Malaysia, IEEE*,2003

[81] Sanjay Bahl, O P Wali, Ponnurangam Kumaraguru," Information Security Practices Followed in the Indian Software Services Industry: An Exploratory Study, "

EWI, 2011.

[82] C. Banerjee1, S. K. Pandey," Research on Software Security Awareness: Problems and Prospects, " *ACM SIGSOFT Software Engineering Notes*, 2010.

[83] Karadsheh L. :Applying security policies and service level agreement to IaaS service model to enhance security and transition, Computers And Security," vol. 31, pp. 315-326, 2012.

[84] Stephen.R.Palm,"Feature-Driven Development－Practices, *"A Practical Guide to Feature-Driven Development*, Chap.3, pp. 35-54, 2002

[85] John Steven,"Security Testing of Internal Tools, " *Basic Training*, 2007

[86] Kruys J. P. " Security of Open Systems. Computers and Security", vol. 8, pp. 139-147, 1989

[87] Kyung Cheol Choi and Gun Ho Lee," Automatic Test Approach of Web Application for Security, " *ICCSA*, pp. 659－668, 2006.

[88] Haralambos Mouratidis and Paolo Giorgini," Secure Tropos: a Security-Oriented Extension of the Tropos Methodology, " *International Journal of Software Engineering and Knowledge Engineering* , Vol. 17, pp.285-309, 2007

[89] Aaron Marback, Hyunsook Do, Ke He, Samuel Kondamarri and Dianxiang Xu," A threat model-based approach to security testing, " *Software Practice Expert, JohnWiley & Sons, Ltd.* ,2012

[90] Venter H.S. and Eloff J.H.P. "A taxonomy for information security technologies, " *Computers and Security*, Vol. 22, Issue: 4, Pages: 299-307, 2003

[91] Purser S. A. "Improving the ROI of the security management process, " *Computers and Security*, vol. 23, pp. 542-546, 2004.

[92] Hone K. and Eloff J.H.P. "Information security policy － what do international information security standards say?, "*Computers and Security*, pp. 402-409, 2002

[93] S. Rehman & K. Mustafa," Research on Software Design Level Security Vulnerabilities, *"ACM SIGSOFT Software Engineering Notes*, Vol. 34, Number 6, 2009.

[94] Dlaminia M. T., Eloffa J. H. P., Eloffb M. M. "Information security: The moving target, " *Computers & Security,* vol. 28, pp. 189－198,2004.

[95] Daniel Mellado, Eduardo Fernández-Medina, Mario Piattini," A Comparison of Software Design Security Metrics, " *ECSA*,2010.

[96] Abdullahi SaniAdila FirdausSeung Ryul JeongImran Ghani, A Review on Software Development Security Engineering using Dynamic System Method (DSDM), *International Journal of Computer Applications*, Volume 69 - Number 25, 2013.

[97] Imran Ghani, Izzaty Yasin, Software Security Engineering in eXtreme Programming Methodology: a Systematic Literature Review,*S ci.Int. (Lahore)*, 25(2), 215-221,2013.

[98] Coad, P., Lefebvre, E. & De Luca, J. Java Modeling In Color With UML: Enterprise Components and Process. *Prentice Hall International.* (ISBN 0-13-011510-X), 1999.

[99] Palmer, S.R., & Felsing, J.M. A Practical Guide to Feature-Driven Development. *Prentice Hall.* (ISBN 0-13-067615-2), 2002.

[100] http://www.skillresource.com, accessed on 03, December 2013.

Appendix A

ID	Author	Year	Title	Type	Q1	Q2	Q3	Q4
S1	Nicolaysen	2010	Software Development: The Straight and Narrow Path to Secure Software?	Journal	P	Y	P	P
S2	Lane	2011	Agile Development, Security Fail	Conference	Y	Y	N	Y
S3	Siponen	2005	Integrating Security into Agile Development Methods	Conference	Y	Y	N	Y
S4	Julia H. Allen	2008	Software Security Engineering: A Guide for Project Manager	Book	P	Y	N	Y
S5	Branstad and Smid	1982	Integrity and Security Standards Based on Cryptography	Journal	N	Y	Y	Y
S6	Jim Highsmith	2002	What Is Agile Software Development?	Book	P	N	N	Y
S7	James Shore	2007	The Art Of Agile Development	Book	P	N	N	Y
S8	Donna D. Gregorio	2012	How the Business Analyst Supports and Encourages Collaboration on Agile Projects	Conference	P	N	N	Y
S9	Dejan Baca	2002	Agile development with security engineering activities	Conference	P	Y	N	Y
S10	Pyla et al.	2011	Common Criteria	Websites	Y	Y	N	Y
S11	Rusu et al.	2011	SSE-CMM	Websites	Y	Y	N	Y
S12	Gencer Erdogan	2010	Security Testing in Agile Web Application Development - A Case Study Using the East Methodology	Book	Y	Y	Y	Y
S13	Walker Royce	2009	Improving Software Economics	White Paper	P	N	N	Y
S14	Secure Software Inc	2006	CLASP: Comprehensive Lightweight Application Security Process	Websites	P	Y	N	Y
S15	Agile!= security	2011	Agile!=security	Websites	Y	Y	N	Y
S16	Lunt	1992	Security in Database Systems: A Research Perspective security in database system	Journal	N	Y	N	Y
S17	Stephen de Vries	2007	Software Testing for security	Journal	P	Y	Y	Y
S18	Mikko Siponena	2005	Integrating Security into Agile Development Methods	Conference	Y	Y	N	Y
S19	Neugent	1982	Teaching Computer Security: A Course Outline	Journal	N	Y	Y	Y
S20	Hossein Keramati	2008	Integrating Software Development Security Activities with Agile Methodologies	Conference	Y	Y	N	Y
S21	Zeng Min	2010	of Agile Manufacturing Enterprise Data Security and Software Protection	Conference	Y	Y	N	Y
S22	Rick Dove	2010	Pattern Qualifications And Examples Of Next-Generation Agile System-Security Strategies	Conference	Y	Y	Y	Y
S23	Steffen Bartsch	2011	Practitioners' Perspectives on Security in Agile Development	Conference	Y	Y	N	Y
S24	W. AI-Salihy	2003	Effectiveness of Information Systems Security in IT Organizations in Malaysia	Conference	P	Y	N	Y
S25	Konstantin Beznosov	2008	An Industry Perspective on the Secure-Software Challenge	Journal	P	Y	N	Y
S26	Richard Ford	2007	Becoming a Security Expert	Books	P	Y	N	Y
S27	John Steven	2011	Security Testing of Internal Tools	Journal	P	Y	Y	Y

ID	Author	Year	Title	Type	Q1	Q2	Q3	Q4
S28	Davide Balzarotti	2010	An Experience in Testing the Security of Real-World Electronic Voting Systems	Journal	P	Y	Y	Y
S29	Ryan Riley	2010	An Architectural Approach to Preventing Code Injection Attacks	Journal	P	Y	Y	Y
S30	Pratyusa K. Manadhata	2011	An Attack Surface Metric	Book	P	Y	Y	Y
S31	Kruys	1989	Security of Open Systems	Journal	N	Y	Y	Y
S32	Brian Chess	2011	Resilient Security Architecture	Book	P	Y	Y	Y
S33	Sanjay Bahl	2011	Information Security Practices Followed in the Indian Software Services Industry: An Exploratory Study	Conference	P	Y	Y	Y
S34	Scott Knight	2007	The International Journal of Information Security Special Issue on privacy, security and trust technologies and E-business services	Journal	P	Y	N	Y
S35	Carlos Becker Westphall	2007	Management of Security and Security for Management Systems	Conference	P	N	N	Y
S36	Yves Le Roux	2011	Information Security Governance for Executive Management	Book	P	Y	N	Y
S37	Anwar and Campbell	2008	Automated Assessment Of Compliance With Security Best Practices	Book	P	Y	Y	Y
S38	Richard Stanley	2010	Information Security.Cybercrimes: A Multidisciplinary Analysis	Book	P	Y		Y
S39	Innerhofer-Oberperfler	2010	A methodical Approach and case study	Conference	P	Y	Y	Y
S40	Choi and Lee	2006	Automatic Test Approach of Web Application for Security [Auto Inspect]	Book	P	Y	T	Y
S41	Scott Knight	2011	The International Journal of Information Security Special Issue on privacy, security and trust technologies and E-business services	Journal	P	Y	N	Y
S42	Qiu-Hong Wang	2011	Do Hacker Forums Contribute to Security Attacks?	Book	P	Y	N	Y
S43	A Jones	2007	A framework for the management of information security risks	Journal	P	Y	Y	Y
S44	Mohamed El-Attar	2012	A framework for improving quality in misuse case models	Journal	P	Y	Y	Y
S45	Mouratidis& Giorgini	2012	SECURE TROPOS: A SECURITY-ORIENTED EXTENSION OF THE TROPOS METHODOLOGY	Journal	P	Y	Y	Y
S46	Aaron Marback	2012	A threat model-based approach to security testing	Boook	P	Y	Y	Y
S47	Dejan Baca	2012	Improving software security with static automated code analysis in an industry setting	Book	P	Y	Y	Y
S48	Vibhu Saujanya Sharma	2007	Quantifying software performance, reliability and security: An architecture-based approach	Journal	P	Y	Y	Y
S49	Spruit and Looijen	1996	IT security in Dutch practice	Journal	N	Y	Y	Y
S50	Chess and Arkin	2011	Software Security in Practice	Books	P	Y	N	Y

ID	Author	Year	Title	Type	Q1	Q2	Q3	Q4
S51	Hone and Eloff	2002	Information security policy – what do international information security standards say?	Journal	N	Y	Y	Y
S52	Venter and Eloff	2003	A taxonomy for information security technologies	Journal	N	Y	Y	Y
S53	Leach	2004	TBSEdan engineering approach to the design of accurate and reliable security systems	Journal	N	Y	Y	Y
S54	C. Banerjee	2010	Research on Software Security Awareness: Problems and Prospects	Book	P	Y	N	Y
S55	Purser	2004	Improving the ROI of the security management process	Journal	N	Y	Y	Y
S56	S. Rehman and K. Mustafa	2009	Research on Software Design Level Security Vulnerabilities	Book	P	Y	N	Y
S57	Dlaminia et al.	2009	Information security: The moving target	Journal	N	Y	Y	Y
S58	Jie Ren	2005	Towards An Architectural Treatment of Software Security: A Connector-Centric Approach	Conference	P	Y	Y	Y
S59	Karadsheh	2012	Applying security policies and service level agreement to IaaS service model to enhance security and transition	Journal	N	Y	Y	Y
S60	John B. Dickson	2011	Software Security: Is OK Good Enough?	Books	P	Y	N	Y
S61	Gary McGraw	2006	Software Security: Building Security In	Books	P	Y	N	Y
S62	Jay-Evan J. Tevis	2007	A Security-centric Ring-based Software Architecture	Conference	P	Y	Y	Y
S63	Vibhu Saujanya Sharma	2005	Architecture Based Analysis of Performance, Reliability and Security of Software Systems	Conference	P	Y	Y	Y
S64	Michael Dalton	2007	Raksha: A Flexible Information Flow Architecture for Software Security	Conference	P	Y	Y	Y
S65	Daniel Mellado	2010	A Comparison of Software Design Security Metrics	Conference	P	Y	Y	Y
S66	Valcke and Dumortier	2012	Trust in the information society - In search of trust generating	Journal	N	Y	Y	Y
S67	Sobel and McGraw	2010	Interview: Software Security In The Real World	Book	P	Y	N	Y
S68	Spyros T. Halkidis	2008	Architectural Risk Analysis of Software Systems Based on Security Patterns	Journal	P	Y	Y	Y
S69	Chowdhury and Huda	2011	Comparison between Adaptive Software Development and Feature Driven Development	Conference	P	N	N	Y
S70	Stephen.R.Palm	2002	A Practical Guide to Feature-Driven Development	Book	P	N	N	Y
S71	Bala Musa.S	2011	Improved Extreme Programming	Conference	Y	Y	N	Y
S72	Rhoden	2002	People and processes — The Key Elements to Information Security	Book	N	Y	Y	Y
S73	Dyba and Dingsoyr	2008	Empirical studies of agile software development: A systematic review	Journal	P	N	Y	Y
S74	Mchugh *et al.*	2012	Agile Practices: "The Impact on Trust in Software Project Teams	White Paper	Y	Y	Y	Y

ID	Author	Year	Title	Type	Q1	Q2	Q3	Q4
S75	Slaten *et al*	2005	Undergraduate Student Perceptions of Pair Programming and Agile Software Methodologies: Verifying a Model of Social Interaction	Conference	P	N	N	Y
S76	Azim *et al.*	2008	Embedding Architectural Practices into Extreme Programming	Conference	P	N	N	Y
S77	Breivold *et al*	2010	What Does Research Say About Agile and Architecture	Conference	P	N	N	Y
S78	Wäyrynen *et al*	2004	Security Engineering and eXtreme Programming: An Impossible Marriage?	White Paper	P	Y	N	Y
S79	Azham *et al.*	2011	Security Backlog in Scrum Security Practices	Conference	P	Y	Y	Y

◐ 저 자 소 개 ◑

Adila Firdaus Arbain

2012 B.Cs. in Software Engineering, Universiti Teknologi Malaysia, Johor, Malaysia.
2013~Present: MS-Leading to Ph.D. Universiti Teknologi Malaysia, Johor, Malaysia.
Research Interests: Agile Development Methods, Software Engineering etc.
E-mail : adilafirdaus@gmail.com

Imran Ghani

1994 B.A. in Arts, Bahaudin Zakariya Univ., Multan, Pakistan.
2002 Master in IT, Univ. of Arid Agriculture Rawalpindi, Pakistan.
2006 M.S. in Computer Science, Universiti Teknologi Malaysia, Johor, Malaysia.
2010 Ph.D. in Business IT, Kookmin Univ, Seoul, Korea.
2010~Present: Senior Lecturer, Faculty of Computing, Dept. of Software Engineering, Universiti Teknologi Malaysia, Johor, Malaysia.
Research Interests: Agile Development Methods, Software Engineering, Semantic Web, Enterprise Architecture Management etc.
E-mail : imran@utm.my

Seung Ryul Jeong

1985 B.A. in Economics, Sogang Univ., Seoul, Korea
1989 M.S. in MIS, Univ. of Wisconsin, WI, U.S.A.
1995 Ph.D. in MIS, Univ. of South Carolina, SC, U.S.A.
1997~Present: Professor, Graduate School of Business IT, Kookmin Univ., Korea
Research Interests: System Implementation, Process Innovation, Project Management, Information Resource Management etc.
E-mail : srjeong@kookmin.ac.kr