Secure Software Practices among Malaysian Software Practitioners: An Exploratory Study

Shafinah Farvin Packeer Mohamed[1, a)], Fauziah Baharom[1, b)], Aziz Deraman[2, c)], Jamaiah Yahya[3, d)] and Haslina Mohd[1, e)]

[1] *School of Computing, Universiti Utara Malaysia, 06010 Sintok, Kedah, Malaysia*
[2]*Faculty of Science and Technology, Universiti Malaysia Terengganu, 21030 KualaTerengganu, Terengganu, Malaysia*
[3]*Faculty of Information Science & Technology, The National University of Malaysia, Bangi, 43600 Selangor, Malaysia*
[a)] Corresponding author: shafinah@uum.edu.my
[b,e)] {fauziah, haslina}@uum.edu.my
[c)] a.d@umt.edu.my
[d)] jhy@ftsm.ukm.my

Abstract. Secure software practices is increasingly gaining much importance among software practitioners and researchers due to the rise of computer crimes in the software industry. It has become as one of the determinant factors for producing high quality software. Even though its importance has been revealed, its current practice in the software industry is still scarce, particularly in Malaysia. Thus, an exploratory study is conducted among software practitioners in Malaysia to study their experiences and practices in the real-world projects. This paper discusses the findings from the study, which involved 93 software practitioners. Structured questionnaire is utilized for data collection purpose whilst statistical methods such as frequency, mean, and cross tabulation are used for data analysis. Outcomes from this study reveal that software practitioners are becoming increasingly aware on the importance of secure software practices, however, they lack of appropriate implementation, which could affect the quality of produced software.

INTRODUCTION

The need for secured software is gaining much emphasis in recent years. This is because currently software customers are losing hundred million of dollars every year as a consequence from frauds and computer crime activities. It is caused by the nature of software nowadays which is exposed to malicious attacks due to the application environment that is more complex, distributed and keep confidential data. Lately, there are many serious computer crimes have been reported in Malaysia, whereby there are 88% increment on the incidents reported via the Cyber999 Help Centre in Malaysia, compared with year 2010 [1]. On top of that, Malaysia has been listed in the Sophos Security Threat Report 2013 as the sixth most vulnerable country in the world to cyber crime, in the form of malware attacks through the computer or smart phone [2]. Consequently, the customers are becoming more concerned about the security of software produced to them. Since it is estimated that 80% of all breaches are application-related, the traditional perimeter defenses like firewalls, intrusion detection and anti-virus systems are unable to protect software. Thus, most researchers believe that security activities should be considered from the beginning of the software development lifecycle and continuous in all phases [3,4]. McGraw defines secure software practices as "*about building secure software: designing software to be secure, making sure that software is secure, and educating software developers, architects, and users about how to build secure things*[5].

Despite its importance, the current practices of software practitioners in Malaysia regarding secure software practices is still scarce. Even though there are many studies conducted on the current practices of software development practices in Malaysia, the focus is more on the conventional software process [6,7]. However it is essential to investigate the current practices of secure software since it has become as a determinant factor for producing high quality software. Based on the abovementioned limitations, an exploratory study is conducted to explore the experiences and practices of software practitioners on the secure software practices. This paper discusses findings from the study. First, the existing work is described, followed by research approach, continued with findings, discussion and ended with the conclusion.

EXISTING EMPIRICAL STUDIES ON SECURE SOFTWARE PRACTICES

There are several studies which focuses on secure software practices conducted in Western countries, for instance Whitehat Security investigated the number of vulnerabilities in small, medium and large organizations [8], while National Cyber Security Alliance [9] surveyed the security trainings provided in software companies, the awareness of security initiatives and the security problems they are facing. In addition, Errata Security [10] found out that 57% of the respondents used secure development methods, while 43% do not consider secure development methods at all. Moreover, Elahi et al. [11] and Wilander and Gustavsson [12] investigated the software practitioners' practices in requirement engineering which focus on security. In Malaysia, there are many studies have been conducted in the software development area which are intended for investigating the current practices of software development in the Malaysian software industry, for instance [6,13]. However, these existing studies focused on the conventional software development practices, rather than secure software practices.

Based on the existing studies discussed, empirical studies on the secure software practices is lacking in Malaysia, since their focus is more on the conventional software process. On the other hand, including secure software practices during software development has become determinant factor for producing high quality software. Nevertheless, its practices among software practitioners in Malaysia is still scarce. Consequently, in this study the secure software practices being implemented by the Malaysian software practitioners have been investigated. Section 3 explains about the execution of the study.

RESEARCH APPROACH

The research was conducted through four (4) phases, as described in Table 1.

TABLE 1. Research Activities and Descriptions

Activities	Descriptions
Instrument design	-instrument was designed by referring previous works such as [6] and [11]. -consists of single and multiple responses, yes/no questions.
Pilot study	-involved 32 respondents (system analysts and programmers with at least 5 years' experience). -they agreed that the questions covers the domain of the secure software practices, however, there are some suggestions: simplify the questions to be more readable and understandable, reduce and reorganize the questions.
Data collection	-data was collected from samples which were identified from Kuala Lumpur, Selangor, Penang and Kedah, since most software development companies are located there in Malaysia [14]. -the questionnaire was distributed through online survey, email or mail.
Data analysis	-the collected data was analyzed using descriptive statistical analysis: the frequencies, mean and cross tabulation by using the SPSS software.

THE FINDINGS

This section discusses the results on the demographic data and the software practitioners' experience and practices regarding secure software.

4.1 Demographic Data

The respondents are asked about their position and experience. Cross tabulation analysis is used to classify them, as depicted in Table 2. Most of the respondents are programmers (41.9%). Out of the 93 respondents, only 16.1% have experience more than 10 years, while majority have 1 to 5 years of experience (50.5%).

TABLE 2. Respondents' Experience

Positions	<1 year	1-5 years	6-10 years	11-20 years	Total
Project Managers	1(1.1%)	3(3.2%)	2(2.2%)	4(4.3%)	10(10.8%)
Programmers	7(7.5%)	26(28%)	3(3.2%)	3(3.2%)	39(41.9%)
Quality Assurance/Testers	0(0%)	5(5.4%)	0(0%)	1(1.1%)	6(6.5%)
System Analysts	2(2.2%)	10(10.8 %)	11(11.8 %)	3(3.2%)	26(28%)
Security Advisors	1(1.1%)	0(0 %)	0(0 %)	0(0 %)	1(1.1%)
Team Leaders	1(1.1%)	3(3.2%)	3(3.2%)	4(4.3%)	11(11.8%)
Total	**12(13%)**	**47(50.5%)**	**19(20.4%)**	**15(16.1%)**	**93(100%)**

The respondents work in software development, education/training, service and public administration, manufacturing, telecommunication, consultation, health and social work or banking/insurance/financial sectors, as presented in Table 3. Most of the respondents are from private sectors (76%), with 47% from software development organizations.

TABLE 3. Classification of Organization Sector

Sectors	Organization Types		Total
	Private	Government	
Software Development	44(47%)	0(0%)	44(47%)
Education/Training	10(11%)	11(12%)	21(23%)
Service and Public Administration	5(5.4%)	4(4.4%)	9(9.7%)
Manufacturing	4(4.3%)	0(0%)	4(4.3%)
Consultation	3(3.2%)	1(1%)	4(4.3%)
Telecommunication	4(4.3%)	0(0%)	4(4.3%)
Health & Social Work	0(0%)	5(5.4%)	5(5.4%)
Banking/Financial/Insurance	1(1%)	1(1%)	2(2.2%)
Total	**71(76%)**	**22(24%)**	**93(100%)**

4.2 Software Practitioners' Experience & Practices in Secure Software

Firstly, the respondents were asked whether they agree that secure software practices can influence the quality of produced software. 96% agreed, while only 4% disagreed. Secondly, the respondents were asked about the security incidents that they faced (they can give multiple answers). It is found that respondents faced many security incidents, as depicted in Figure 1. The most common security incidents faced by them are password cracking (45%), followed by malicious code (39%) and SQL injection (35%). Only small percentage (9%) of them never face any security incidents.

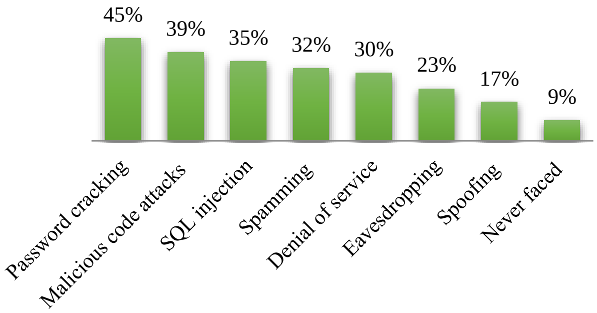

FIGURE 1. The security incidents faced

Thirdly, the respondents were asked whether they elicit and document security requirements explicitly from early stage. 21.5% of the respondents discuss about the security requirement from early stage. Unfortunately, the requirements are not documented. However, 24% of them are aware of this, whereby they gather and document the security requirements explicitly during requirement gathering. Meanwhile, 32% of the respondents only deal with security issues during the implementation phase or after the system being developed. On top of that, 22.5% do not even deal with the security requirements, as presented in Table 4.

TABLE 4. Eliciting Security Requirements Explicitly

Answers	**Frequency/ Percentage**
Security issues are only dealt during the implementation phase or after the system being developed	30(32%)
Security requirements are gathered and documentedin the early stages of the pro jects before the development starts	22(24%)
Do not deal with security requirements	21(22.5%)
Security requirements are discussed from early stages butnot documented	20(21.5%)
Total	**93(100%)**

Table 5 depicts the analysis result regarding the notations used to represent security requirements (respondents can give multiple answers). Unfortunately, the analysis result found that majority of them (76%) do not document the security requirements, while 4% do not use any specific notation to represent the security requirements.

TABLE 5. Notations used

Notations	**Frequency**	**Percentages**
Do not document	71	76%
Abuse case	10	11%
Misuse case	9	10%
Attack tree	7	8%
No specific notation	4	4%
Misuser stories	2	2%

Additionally, the respondents were asked about how they prevent from introducing common attacks that occurred previously. Surprisingly, majority of them did not consider the attacks that have happened in the past (41%). However, fortunately the remaining respondents referred to the document which records the security attacks that have occurred previously (37%), while 35% of them consulted with the security experts. Table 6 demonstrates the analysis result.

TABLE 6. Prevention techniques from common attacks

Prevention techniques	Frequency	Percentage
Do not consider attacks that have happened in the past	38	41%
Refer to document which records the security attacks that have occurred	34	37%
Consult with security experts to prevent common attacks	33	35%
Look for well-known common security attacks in attack and vulnerability databases	32	34%

Moreover, the respondents were asked about the percentage of security trainings provided for the staff. Cross tabulation analysis was used in order to classify the respondents based on their position and amount of security training provided for them. Most of the respondents (38.7%) are provided with 25% or less security trainings in a year. Quite a big percentage is not provided with any security trainings (19.4%). Only 24.7% are provided with security trainings within 25 to 50 percent in a year. The result of analysis is depicted in Table 7. Meanwhile, the trainings are provided mostly for the programmers and system analysts, 41.9% and 28% respectively.

TABLE 7. Percentages of security training provided

Positions	Percentages of trainings per year					Total
	None	<= 25%	25% - 50%	50% - 75%	> 75%	
Project Manager	1.1%	3.2%	3.2%	2.2%	1.1%	10.8%
Programmer	7.5%	15.1%	11.8%	2.2%	5.4%	41.9%
Quality Assurance/Tester	2.2%	3.2%	1.1%	0%	0%	6.5%
System Analyst	7.5%	10.8%	5.4%	2.2%	2.2%	28%
Security Advisor	0%	0%	1.1%	0%	0%	1.1%
Team leader	1.1%	6.5%	2.2%	0%	2.2%	11.8%
Total	**19.4%**	**38.7%**	**24.7%**	**6.5%**	**10.8%**	**100%**

DISCUSSION

The software practitioners are aware with the importance of secure software practices. However, their experience in implementing the proper practices still can be considered as low. Although the respondents faced many security incidents such as password cracking and SQL injection (Refer Figure 1), most of them did not consider security requirements from the early stage of software development, but only dealt with security requirements during the implementation phase or after the system being developed (Refer Table 4). This result is aligned with the outcomes of [11] whereby most of their respondents left the security requirements undocumented and only consider them implicitly. However, incorporating security in later stages of software development will increase the risks of introducing security vulnerabilities into software. On the other hand, the outcome of Errata Security survey [10] found that half of the respondents gave high concern on security during software development. There exist among the respondents who discuss the security requirement from early stages, yet, they do not document them. Fortunately, some of the respondents gather and document the security requirements from early stage. This explains that there are among the respondents who are aware about the importance of security activities during software development. Similar outcome is found in [10].

In addition, representing the security requirements in particular notation is vital in order to get good understanding about the requirement of proposed system. Yet, majority of the respondents do not even document the security requirements (Refer Table 5). In contrast, Elahi et al. [11] indicated that their respondents used modelling notations widely. By neglecting this important software practice, the software practitioners might ignore relevant threats that might surface in the proposed system. Fortunately, there exist among them who use abuse case, misuse case, attack tree and misuser stories.

Moreover, to efficiently elicit security requirements, software practitioners should refer to references which provide guidelines on handling security issues. Majority of the respondents referred to the documents which record the previous attacks occurred, which is aligned with the findings from the study of Elahi et al. [11]. They also consulted security experts and looked for the common attacks from the attack and vulnerability database. However, almost half of the respondents did not make any security references while eliciting security requirements (Refer Table 6). This might cause the software practitioners to be outdated from the current threats, attacks and countermeasure available in the industry, as well as repeating the same threats which occurred in previous projects.

Besides, trainings have been accepted as one of the major ways to create awareness on the security issues among the software practitioners. However, less security trainings are provided for the respondents, whereby majority of them attended security trainings only for 25% or less (Refer Table 6). On top of that, there exist among them who did not receive any security trainings. This result is contradicted with the findings in the study of Elahi et al. [11]. Without attending proper trainings may lead to improper implementation of secure software practices, since proper guideline on its actual implementation is not received.

CONCLUSION

This study has discussed the software practitioners' experiences and practices with the secure software practices in Malaysia. It is found that software practitioners in Malaysia are increasingly becoming aware on the importance of the secure software practices. However, they are lack of its proper implementation. This might possibly because less security trainings are provided to them. Nonetheless, with the current business environment which is fast-paced and exposed to threats, software practitioners must include secure software practices when developing software. For our next step, the important secure software practices that influence the quality of software will be investigated and included in the proposed software process certification model.

ACKNOWLEDGMENT

The authors would like to thank the participants of this study. Additionally, special thanks go to the Ministry of Higher Education for supporting this study through the FRGS grant (S/O Code: 11889).

REFERENCES

1. K. L. Koi. 15200 cases of cyber crimes last year. *New Straits Times*. Retreived from http://www.nst.com.my/opinion/columnist/15-200-cases-of-cyber-crimes-last-year-1.30592 (2012)
2. Bernama. Malaysia sixth most vulnerable to cyber crime. *The Star*. Retreived from http://www.thestar.com.my/News/Nation/2013/05/16/Malaysia-sixth-most-vulnerable-to-cyber-crime/(2013)
3. N. R. Mead. *Security requirement engineering*, BSI Articles, SEI Institute (2010).
4. G. McGraw. *Building security in*. Boston: Pearson Education (2006)
5. McGraw, G. (2004). Software security. *Security & Privacy*, *IEEE*, *2*(2), 80-83. doi: 10.1109/MSECP.2004.1281254
6. Fauziah Baharom, Aziz Deraman and Abdul Razak Hamdan . "A survey on the current practices of software development process in Malaysia". *Journal of ICT*, 57-76 (2005).
7. Yazrina Yahya, Maryati Mohd Yusof, Mohammed Yusof and Nazlia Omar. "The use of Information System development methodology in Malaysia". Jurnal Antarabangsa,15-34 (2002).
8. Whitehat Security. Website security statistics report, WhiteHat Security, California (2013).
9. National Cyber Security Alliance.National small business study (2010).
10. D. Geer. "Are companies actually using secure development life cycles?". *Comp.*, ***43*****(6)**, 12-16 (2010).
11. G. Elahi,, E.Yu, L and Tong, L.Lin. "Security requirements engineering in the wild: a survey of common practices". *IEEE Ann. Comp.Soft. and App. Conf.* 314-319 (2011).
12. J.Wilander and J.Gustavsson. "Security requirements–A field study of current practice". *Symp. on Req. Eng. for IS* (2005).
13. Amjed Tahir, Rodina Ahmad and Zarinah Mohd Kasirun. An empirical study on the use of standards and procedures in software development projects. *Int.Conf.on Soft.Tec.& Eng* (2010).
14. Ani Liza Asnawi, A. M. Gravell, and G. B. Wills. Factor analysis: Investigating important aspects for agile adoption in Malaysia. *AGILE India, 60-63* (2012).