Association for Information Systems
AIS Electronic Library (AISeL)

PACIS 2017 Proceedings

Pacific Asia Conference on Information Systems (PACIS)

Summer 2017

Security-Based BYOD Risk Assessment Metamodelling Approach

Zamhariah Md. Zain
Universiti Teknologi Malaysia, zamhariahzain@gmail.com

Siti Hajar Othman
Universiti Teknologi Malaysia, hajar@utm.my

Rashidah Kadir
Universiti Teknologi Malaysia, rashidah@utm.my

Security-Based BYOD Risk Assessment Metamodelling Approach

Research-in-Progress

Zamhariah Md. Zain[1], Siti Hajar Othman[2], Rashidah Kadir[3]
[1],[2],[3]Department of Computer Science
Faculty of Computing,
Universiti Teknologi Malaysia,
81310 Skudai, Johor, Malaysia
zamhariahzain@gmail.com[1], hajar@utm.my[2], rashidah@utm.my[3]

Abstract

Rapid changes in mobile computing and modern devices, for example, smartphones, tablets and iPads encouraged the employees to use their personal devices at the workplace. Bring Your Own Devices (BYOD) phenomenon has become pervasive and on-demand for business purposes. Nowadays, employees are allowed to bring personal devices to their workplace. Nevertheless, organizations are practicing BYOD to increase efficiency, work productivity, and cost-saving which lead to employee's satisfaction. However, BYOD may cause harm in an organization if there are no security policies, regulations and management of the employee's devices. The common security threats engaged to BYOD implementation are data leakage, exposed to malicious malware and sensitive corporates information. Hence, this study proposed a strategic solution, which is Security-Based BYOD Risk Assessment Metamodel (Security-Based BYODRAM) in reducing BYOD-related issues. The existing BYOD models were reviewed to identify the important concepts in the metamodel development. The Meta Object Facility (MOF) language was used to develop the proposed metamodel.

Keywords: Metamodelling, metamodel, risk assessment, security, BYOD

Introduction

Recently, the use of BYOD in enterprises have become extensive and the operational methods for the devices are rapidly changing over time. BYOD refers to allowing employees' using their own mobile devices such as smartphones, tablets, laptops and iPads for their work purpose. Since 2012, the use of personal devices at the workplace has become pervasive (Jamaluddin et al. 2015). The business benefits of practicing BYOD in the enterprise is it can improve the productivity of the worker, cost saving, increase employee's satisfaction and simplify the corporate system management. These proved with the assertion of previous research that claimed BYOD usage is a good practice in an enterprise since it can increase work quality, comfort and reduce the cost of IT infrastructure management (Fiorenza 2013). However, the companies also have high tendencies of getting risks results from the BYOD implementation. Data leakage, confidential data concern, and malware threats are examples of BYOD risks.

This paper aims to develop a Security-Based BYODRAM to provide the users with security-based knowledge in assessing risks and actions in facing various BYOD risks. For Security-Based BYODRAM development, Meta Object Facility (MOF) is adapted for the metamodelling process. The proposed metamodel covers four main views (*Prepare, Analyse, Assess* and *Control* phases, class of concepts). The rest of this paper is organized as follows: The first part of this paper describes the background and related work. The second part describes the research method in developing the metamodel. Third part describes the metamodel development based on the existing models. While the fourth part presents the Security-Based BYODRAM and the results from the metamodel. The fifth part describes the techniques used in validating the developed metamodel. Finally, this paper is concluded with the future works of this research.

Background and Related Work

BYOD has created a new business phenomenon in the smart enterprise environment (Miller et al. 2012). It also can be referred as a new independence in mobile computing that grows extensively in the worldwide. In general, BYOD allows employees to bring and use their own devices at work. Employees also can create, store, and manage the corporate data using the devices. As noted by (Qing 2013), it is about more than 71 percent of organizations that undergo at least one process changes accordance to BYOD adoption. Many corporations deployed BYOD in the working environment, for example, Citriz Systems, Intel, Apple and the White House (French et al. 2014). However, there are security risks in BYOD adoption. BYOD implementation causes the greatest challenge in organizations when the confidential data not managed strategically by the organization itself (Olalere et al. 2015). BYOD policy becoming a serious phenomenon when it affects the information security risks on the employers information such as data preserving and data leakage. The employee can distribute the sensitive information of the company to others which will cause data leakage. Security risks include mobile malware attacks, for example, Trojan, virus and spyware. (Wang et al. 2014). The malware attack vector is an attack through mobile that occurs by inadvertently downloading and installing of mobile applications, for example, Dream Droid malware. Some organizations, for example, Cisco and Intel have developed BYOD solutions. Security issues in BYOD are the major factors that enterprises should concern and pay attention. This research has proposed Security-Based BYODRAM to minimize the BYOD security problems in enterprises.

Metamodelling language is self-descriptive and supports the effort in creating an efficient process for models. As mentioned earlier, MOF language will be used to develop the Security-Based BYODRAM. MOF is an Object Management Group (OMG) standard for model-driven engineering. The metamodelling approach able to minimize the BYOD security issues as the metamodel will give an advanced knowledge to the user in security-based assessing risks. Figure 1 shows the MOF Visualization. Metamodel that contains constructs and rules needed in building specific models within the domain application. In the previous research, the Disaster Management Metamodel (DMM) also used MOF in developing the metamodel to represent the domain of disaster management (Othman et al. 2014).

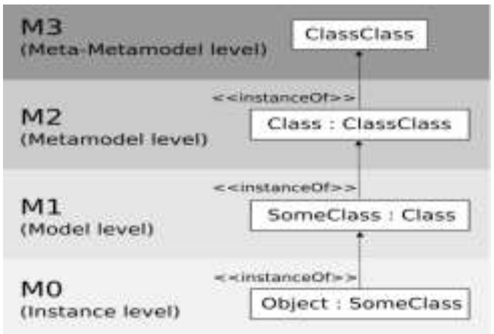

Figure 1. MOF Visualization (Thomas et al. 2014)

Security-Based BYODRAM Synthesis Process

Figure 2 shows the 7 steps that are used in the process of Security-Based BYODRAM development. The steps and operations involved in the development of Security-Based BYODRAM are well described in Figure 2. Furthermore, The *7 step Metamodelling Creation Process* are adapted from (Othman and Beydoun 2010; Othman et al. 2014).

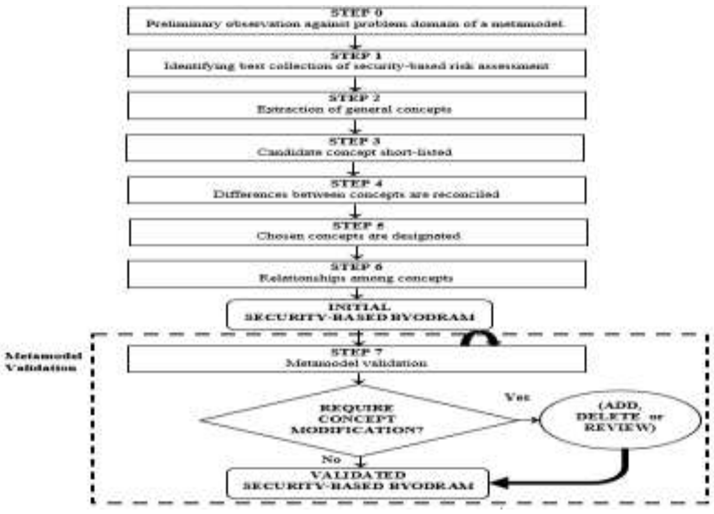
STEP 0
Preliminary observation against problem domain of a metamodel
STEP 1
Identifying best collection of security-based risk assessment
STEP 2
Extraction of general concepts
STEP 3
Candidate concept short-listed
STEP 4
Differences between concepts are reconciled
STEP 5
Chosen concepts are designated
STEP 6
Relationships among concepts
INITIAL SECURITY-BASED BYODRAM
Metamodel Validation
STEP 7
Metamodel validation
REQUIRE CONCEPT MODIFICATION?
Yes
(ADD, DELETE or REVIEW)
No
VALIDATED SECURITY-BASED BYODRAM

Figure 2. The Step-by-Step process of developing Security-Based BYODRAM

In Step 0, preliminary observation against problem domain is important to gather the problem background and preparing the knowledge of the research study. Step 1 is to identify the best collection of risk assessment models for metamodel development and validation. A collection of 20 existing models has reviewed inclusive of 10 risk assessments and 10 BYOD security models that are analysed to determine the important components for metamodel development. Step 2 is the extraction of general concepts. The concepts extraction are done by identifying the potential security and concepts that are needed in assessing BYOD risks. In Step 3, all the collection of concepts in the risk assessment models is reviewed and refined. The process to harmonize the definition of the metamodel is required when two or more concepts shared the same concept name or more concepts shared the same definition. In Step 4, differences between concepts are reconciled. The process to harmonize the definition of the metamodel is needed if there are any contradictory in using the concept definition between two or more sources. Next Step 5, which is the chosen concepts are designated. Designation of concepts is done based on the analysis and reviews in order to produce a new concept. This step is important because it includes all the important activities from chosen concepts. Step 6 represents the relationships among the main concepts. The output from this step is the initial version of Security-Based BYODRAM. The final step is the metamodel validation. This step is required to validate the developed metamodel through the completeness, efficiency and coverage covered.

Development of Security-Based BYODRAM

This section includes the detailed development process of Security-Based BYODRAM from Step 1 until Step 7.

Step 1: Identify Risk Assessment Models

Table 1 shows the sample of Set I models that consist of 20 existing risk assessment models and BYOD security models. The 20 models are classified based on model name, published year, source, R coverage and perspective of models. Concluding from the review, most of the concepts used in the existing models are *Prepare*, *Analyse*, *Assess,* and *Control* concepts.

SET I (Models to be used in Step 2 of Security-Based BYOD Risk Assessment Metamodelling Creation Process)		**Year Publish**	**Source**	**R Coverage**	**Coverage of Model Perspectives**
1.	Risk Assessment Process Model	2012	Journal	0.4	*Prepare, Analyze, Assess, Control*
2.	BYOD Security Framework	2015	Journal	0.4	*Prepare, Analyze, Assess, Control*

Table 1. Set I (Step 2 of Security-Based BYODRA Metamodelling Process)

Step 2: Extraction of Model Concepts

This section covers the extraction concepts based on the 20 existing models reviews. Table 2 shows the sample of main concepts that obtained from the existing models. The models adopt these main concepts to establish a good context for the security-based risk assessment. This planning is performed by using strategic steps for risk assessment.

Model	First Concept	Second Concept	Third Concept	Fourth Concept
Risk Assessment Process Model	*Prepare*	*Conduct*	*Communicate*	*Maintain*
BYOD Security Framework	*Plan*	*Identify*	*Information*	*Security*

Table 2. Sample of Concepts that derives from 20 Existing Models

Step 3 and 4: Short-listing and Reconciliation of Candidates Concept Definition

For the short-listed concepts, it is classified by differentiates of the assessing risk concepts with other concepts that are not relevant and cannot be used to develop Security-Based BYODRAM. Thus, only assessing risk concepts are chosen and drawn from the 20 existing models. This method is from the Framework for Agent Modelling Language (FAML) Creation Process by (Othman and Beydoun 2013). Next is the reconcilement concept of 20 existing risk assessing models. For an example, '*Prepare*' definition in Risk Assessment Process model is preparing all activities in risk assessments and the tasks that consist of identifying the purpose, scope, expectation and the constraints, assessment sources, and risk model (NIST 2012). In BYOD Security Framework, the model represents the concepts of '*Plan*' which is referring to the same meaning of '*Prepare*' concepts. The '*Plan*' concepts include planning user identification, resources needed, BYOD Standards and context establishment. The concept definition of *'Prepare'* and *'Plan'* concepts are both referring to the similar meaning even they have different concept name.

Step 5: Designate Concepts

There are four main phases in the Security-Based BYODRAM which are *Prepare, Analyse, Assess* and *Control* that encompasses with the security and risk assessment concepts. *Prepare* is the phase where the preparation of the overall plans, tasks, and related information regarding BYOD risk problems. *Analyse* phase undergo analysis of risk characterization, prevention method, impact and critical factors of the BYOD risk as to get the valuable results to improve the risk assessment approach if there are any lacks. For *Assess* phase, it is designed to make an evaluation or assessment to determine the likelihood or possibilities of risk to occur, categorize the risks, and determine the risk level. *Control* will provide all the procedure of prevention, mitigation, and control methods to minimize the BYOD security issues. The designation of Security-Based BYODRAM concepts is as shown in Table 3.

Prepare	Analyze	Assess	Control
BYOD Assessment Plan	*Structural Analysis*	*Risk Prioritization*	*Risk Mitigation*
Business	*BYOD Risk Analysis Strategy*	*RiskMatrix*	*Assessment Categorization*

Table 3. Sample Designation of Security-Based BYODRAM Concepts

Step 6: Relationship among Concepts

Table 4 shows the sample relationships created between the four concepts such as *Prepare, Analyse, Assess* and *Control*. The relationship used to provide relationships among the concepts. Association, aggregation and generalize relationships are used to create the relationships. The association relationship denoted by —, while aggregation using —◇ and generalize relationship is denoted by —▷ . There are two concepts that are being associated or created with the relationship. Based on the suitability of the function, one of the concept can perform with another concept. As shown in Table 4, *Structural Analysis* used the aggregation to create a relationship with *BYOD Risk Analysis Strategy* concept. According to the concept understanding, *Structural Analysis* use the 'Aggregation-'is A Group

Of' relationship with *BYOD Risk Analysis Strategy* concept to ensure a strategic analysis plan. This concludes that this step can generate the functional relationships for the concept.

Concept 1	Relationship	Concept 2	Phase
Survey	Specialization– '*isAKindOf*'	*Preliminary Investigation*	Prepare
BYOD Risk Analysis Strategy	Aggregation– '*isAGroupOf*'	*Structural Analysis*	Analyse

Table 4. Sample of Relationships created among Concepts

Resultant of Security-Based BYODRAM

Following are the metamodel development steps, which produce significant results to the users:

a) The result of this study is the proposed Security-Based BYODRAM that grouped into four classes which include four main phases such as *Prepare* phase, *Analyse* phase, *Assess* phase and *Control* phase.
b) Security-Based BYODRAM navigation prototype functions in giving knowledge to the users on how to solve BYOD risk problems. The navigation metamodel is based on the conceptual data of Security-Based BYODRAM and users can navigate the prototype.
c) With Security-Based BYODRAM, users can assess the BYOD risks to determine the risk level.

The four main phases of an initial version of Security-Based BYODRAM such as *Prepare* phase (Figure 3), *Analyse* phase (Figure 4), *Assess* phase (Figure 5) and *Control* phase (Figure 6) are illustrated in the stated figures. Survey and Interview concepts are as shown in Figure 3. The preliminary investigation concept is to collect the findings from the problem domain. The Business, Technology Team, and Organization concept is a group of BYOD Assessment Plan. The Technology Team concept functions in planning the technology implementation and manages the technology cost in an organization. Technology Team will plan for the BYOD Assessment Plan based on the model reviews and assured it can be practically used in any enterprise environment.

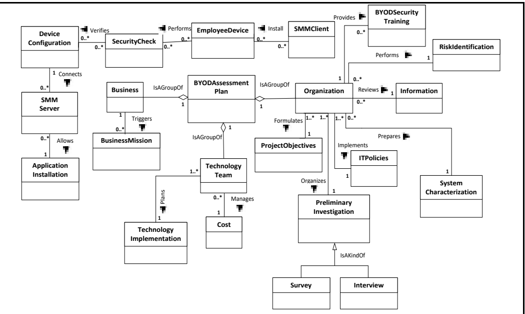

Figure 3. Prepare-phase class

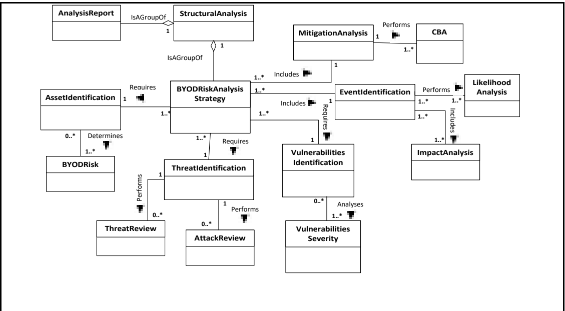

Figure 4. Analyse-phase class

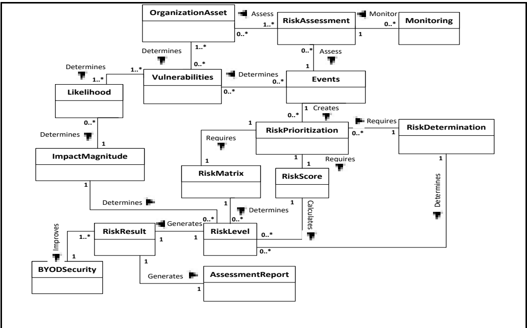

Figure 5. Assess-phase class

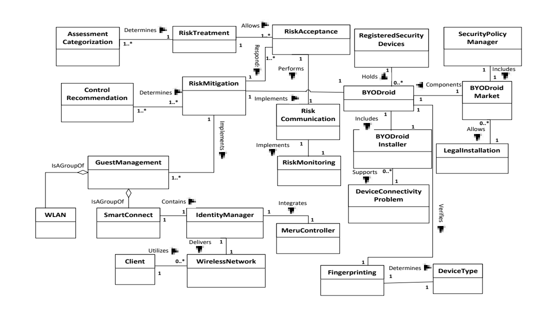

Figure 6. Control-phase class

Techniques used in Metamodel Validation

Security-Based BYODRAM development requires validation to check the completeness of the important components. For the purpose of validation, three types of validation are chosen, namely comparison to other models, face validity and tracing. For the comparison to other models validation, concepts of the developed metamodel are being compared to other 15 models under the same domain. Face validity is aimed to validate the correctness of the metamodel by interviewing the domain experts to ensure the metamodel or main concepts used are reasonable. Tracing will be performed to evaluate the logics of the proposed concepts in the developed metamodel. Therefore, for performing 'Tracing', the Ottawa Hospital case study will be used to map concepts in the metamodel.

Conclusion

This article has proposed the Security-Based BYODRAM metamodel which has four main phases: *Prepare*, *Analyse, Assess*, and *Control* phases to assess security risk in organizations. For each phase, it includes the plans and steps that are needed to accomplish the BYOD goals. Based on the reviews of the 20 existing models, the concept of *Prepare*, *Analyse, Assess*, and *Control* are common concepts used in risk assessment and BYOD security models. For future works, it is good to have an automated application that can be used by the users to overcome the BYOD-related security problems faster. It is suggested for the future researchers to use Artificial Intelligence aspects in designing the Security-based BYODRAM application. Thus, the researchers could enhance the metamodel by applying new practicable concepts.

Acknowledgements

This research is under the Tier 1 Research Grant (Vote Q.J130000.2528.14H82) supported by the Ministry of Higher Education Malaysia (MOHE) by sponsoring the first author of this article, Universiti Teknologi Malaysia (UTM).

References

Fiorenza, P. 2013. "Mobile Technology Forces Study of Bring Your Own Device," *Public Manager*, (42), pp. 12–14.

French, A., Guo, C., and Shim, J. P. 2014. "Current Status, Issues and future of bring your own device (BYOD)," *Communications of the Association for Information Systems*, (35:11), p. 10.

Jamaluddin, H., Ahmad, Z., Alias, M., and Simun, M. 2015. "Personal Internet Use: The Use of Personal Mobile Devices at the Workplace," *Procedia - Social and Behavioral Sciences*, (172), Elsevier B.V., pp. 495–502.

Miller, K. W., Voas, J., and Hurlburt, G. F. 2012. "Byod: Security and Privacy Considerations," *It Professional* (14:5), pp. 53-55.

NIST Special Publication 800-30 Revision 1. 2012. "Information Security - Guide for Conducting Risk Assessments,".

Olalere, M., Abdullah, M. T., Mahmod, R., and Abdullah, A. 2015. "A Review of Bring Your Own Device on Security Issues," *SAGE Open*, (5:2), p. 2158244015580372-.

Othman, S. H., and Beydoun, G. 2010. "Metamodelling Approach To Support Disaster Management Knowledge Sharing," *ACIS 2010 Proceedings*, (2010), pp. 1–10.

Othman, S. H., and Beydoun, G. 2013. "Model-Driven Disaster Management," *Information & Management* (50:5), pp. 218-228.

Othman, S. H., Beydoun, G., and Sugumaran, V. 2014. "Development and validation of a Disaster Management Metamodel (DMM)," *Information Processing and Management*, (50:2), Elsevier Ltd, pp. 235–271.

Qing, L. 2013. "Byod on Rise in Asia, but Challenges Remain," *ZDNET*.

Thomas, K., Leuth, M., and Sebastian, G. 2014. "A Metamodel Family for Role-Based Modeling and Programming Languages," *Software Language Engineering. Springer International Publishing*, pp. 141–160.

Wang, Y., Wei, J., and Vangury, K. 2014. "Bring your own device security issues and challenges," *2014 IEEE 11th Consumer Communications and Networking Conference (CCNC)*, pp. 80–85.