View metadata, citation and similar papers at core.ac.uk

brought to you by CORE

provided by ExcelingTech Publishing Company (E-Journals)

A Secured Model of E-Tendering Using Unified Modeling Language Approach

Haslina Mohd[1], Fauziah Baharom[2], Norida Muhd Darus,[3] Mohamed Ali Saip[4], Zaharin Marzuki[5]

School of Computing
University Utara Malaysia, Malaysia
[1]haslina@uum.edu.my
[2]fauziah@uum.edu.my
[3]nor854@uum.edu.my
[4]mdali@uum.edu.my
[5]zaharin@uum.edu.my

***Abstract*— This E-Tendering systems remain uncertain on issues relating to legal and security compliance, in which unclear security framework is one of the issues. In te current situation, tendering systems are lacking in addressing integrity, confidentiality, authentication, and non-repudiation. Thus, ensuring the system requirements, consider security and trust issues has to be regarded as one of the challenges in developing an e-Tendering system. Therefore, this paper a model of a secured e-Tendering system using Unified Modeling Language (UML) approach. The modelling process begins with identifying the e-Tendering process, which is based on Australian Standard Code of Tendering (AS 4120-1994). It is followed by identifying the security threats and its countermeasure. The use case approach has been proven reliable in determining appropriate requirements for handling security issues. Having considered that, the outcome of this paper is a secured e-Tendering model. The model can guide developers as well as other researchers.**

***Keywords*—** *e-Tendering, IT Project, Security threats and counter measure; misuse case.*

1. Introduction

Tendering refers to the process of choosing the best offer for certain needs, through a principle, involving a legally binding contract [1, 2]. The tendering process involves two parties, (1) Tenderer – any party submitting tenders, including contractor, subcontractor, and supplier [3], and (2) Principal – any party inviting and receiving tenders, which may include contractor or subcontractor [3]. Generally, the process involves four stages; announcement of tender lists, submission of tender proposals, assessment of the proposals, and acceptance of the proposal[3]. However, it could be adapted to suit the context. As an example, Australian Standard Code of Tendering [3] underlines seven components, which extends the general tendering process; registration of qualified tenderer, public announcement of tender lists, submission of tender proposals, close of tender, assessment of tender proposals, award of tender, and archival of the tender.

Now, the tendering process could be carried out electronically (e-tendering). E-tendering translates the tendering process into an electronic form. It refers to the electronic publishing, in which accessing, communicating, receiving, and submitting of every information and document are carried out via the Internet. This has been proven to offer a more efficient and effective process in the business, which also reduces cost significantly (NT Government; NSW Department of Commerce) [3]. However, even though there is a significant improvement in the e-Tendering over the conventional technique, in terms of reduction of capital and time, and less reliance on human capability [4], it is still lacking and uncertain in terms of legal and security issues [5]. In terms of this, such systems have vague framework. It was also found that transactions are not highly trusted and users are not sure of the system's ownership [6,7,8]. When the security is not protected, many cases have shown that hacking, pirating, virus, fraud, illegal trading, defamatory libel, and money laundry have been [9,10,11] negatively impacting users' trust. As a result, studies need to identify all possible threats and determine the most appropriate solution so that the e-tendering process secures and make users feel confident.

Not only that, tendering systems also deal with transparency, accountability, integrity, corruption,

International Journal of Supply Chain Management
IJSCM, ISSN: 2050-7399 (Online), 2051-3771 (Print)
Copyright © ExcelingTech Pub, UK (http://excelingtech.co.uk/)

and cronyism issues [12]. This deals closely with trust. However, most existing e-tendering systems do not address them, leaving such issues unattended. As result, it negatively affects the utilization of the e-Tendering systems too. Thus, studies also need to determine the solutions for that. Therefore, this paper aims to model a secure e-tendering system using misuse case approach.

2. Modeling Process of the e-Tendering

The modelling process comprises of four phases. It begins with identifying the e-tendering process (based on the Australian Standard Code of Tendering [3]), followed by identifying the security threat, and it countermeasures the system. Finally, based on the identified secured e-tendering, the modelling process commenced using misuse case approach.

Phase 1: Identifying e-tendering process

E-tendering process by the Australian Standard Code of Tendering procedures [3] is almost similar to the traditional tender process. It varies only on certain procedures for certain particular systems. Accordingly, the common features are mapped against the general component of the conventional tendering process. The outcome of this phase is the e-Tendering processes that this study further uses as the benchmark in constructing a secured e-Tendering model. Among the various stages in the tendering process, this paper focuses only on public invitation and tender submission components.

Phase 2: Identifying e-tendering security threats and countermeasures of the security threats

Threat is a potential activity that could lead to vulnerability of the e-Tendering system [13]. Identifying threat is important to ensure such system is secured. It could be done by eliciting the security requirements for the system. For this study, the elicitation was made through discussions in related journal articles on security mechanism of electronic application. The threats and secured practices listed in a matrix. The matrix of the threats and possible security practices are discussed in the following section.

Phase 3: Constructing a secured e-Tendering model on public invitation and tender submission

The aim of this phase is to construct a secure e-Tendering model. Findings from the previous phases are used to construct the model. The model is based on generic components of e-Tendering and security requirements. The generic components of the e-Tendering requirements drive as the basis for eliciting the functional user requirements. Meanwhile, the security-focused requirements have been regarded as non-functional requirements that are specified as supplementary specifications. The detailed activities for each phase are described in the following section. In each phase, a set of related UML model has been developed to illustrate both process (public invitation and tender submission).

2.1 Finding of the E-Tendering Modeling Process

Equations Table 1 shows the mapping between the components of the e-Tendering system and the Australian Standard Code of Tendering procedures [3].

Table 1. E-Tendering System Components

Tendering System Component [3]	**E-tendering General System Function (Conventional Tender Process)**
Registration of tenderers	Pre-registration
	Tenderers are issued with password and id.
Public announcement of tender	Advertisement of tender in public newspapers
	Tenderer views the tender advertisement
Submission of tender proposal	Tenderer registers for the tender
	Tenderer downloads tender documents
	Tenderer submits tender proposal
Close of tender	Tender is closed
	The principal opens the tender proposals
Tender evaluation	The proposals are assessed
	Principle requests for additional information
	Most qualified proposal is awarded the tender
Award of Tender	A formal agreement is signed by both parties
Archiving	Documents are archived

The e-Tendering process in Table 1 is used in this study as the benchmark in modelling a secured e-Tendering system, specifically for public invitation and tender submission processes (shaded in Table 1). The modelling process is detailed in the modelling section.

2.2 Security Threats and Countermeasures

Generally, threats and possible violations comprise actions that insecure secured e-Tendering systems. That is why they have to be carefully handled. Hence, the identification of threat and security problem enable this study to define the system requirements as well as its security requirements. Accordingly, with reference to [14], the requirements are listed below:

- Impersonate - it is common in terms of identifying fraud and malicious parties. It is dangerous because other parties could have similar access to tenderer's account and do whatever they intend.
- Repudiation - the third party could deny or decline any content while communicating, especially during tender process. This could dispute principal and tender.
- Confidential violation – sensitive information is viewed by unauthorized malicious parties. Then, they could notice about the tender progress and distort the process.
- Non-verifiable evidence – in most cases, tenderers could make a claim for fair treatment when they are unable to meet the tender requirements because they do not have access to the right information.
- Denial of service – processing of user requests are discarded when technical problems happen.
- Integrity violation - malicious party changes, alters or deletes information or document submitted by the tenderers or the principle.

The requirements listed above are used in this study to determine how they affect the tendering process. Hence, a matrix is come out with, which is adapted from Cooperative Research Centre for Construction Innovation Technical (CRCCIT). Accordingly, Table 2 details the possible threats in tendering process along the phases outlined in Table 1.

Table 2. Possible Threats in Tendering Process

-Tendering Phases	TIV	IV	CV	I	NVE	DoS	R
-Qualification and registration	-	Yes	Yes	Yes	Yes	-	-
blic invitation	-	Yes	Yes	Yes	Yes	-	-
Tender submission	Yes	Yes	Yes	Yes	-	Yes	Yes
Close tender	Yes	Yes	Yes	Yes	-	Yes	Yes
Tender evaluation	-	Yes		-	Yes	-	-
ward of tender	-	Yes	Yes	Yes	Yes	-	Yes
Archiving	-	Yes	Yes	-	-	-	-

Note: ITV-Time Integrity Violation, IV-Integrity Violation, CV=Confidential Violation, I-Impersonation, NVE-Non-Verifiable Evidence, DoS-Denial of Services, R-Repudiation.

Further, Table 3 details the countermeasure for the e-Tendering security threats in this study.

Table 3. Countermeasures of the in e-Tendering Security Threats based on Non-Functional Requirements

Non-Functional Requirements	Countermeasures
1) Integrity (ISO 27000-Information Security)	To protect the original data from manipulation by malicious party. The integrity property is maintained, in which the recipient is allowed to identify whether the message is in original state. It is to ensuring the data is genuine. Appropriate security tools for this include secure sockets layer (SSL) for communication integrity, digital time stamping to provide timestamp integrity, biometric, and digital signature.
2) Confidentiality (ISO 27000-Information Security)	To avoid information leaking during communication to ensure confidentiality. This could be done using cryptography encryption.
3) Data Origin authentication [15]	Allowing the recipient to verify the messages to ensure they have not been tampered in transit and that they come from an expected sender. This sis possible done using proof-of-possion.
4) Availability (ISO 27000-Information Security)	To ensure only authorized parties can have access to the data after getting into the system. In response to that, this study recommends all principles to ensure the

	system is available at all time.
5) Non-Repudation [16,17]	Is crucial in handling legal issues in providing evidence to debate or officially accept a business transaction. For this, the evidences have to be at all time available.
6) System Reliability [15]	This requires the system to be performing what it is supposed to at all time under stated conditions.

Having the e-Tendering process, threat and countermeasure, and security solution determined, the misuse case modelling is constructed as discussed in the following section.

2.3 Constructing a Secure e-Tendering Model

This study uses Unified Modelling Language (UML) to model the secured e-Tendering model. The scenarios described below are used as the basis in designing the misuse cases:

Step1: Context and Asset Identification. The context of the advertisement and submitting tenders process is shown in the use case in Figure 1. The figure explains that the Principal will first advertise the tender list in public newspapers. It enables tenderers to notice the tender availability. Then, on tenderers' part, they will view the tenders and register for the preferred tender, subjected to their qualification. Having registered, the system will let them (the tenderer) to download appropriate documents, including tender specification. At the same time, the system will record the registration. Eventually, the tenderer has to submit their tender proposal before the stipulated date.

Step 2: Security objective determination. The use case in Figure 1 cannot be used to show the vulnerable assets and security criteria. It can only be used to tell the reason about the security criteria. Among the whole process, this paper discusses three processes: i) tender submission; ii) ensuring the integrity of tender advertisement; and iii) receiving tender document by the principal. This means the submitted tender document cannot be changed once the tender advertisement is published.

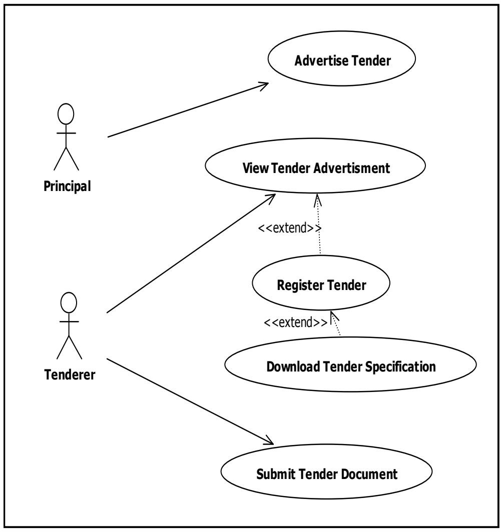

Figure 1. Use Case Modeling of the e-Tendering (Open Tender Component)

Step 3: Risk analysis and assessment. Figure 2 is a use case for the possible threat modelling in the tendering process particularly during the tender is being advertised and submitted. The Attacker in the use case threats the integrity of the advertisement because it could steal principal's identity. This could fake the advertisement. This is a serious matter in the process. Accordingly, the tenderer may take wrong actions as a response to modified information, including late submission.

Step 4: Risk treatment. The use case in Figure 2 suggests no risk treatment. However, specifying appropriate treatments for each particular risk could be done through relationship mitigation.

Step 5: Security requirements definition. Possible threats that may attack the tendering process is also shown in the use case in Figure 2, which is adapted from [18]. However, the security solution is not available in Figure 2. Meanwhile, Figure 3 shows that each threat has its own mitigation relation. This mitigation relation acts as a countermeasure for specific threat that can reduce the effect of vulnerabilities.

Step 6: Control selection and implementation. Use cases suggest no technique for selecting and implementing control mechanism.

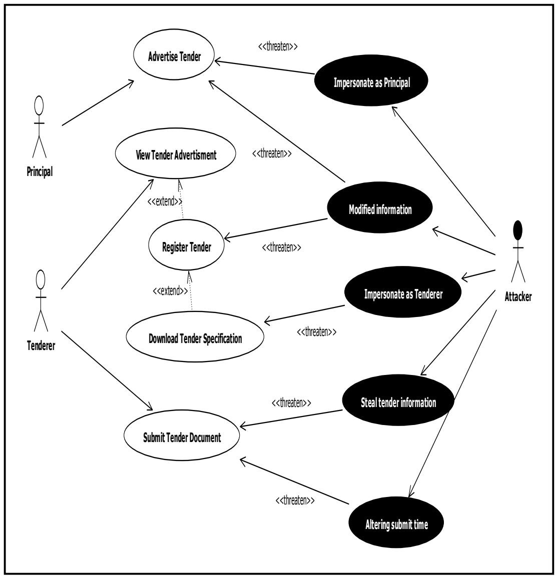

Figure 2. Threat Modeling of e-Tendering System

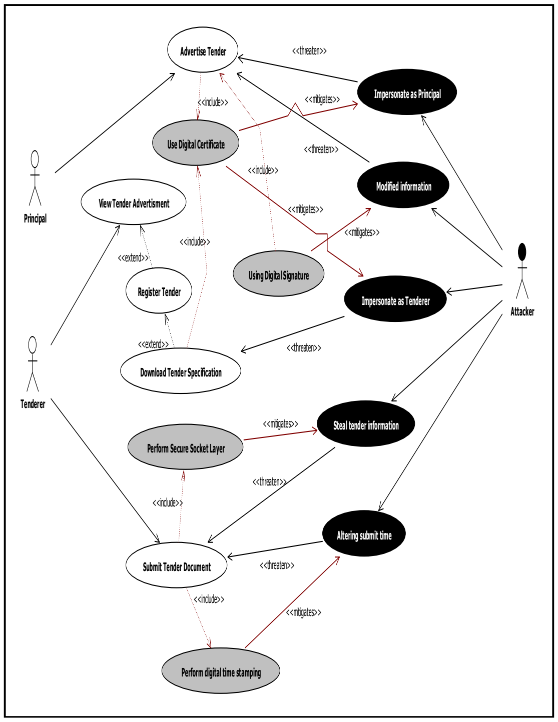

Figure 3. Modelling of Security Requirement of e-Tendering System

3. Discussion And Conclusion

This study retains the security and accountability of trust as they are emphasized in conventional tendering process. Hence, the e-Tendering framework that this study proposes is capable to deliver the same quality with more efficient and effective business process. Based on the framework, to cater for the ethical issue, developers of the e-Tendering systems should also consider technological factors that expose information malicious parties to invade or attack the system. In particular, the utilization of digital signature could curb ethical issues like repudiation in the e-Tendering system. It is a second layer authentication. Obviously, a secured e-Tendering system is not enough with a simple cryptographic algorithm for document transfer because any transacted document cannot be trusted since it may come from impersonator. These are only some examples of security issues in e-Tendering that might require security mechanisms to overcome the problem. Without a proper planning, developing and maintaining the system might consume high cost. Besides that, developers should also consider other security issues and threats like integrity, confidentiality, non-repudiation, and availability, which interrelate among each other and involve organizational practice and regulations.

As a response to that, this paper exhibits the use cases that map the security risk in the tendering phases and countermeasure in overcoming security problems. However, the use cases only showcase what malicious parties could do. However, through the use of mitigation relationship, it is able to show what a user can do or enforce to curb the misdeeds by malicious parties. Also based on the use cases, developers are able to clarify what happens in the e-Tendering system (similarly to the use case function) in order to enforce security mechanism in a secured e-Tendering system.

Acknowledgments

This study was funded by University Utara Malaysia under PBIT grant scheme. Special thanks to all research members in Software Technology Research Group (SOFTECH) for their commitment in completing this research.

References

[1] C.P. Thorpe, and J.C.L. Bailey, "*Commercial Contract. A practical guide to deals, contracts, agreements and promises*," Woodhead, Cambridge England, 1996.

[2] I. Atlas, A. Pitney, J. Curtis, P. Greenham, G. Hanly, D. Glodstein, J. Mansfield, and T. Grace, *The Tendering Process*. BLEC Business Law Education Center from the Training Division of Longman Cheshire, 1993.

[3] AS 4120, *Standard Australia Committee on Construction Industry Practices. Code of Tendering, Australia Standard.* Standards

Association of Australia, 1 the Crescent, Homebush, NSW 2140, 28 October 1994.

[4] C. W. Lou, and M. Alshawi, "*Critical success factors for e-tendering implementation in construction collaborative environments: people and process issues*," ITcon Vol. 14 , pp. 98-109, 2009.

[5] D. Betts, P. Black, S. Christensen, E. Dawson, R. Du, and W. Duncan, "*Towards secure and legal e-tendering,*" Journal of Information and Tecnology in Contruction, XI , 89-102, 2006.

[6] Y. Rezgui, A. Brown, G. Cooper, G. Aouad, J. Kirkham, and P. Brondon, "*An integrated framework for evolving construction models,*" 2004.

[7] V. Pasupathinathan, and J. Pieprzyk, *A fair e-tendering Protocol*, 2008.

[8] S. Kumar Dey, M. Noor Nabi, and M. Anwer, "*Challenges in building trust in B2C e-Commerce and proposal to mitigate them: developing countries perspective*," 12th International Coference on Computers and Information Technology, 2009.

[9] R. Darlington, *Crime on the net*, 2006.

[10] J. Dara, and L. Gundemoni, *Credit card security and e-payment: Enquiry into credit card fraud in e-payment*, 2006.

[11] O.S. Oyediran, and A. A. Akintola, "*A survey of the state of the art of e-tendering in nigeria*," ITcon Vol. 16 , pp.557-576, 2011.

[12] W.S. Hui, R. Othman, N.H. Omar, R. Abdul Rahman, and N.H. Haron, "*Procurement Issues in Malaysia,*" International Journal of Public Sector Management, Vol. 24, No. 6 , pp. 567-593, 2011.

[13] P. Gregory, *CISSP Guide to Security Essentials. Course Technology*, 2010.

[14] E. Dawson, S. Christensen, B. Duncan, E. Foo, R. Du, J.N. Gonzalez, J. and P. Black, *eTendering – Security and Legal Issues. Technical report, CRC Contruction Innovation,* www.consruction-innovation.info. 2006.

[15] R. Du, E. Foo, C. Boyd, K.C. Raymond, "*Formal Analysis of Secure Contracting Protocol for E-tendering,*" Australian Computer Society, pages pp 155-164, 2006.

[16] A. Rodriguez, E. Fernandez-Medina, J. Trujillo, and M. Piattini, *Secure business process model specification through a UML 2,0 activity diagram profile*, 2011.

[17] Z. Hu, *The Study of E-Commerce Security Protocol*, 2011.

[18] M. Haslina, N. Nazib, B. Fauziah, M.D. Norida, H. Nor Laily, M. Zaharin, Y. Azman, Z. Azida, "*An Investigation of Possible Security Threats and the Proposed Secure Solution for Electronic Tendering Systems of Information Technology (IT) Projects*," In Proceedings of the International Soft Science Conference 2011(ISSC2011), 23-25 November, 2011 Ho Chi Minh, Vietnam, 2011.

[19] I. Alexander, "*Misuse Cases: Use Case with Hostile Intent. IEEE Software* ", 58-66. 2003.

[20] M. El-Attar, and I. Ahmad, (2011). "*Improving Quality in Misuse Case Models: A Risk-Based Approach*". 10th IEEE/ACIS International Conference on Computer and Information Science. 2011.

[21] L. B. McGuire, and N. S. Roser. "*What your business should know about internet security"*, Strategic Finance, Vol 82, No 5 , 50-54, 2000.

[22] S. Mohammadi and H. Jahanshahi. "*A Secure E-Tendering System*", IEEE, 2009.

[23] J. J. Pauli, and D. Xu. "*Misuse Case-Based Design and Analysis of Secure Architecture*". In Proc. of International Conference on Information Technology: Coding and Computing (ITCC'05), 2005.

[24] G. Qingping, F. Li, and Y. Li. "*Probe into E-commerce Security Technology*". In Proc. of the International Forum on Computer Science-Technology and Applications, Vol.2, 425-428, pp. 25-27 Dec. 2009.

[25] G. Sindre and A. L. Opdahl. *Eliciting Security Requirements with Misuse Cases*. Requirements Engineering Journal, Vol.10, No.1, pp. 34–44, 2005.

[26] H. Songtao. *Security Strategy of E-Commerce in China. Management and Service*, Science International Conference (MASS 2011), IEEE, 2011.DOI: 10.1109/ICMSS. 2011. 5999009