Proc. of the Second Intl. Conf. on Advances in Computer and Information Technology -- ACIT 2013
Copyright © Institute of Research Engineers and Doctors. All rights reserved.
ISBN: 978-981-07-6261-2

Fuzzy-Based IntrusionTolarence for WebServices

Davoud Mougouei[1], Wan Nurhayati Wan Ab. Rahman[2],Maryam Eshraghi Evari[3]
Department of Information System
Faculty of computer Science and Information Technology
Universiti Putra Malaysia, Selangor, Malaysia

***Abstract*—Identifying threats in the stage of requirements engineering is a big and complex challenge for web services development.The challenge even grows when the massive number of security faults grows. In addition, security threats existing in a web service may increase the risk of security failure. An Electronic Portfolio System (EPS) is introduced as a web service to serve as our running example in this paper. To overcome the security threats in the target EPS, the web service has to be flexible and tolerant. EPS should tolerant in presence of inevitable security threats. This study presents a fuzzy-based approach to establish security requirements of the EPS as a web service and make a fault tolerant model for the security requirements of the service. For this purpose, we have applied a goal-based modeling approach. The approach develops an intrusion tolerant model for security requirements. The model is developed based on the formally described model of security faults (SFM). In order tomake the Security Requirement Model (SRM) of the system tolerant, the study has employed partial satisfaction of security goals. The partiality is addressed through temporal fuzzy-based language of RELAX to mitigate unavoidable threats during the requirement analysis process. Ultimately, the approach leads to a fault tolerant model for security requirements of the target EPS.**

Keywords*—fuzzy syntax; RELAX; goal-based modeling intrusion tolerance; web service security.*

I. INTRODUCTION

Thissecurity brings major challenges to the development of web services. There is not enough attention to engineering of security in the course of analysis and design [1]. Some existing approaches have considered the security analysis throughout the requirement engineering process [2]. However, it still has not specified how to automate security analysis at the requirement engineering phase. It is impossible to identify all security threats during the process of requirements engineering [3]. Hence, inevitable threats have to be removed. Threat removal may contribute to new threats. Then, it is not always possible to achieve a comprehensive intrusion tolerant model for e-portfolio web services, and all the possible security threats may not mitigated during security requirements analysis [4].This study aims at introducing a goal-oriented approach for modeling and analyzing requirements-and possible threats; to provide an intrusion tolerant e-portfolio web service. Goals describe required properties of the target web service that are satisfied by different agents such as web service components or humans in the system's environment [5].the proposed model plans to assist security analyzers in order to make the target web service intrusion tolerant in presence of unavoidable security threats. This could be obtained by factoring the security threats into the development process explicitly. The study suggested a fuzzy approach for partial satisfaction of security goals in presence of intrusion threats. In other word, if the goal refinement is not sufficient to mitigate all the security threats, applying partial satisfaction of the security goals, make the model tolerable and flexible and consequently, constructs the generated model amenable to analysis (refine) during the requirement engineering phase. Therefore, to modeling goals, the study applies the temporal fuzzy requirement engineering language of RELAX [7] incorporated into the KAOS syntax, a goal-oriented requirements engineering language [6]; an influencing factor for using KAOS is the support of threat modeling [8]. Moreover, to mitigate the security threats, formal mitigation techniques has been employed and this eventually contributes to an intrusion tolerant SRM of the target wb service [10].

Our study indicates the process of formal description of security requirements and threats. Then, it presents a novel application of fuzzy-based language of RELAX. Whereby incorporates the fault tolerance into the requirement model of the system through partial satisfaction [9] of security goals. It also explicitly factors the security faults into the requirement and fault model [8]. Finally the interrelation of SRM and SFM has been introduced, to address the mitigation of security faults.

On the oher hand, because security is a critical issue in electronic portfolio systems as discussed by [11], [20] in this paper we consider the security issues and application of proposed method in EPS. Particularly, EPS aims to keep users' document confidentiality and privacy at highest level. Additionally, it is important for EPS to hold financial losses at the minimum level in order to reach a secure portfolio web service.

The rest of the paper is organized as follows, section II describe existing security engineering and fuzzy-related techniques. In section III, details of the proposed fuzzy -modeling approach is presented. The proposed approach has applied a typical electronic portfolio service (EPS) as a case study. Finally, in section IV, concluding remarks and describing future direction of our research is offered.

SEEK DIGITAL LIBRARY

Proc. of the Second Intl. Conf. on Advances in Computer and Information Technology -- ACIT 2013
Copyright © Institute of Research Engineers and Doctors. All rights reserved.
ISBN: 978-981-07-6261-2

II. RELATED WORKS

Attack trees are one of the most applicable techniques in the field of security engineering. The attack behavior and its impacts are used to be modeled by means of attack trees. According to [13], attack trees technique was applied to analyzing threats and risks. However, this work did not mention the way threats can be mitigated. In another contribution; Edge et. in [14] suggested protection trees approach to mitigate threats. Nevertheless, He did not consider partial satisfaction towards security goals.

Attempts in [15] were targeting the aforementioned issue of partial satisfaction of security goals. Whereby a method is proposed for clarifying security requirements in order to construct anti-goals. The proposed method was performed through formal description of security goals and anti-goals in terms of first order logic expressions. In spite of that, the proposal was lack of explicit factoring the security faults into requirements. This in turn reflects some violations of the partially satisfying security goals.

Further enhancement on the former model was introduced by [16]. Wherein authors investigated the problem of partial satisfaction of goals and adopted probability theory to care for partial satisfaction degree in goal refinement process. Nevertheless, the probabilistic model did not mention the level of secureness in the software system or the way to bring security concerns into design stage.

In order to eliminate the weakness of probabilistic logic to answering partial satisfaction of goals and even to identify uncertainties during requirements engineering, [8] investigated the ability of fuzzy logic in order to "roughly" satisfying security goals. A significant work done by [4] considered security critical systems. This work tried to systemize new design principles to have a fault tolerant model. The proposal described the association of security and classical fault tolerance. Additionally, the work demonstrated the basic concepts of intrusion tolerance.

In furtherance of security considerations and involve them into development stage [2] introduced SQUARTE project. Whereby a methodology specified to prioritizing, categorizing and eliciting requirements of security engineering. SQUARTE addressed issues of traceability by specifying required tasks within each step. But this work did not determine how to describe the security requirements.

To carry off uncertainty in dynamically adaptive requirements of systems; [7] and [8] represented a textuallanguage of RELAX. The proposed language temporarily relaxed the security requirements in order to support adaptation. In [9] the author has also addressed the partial satisfaction of goals in dynamically adaptive systems by applying RELAX. The proposed technique explicitly factored uncertainty characteristics into the security engineering routine. To the best of our knowledge, this paper mentioned the work in the former model above.

Furthermore, [17] investigated the fault tolerance in some electronic applications. The authors stated that security and reliability issues are the major concerns that discourage people from engaging in electronic communications. In another attempt, [11] clearly mentioned some security issues and requirements of electronic portfolio system.

III. OVERVIEW OF APPROACH

A. E-Portfolio Security System Description

Security is a critical concern in portfolio web services, affect usability and reliability of the web service. On the other hand, maintaining integrity and availability in addition to improve confidentiality are important concepts about security of portfolio systems. This study has explored security concerns of electronic portfolio systems. We investigate validity of our proposed method on a typical electronic EPS [12] to achieve a higher level of security. The following paragraph has considered the scenario of a typical EPS:

EPS provides functionalities required for a web portfolio such as providing information related to courses, research activities and grant through the EPS. Then, it is possible to update or remove the information. EPS will charge the client for each service request and maintains the credit information of the clients. The lecturer's information may be misused by criminals. Hence, EPS transactions must be protected to keep financial losses to a minimum. The availability of EPS is as important as the confidentiality and integrity of information transmitted from EPS to the clients. The EPS also has a server which should be protected from any possible misuse. In addition to that, an attacker may exploit the EPS' internal communication network to threaten the transactions. EPS should prevent unauthorized online access to the service. Hence, it supports user authentication by checking the user name and password. However, the attacker still can guess either user name or password but it is supposed to be difficult. EPS must provide a reasonable assurance that their lecture's information is secure. The main threat that concerns EPS is that an attacker will get access to confidential information at the server side. Anotherattack is to alter or misuse the crediting information at server side.

B. EPS Security Requirements Specification

Our investigation starts with specifying security goals of EPS according to its business goals. After that, the requirements of these security goals are determined. In this step, we specify possible security faults concurrently with requirements analysis. Subsequently, we apply mitigation process to mitigate (tolerate) detected security faults. Security requirement model and security fault model of EPS are designed at this stage. To finalize the risk analysis we refine requirement and fault models. In refinement process it is possible that some goals have been modified. This process will repeatedly continue, until the Requirement model of EPS mitigates its Fault model.

SEEK DIGITAL LIBRARY

Proc. of the Second Intl. Conf. on Advances in Computer and Information Technology -- ACIT 2013
Copyright © Institute of Research Engineers and Doctors. All rights reserved.
ISBN: 978-981-07-6261-2

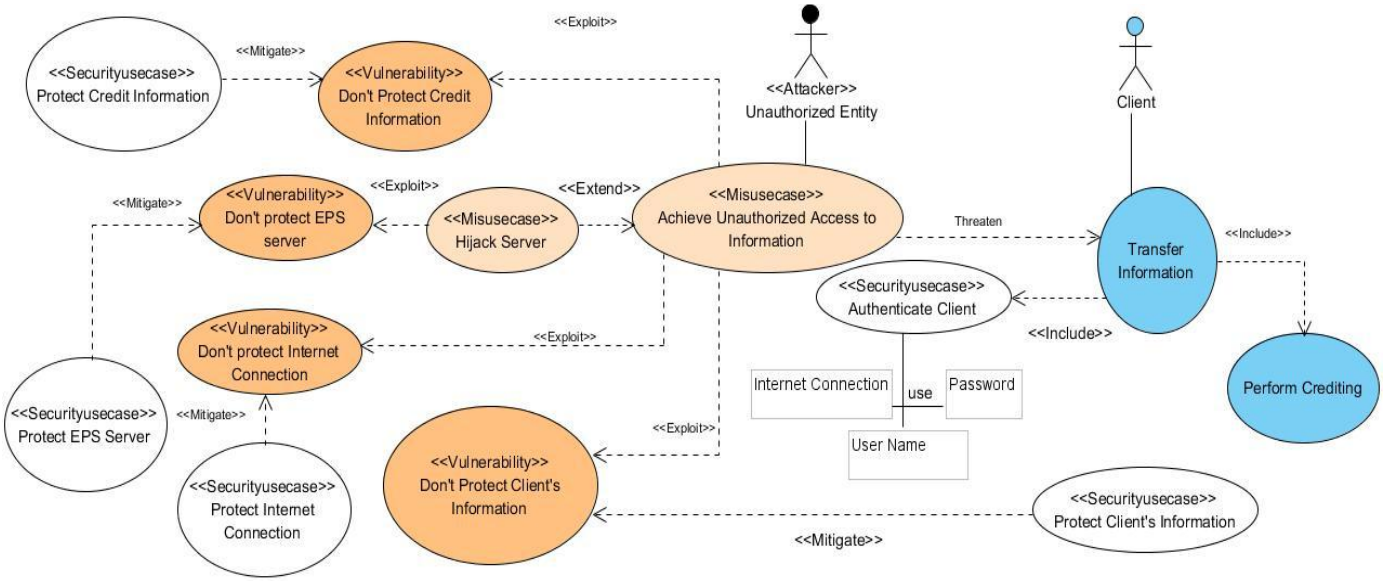

Figure 1. Use case- Misuse case model of the EPS

Requirement analysis starts with creating conceptual domain model of EPS. For this purpose, we apply UML use case and misuse case diagrams. This conceptual domain model reveal the basic scenarios/outlines and their relationships. Fig. 1 depicted the conceptual domain model of EPS and its security functionalities. Similar to what has been stated in [18]; our model also indicates that the attacker varied from harmless user.

D. EPS Security Requirement Formal Description

Model checking and mathematical analysis of the proposed SRM and SFM, need a formal description of these two models. To formally describe SRM and SFM we apply a combination of RELAX and KAOS. In fact, fuzzy nature of RELAX brings flexibility to our goal specification and analysis. Requirements and faults present in terms of RELAX statements and described with their attribute values. Table 1 shows requirements and faults attributes values.

To factor faults into SRM, it is supposed that goals are completely satisfied. However, complete satisfaction is not always possible. For this reason, we accept partial satisfaction of security goals [16]. In this statepartiality is addressed through RELAX attributes. In other words, as in [2], RELAX statements describe partiality in terms of fuzzy temporal logics during the RE process.

For each requirement in SRMwe take a ‘relax’ attribute with the value of security faults such as threats or vulnerabilities. We factorize the faults by accepting the presence of them. Then try to tolerate these faults instead of preventing or removing them. In addition, we partially satisfy security goals by using mitigation techniques. Rest of the paper will explain the approach through few steps and the way fault tolerance positively affects EPS.

A. Identification of Security Requirement Model of EPS

At the first step, to protect EPS against possible attacks, high level security goals and assets are recognized. For this purpose SRM should be initiated by refining top-level security goals. Assets are recognized based on EPS scenario, and included users’ private information, users’ accounts, and so on. Furthermore, considering EPS as a service provider leads to consider availability and reliability critical issues. The initial state of SRM is shown in Fig. 3 in terms of R1 to R4. In this state ‘attack’ goals are the inverse of ‘protect’ goals. Consequently, we initiate the SFM by inverting SRM. Fig. 2 depicted the model in terms of nodes F1 to F4.

B. Development of Security Fault Model of EPS

After EPS requirement model formed, in the next step fault model initiated based on EPS security artifacts. Artifacts included attack scenarios, attack trees, misuse cases and any other artifact which used to identify security threats in the system. It is supposed that security artifacts developed by EPS security expertise based on security fault model of a typical EPS. In this step, possible misuses which might threat the security goals also fiend.

C. Ground mitigation

EPS security requirement model is completed by mitigating the threats, represented in SFM. Considering SFM and SRM as two mathematical graphs make it easier to process SFM and generate SRM. Inverting SFM results the next generation of SRM. To illustrate, R.1.1.1 is requirement node in SRM mitigate F.1.1.1 which is a fault goal in SFM. The statement means that EPS should generally avoid highjack server. In the next step, SRM should refine sub-goals and mitigate related faults in SFM. Refinement process stops when the SRM mitigates all SFM requirements. Each security goal placed at leaf of SRM graph.

SEEK DIGITAL LIBRARY

Proc. of the Second Intl. Conf. on Advances in Computer and Information Technology -- ACIT 2013
Copyright © Institute of Research Engineers and Doctors. All rights reserved.
ISBN: 978-981-07-6261-2

D. Mitigation

In this step mitigation is done based on the type of faults that EPS faced with. We divide security faults into different groups based on mitigation techniques they use:

(i) Type one- avoidable Faults

All those security faults that do not threaten EPS assets has been neglected to mitigate.

(ii) Type Two- new low-level goals-Required Faults

Mitigating some security faults required to add some new sub-goals. For example, in Fig. 2 'ID and password to guess' is a security fault represented by R.1.3.2, has been mitigated by adding a new goal [hard to guesses]. It is shown by arrow 4(ii) in Fig.3. The presented node means that the probability of outside attacks will decreased and consequently makes it harder for attackers to access to EPS resources.

(iii) Type Three- unavoidable faults

Some faults are unavoidable. For instance, while it tried to protect ID and pssword, still possible that attacker guesses it. However, to reduce the effect of unavoidable faults, we suggest to partially satisfying these faults.

Partial satisfaction can be applied if it is acceptable to EPS. We RELAX goals and partially mitigate threats. Relaxation brings flexibility to the EPS security system. Partiality reserved by factoring the security faults explicitly into security requirement modeling phase. Consequently, we make EPS more fault tolerant in presence of unavoidable faults. To illustrate that, EPS security system can generate random IDs and adding new password policy, helps to avoid ID and password to guess. Although, EPS still cannot guarantee ID and password which are not guessable by attacker. EPS cannot guarantee the goal R.1.3.2 in Fig. 3 will satisfy-able under all conditions. To prevent EPS from security failure, the responded threat should be satisfied and tolerated in the requirement model. The problem showed in Fig. 3, where the requirement R.1.3.2 RELAX-ed by assigning the fuzzy statement of 'as many as possible' to the related relax attribute of R.1.3.2, described by the arrow 4(iii). Hence, we fully describe the R.1.3.2 as below:

"R.1.3.2: EPS shall avoid [ID and password to guess] as close as possible to hard guess"

In this statement 'hard to guess' is a constant value, which represent the optimal level of difficulty to guessing ID and password. Obviously, the optimum value is not necessarily the maximum value. In other words, the difficulty of guessing ID and password might not be maximum, while it still optimum value. To formally describe the above statement we apply fuzzy logic. Whereby it is the semantic basics for the language of RELAX which we use to describe security requirements and faults statements. Therefore, the fuzzy description of the above statement would be as follow:

"AG ((Δ (avoid ID and Password to Guess) – HardToGuess) ∈ S)"

Where, S refers to the purposed fuzzy set with membership value of 1 at the zero (m (1) =0) and decrease continuously down to zero.

(Δ (avoid ID and Password to Guess) indicates the level of hardness of ID and Password to be guessed. It compare with 'HardToGuess'. In fact, 'HardToGuess' play the role of threshold value for the (Δ (avoid ID and Password to Guess) to not exceeded it. In other words, if the level of hardness is more than 'HardToGuess', then cost efficiency, resource allocation and usability of the system will be affected. The acceptable level of difficulty is determined by EPS designer. The EPS designer is a person whose aware of how R.1.3.2 can partially satisfied and how proper design stages can be applied to mitigate the partiality and make the target EPS tolerant, while security threats are present.

(iv) Type Four- High-level goals-Required Faults

Type four considers those security threats, which cannot be tolerated by EPS. In these situations we may add supplementary mechanisms as high-level security goals. For instance, suppose the pssword and ID are guessed by attacker and EPS cannot tolerate the attack. In this situation, we add extra contrivance as high-level security goal(s) to tolerate the threat. Fig. 4 shows some supplementary authentication techniques that include challenge response and biometrics prepared for R.1.3.2.

TABLE I. REQUIREMENT AND FAULT ATTRIBUTES IN SRM AND SFM

Attribute	Description	Sample Value
ID	Requirement/Fault identification Code	R1.2.3, F1.2.3
Actor	Someone who do"Goalsatisfaction":Human/Software Agent	EPS-Analyzer (Name of agent)
MODAL	Modals use for Fuzzy descriptions of Requirements/Faults	Shall, May
State	Oprator for Logic Description	AF(for all states)
Phrase	KAOS statements Expanded to describe EPS Security goals.	Mitigate, attack, protect
Relaxed	RELAX statements expanded to describe partiality in Security Requirements of EPS	As close as possible to hardtoGuess

SEEK DIGITAL LIBRARY

Proc. of the Second Intl. Conf. on Advances in Computer and Information Technology -- ACIT 2013
Copyright © Institute of Research Engineers and Doctors. All rights reserved.
ISBN: 978-981-07-6261-2

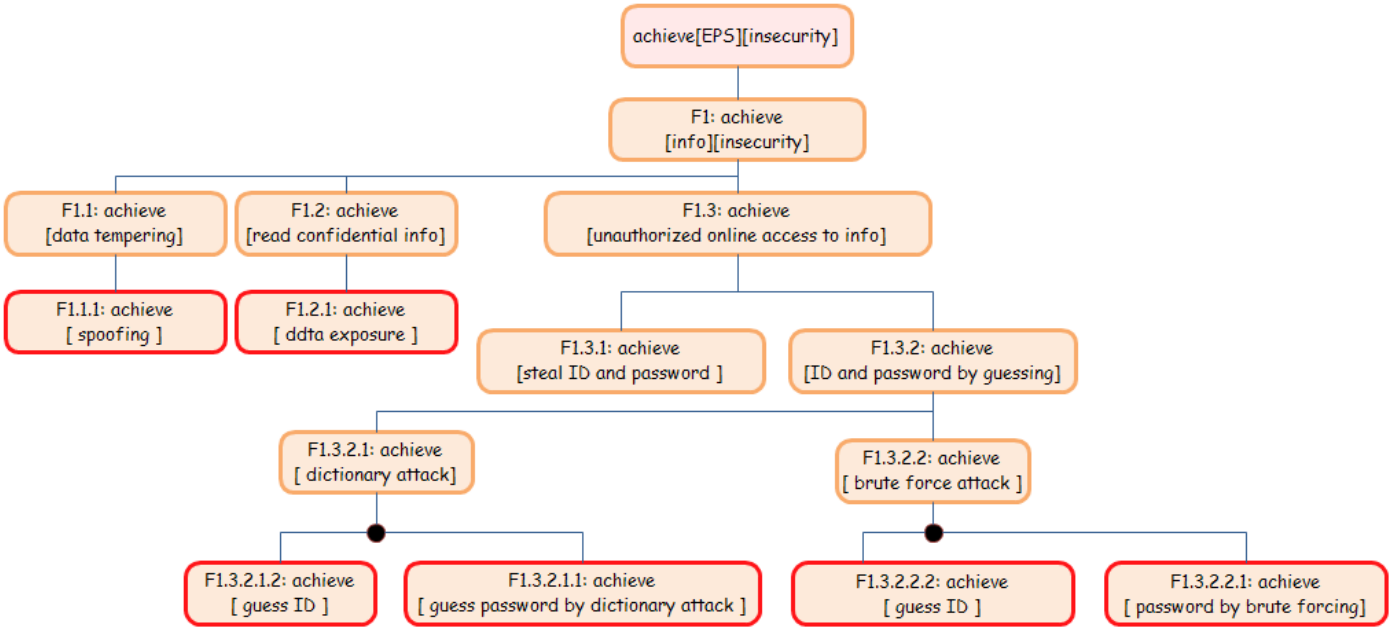

Figure 2. SFM of EPS *(dot Junction points represent AND relation, simple junction points represent OR relation)*

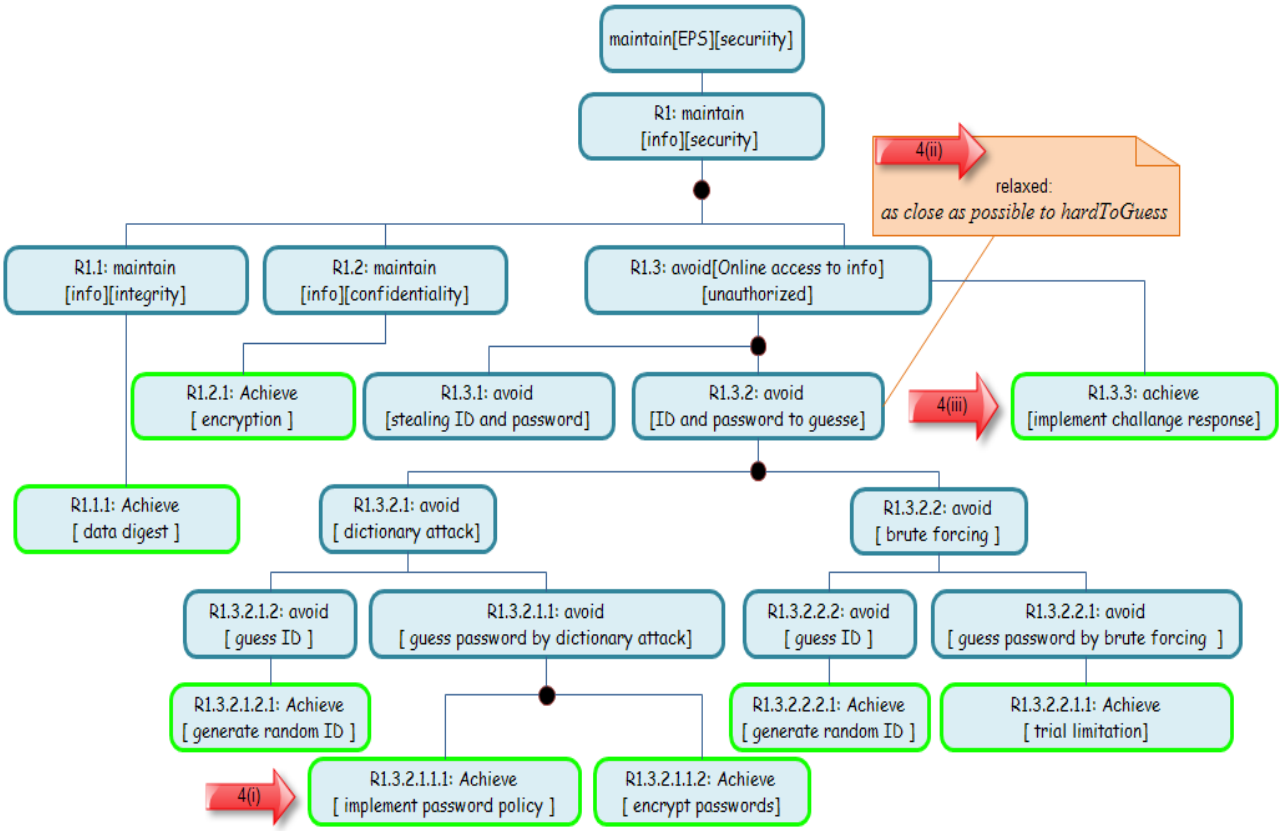

Figure 3. SRM of EPS

SEEK DIGITAL LIBRARY

Copyright © Institute of Research Engineers and Doctors. All rights reserved.
ISBN: 978-981-07-6261-2

IV. CONCLUSION

Identifying security threats in the phase of Requirements engineering is a big challenge for development of web services. To avoid from security failure, the web service has to be flexible and tolerant. The web service should be tolerant in presence of inevitable security threats. In this paper we presented a goal-based approach to establish an intrusion tolerant model for security requirements of the web service. Our proposed approach develops an intrusion tolerant model for security requirements, based on the formally described model of the security faults. Fault tolerance is achieved through manipulating for partial satisfaction of security goals. Partiality is addressed through temporal fuzzy-based language of RELAX to mitigate unavoidable threats. We have applied our proposed approach on an electronic portfolio system as a web service. The designed model is much more fault tolerant when the faults still exists.

REFRENCES

[1] C. B. Haley, J. D. Moffett, R. Laney, and B. Nuseibeh, “A framework for security requirements engineering,” in Proceedings of the 2006 international workshop on Software engineering for secure systems, pp.35-42, Shanghai, China, 2006.

[2] N. R. Mead and E. D. Hough, "Security requirements engineering for software systems: Case studies in support of software engineering education," Proceedings of the 19th Conference on Software Engineering Education and Training, pp. 149-158, 2006.

[3] A. Avizienis, J. C. Laprie, B. Randell, and C. Landwehr, "Basic concepts and taxonomy of dependable and secure computing," IEEE Transactions on Dependable and Secure Computing, vol. 1, pp. 11-33, 2004.

[4] P. E. Verissimo, N. F. Neves, and M. P. Correia, "Architecting dependable systems," R. De Lemos, C. Gacek, A. Romanovsky and er,Eds. Berlin, Heidelberg: Springer-Verlag, pp. 3-36, 2003.

[5] B. Cheng, P. Sawyer, N. Bencomo, , and J. Whittle, “A Goal-Based Modeling Approach to Develop Requirements of an Adaptive System with Environmental Uncertainty”, in Editor (Ed.)^(Eds.): ‘Book A Goal-Based Modeling Approach to Develop Requirements of an Adaptive System with Environmental Uncertainty’ (Springer Berlin / Heidelberg, 2009, edn.), pp. 468-483

[6] E. Letier, and A. van Lamsweerde: “Reasoning about partial goal satisfaction for requirements and design engineering”, SIGSOFT Softw. Eng. Notes, 2004, 29, pp. 53-62.

[7] J. Whittle, P. Sawyer, N. Bencomo, B. H. C. Cheng, and J. M. Bruel,"RELAX: Incorporating uncertainty into the specification of selfadaptive systems," Proceedings of the 17th IEEE International Requirements Engineering Conference, pp. 79-88, 2009.

[8] J. Whittle, P. Sawyer, N. Bencomo, B. Cheng and J. Bruel, "RELAX: alanguage to address uncertainty in self-adaptive systems requirement,"Requirements Engineering, vol. 15, pp. 177-196, 2010.

[9] B. Cheng, P. Sawyer, N. Bencomo, and J. Whittle, "A goal-based modeling approach to develop requirements of an adaptive system with environmental uncertainty," Model Driven Engineering Languages and Systems, A. Schürr and B. Selic, Eds. Springer Berlin / Heidelberg, pp.468-483, 2009.

[10] D. mougouei, M. Moghtadaei and S. moradmand, “A goal-based modeling approach to develop security reqiuirements of fault tolerant security-critical systems,” IEEE international conference on computer and communication Engineering, Kuala Lumpur, Malaysia, July 2012.

[11] H. BEETHAM, “e-portfolios in post-16 learning in UK: developments, issues and opportunities”, A report prepared for the JISC e-Learning and Pedagogy strand of the JISC eLearning Programme, (2005) URL:http://www.jisc.ac.uk/uploaded_documents/eportfolio_ped.doc

[12] A. Coric, I. Balaban,and G. Bubas "Case Studies of Assessment ePortfolios" 14th International Conference on Interactive Collaborative Learning (ICL2011), Piesany Slovakia, September 2011.

[13] B. Kordy, S. Mauw, S. Radomirović and P. Schweitzer, "Foundations of Attack–Defense trees," Formal Aspects of Security and Trust, P.Degano, S. Etalle and J. Guttman, Eds. Springer Berlin / Heidelberg, pp. 80-95, 2011.

[14] K. S. Edge, "A framework for analyzing and mitigating the vulnerabilities of complex systems via attack and protection trees," Doctoral Dissertation, Air Force Institute of Technology, Wright Patterson AFB, OH, USA, 2007.

[15] A. van Lamsweerde, "Elaborating security requirements by construction of intentional anti-models," Proceedings of the 26th International Conference on Software Engineering, pp. 148-157, 2004.

[16] E. Letier and A. van Lamsweerde, “Reasoning about partial goal satisfaction for requirements and design engineering,” SIGSOFT Softw. Eng. Notes, vol. 29, no. 6, pp. 53-62, Oct. 2004.

[17] L. Deron, F. Chen-Liang, C. Chyouhwa, L. and Fengyi, “Fault tolerant Web service’, in Editor (Ed.)^(Eds.): ‘Book Fault tolerant Web service” (edn.), pp. 310-319.

[18] G. Sindre and A. L. Opdahl, "Eliciting security requirements by misuse cases," Proceedings of the 37th International Conference on Technology.

[19] K. S. Edge, G. C. Dalton, R. A. Raines and R. F. Mills, "Using attack and protection trees to analyze threats and defenses to homeland security," Proceedings of the IEEE Conference on Military Communications, pp. 1-7, 2006.

[20] K.. O’Brien, “ePortfolios as Learing Construction Zones: Provost’s Perspective”, Handbook of Research on ePortfolios, Jafari A.&KaufmanC. (Ed.), IGI Global, London, UK, 2006, pp. 74 – 8

SEEK DIGITAL LIBRARY