International Journal of Cyber-Security and Digital Forensics (IJCSDF) 1(2):89-98
The Society of Digital Information and Wireless Communications, 2012 (ISSN: 2305-0012)

Measuring Security of Web Services in Requirement Engineering Phase

Davoud Mougouei[1], Wan Nurhayati Wan Ab. Rahman[2,] Mohammad Moein Almasi[3]
Faculty of Computer Science and Information Technology
Universiti Putra Malaysia, 43400 Serdang,
Selangor, Malaysia
dmougouei@gmail.com[1], wannur@fsktm.upm.edu.my[2], moein.almasi@outlook.com[3]

ABSTRACT

Addressing security in early stages of web service development has always been a major engineering trend. However, to assure security of web services it is required to perform security evaluation in a rigorous and tangible manner. The results of such an evaluation if performed in early stages of the development process can be used to improve the quality of the target web service. On the other hand, it is impossible to remove all of the security faults during the security analysis of web services. As a result, absolute security is never possible to achieve and a security failure may occur during the execution of web service. To avoid security failures, a measurable level of fault tolerance is required to be achieved through partial satisfaction of security goals. Thus any proposed measurement technique must care for this partiality. Even though there are some approaches toward assessing the security of web services but still there is no precise model for evaluation of security goal satisfaction specifically during the requirement engineering phase. This paper introduces a Security Measurement Model (SMM) for evaluating the Degree of Security (DS) in security requirements of web services by taking into consideration partial satisfaction of security goals. The proposed model evaluates overall security of the target service through measuring the security in Security Requirement Model (SRM) of the service. The proposed SMM also takes into account cost, technical ability, impact and flexibility as the key features of security evaluation.

KEYWORDS

Vulnerability; Web Service; Threat; Security Fault; Web Service Security

1 INTRODUCTION

Security has always been a vital concern in development of web services. However, current software development methods are almost neglectful of engineering of security into the system analysis and particularly requirement elicitation process [1]. Even though, some researchers attempted to integrate security analysis into the requirement phase, it is not clearly specified yet how to accomplish this spontaneously during the requirements engineering process [2]. On one hand, it is not always possible to fully mitigate the vulnerabilities or threats within the service and on the other hand, existence of faults in the service may ultimately lead to a security failure. In order to avoid security failure of the target web service requires being flexible and tolerant in the presence of security faults [3]. To facilitate this it is needed to care for fault tolerance in security requirements of the target web service. In the paper [4], we have presented a goal-based approach to address fault tolerance into the security requirements of the security critical systems. The method contributes to a flexible model for requirements of security important systems. Based on this model we have constructed a security requirement model for web services. Our intend in the current work is to help security analyzers assess Overall Degree of Security (ODS) in the target service by explicitly factoring the security factors such as impact, technical ability, cost and flexibility of the security countermeasures introduced by security requirement model of the target web service. For this reason, we divide the applied security mitigations into four categories as described in [4] to support evaluation of the degree of security of security goals with respect to the cost, flexibility, technical ability and impact of the security goals as countermeasures to security threats. Hence, a SMM has been introduced to address assessment of security in security requirements of web services. Integration of it into the SRM makes the proposed models amenable to analysis and alteration at the requirement engineering time. In our previous work [4] we have introduced some mitigation techniques to mitigate security faults and lastly make a flexible model for a given system specification. In this paper we also care for measuring partial satisfaction of security goals we have proposed in [4] to address fault tolerance in the security specification of the system. This paper has three main contributions. Firstly, it presents a model for evaluation of degree of security in security requirements of web service. Secondly, it introduces a method for calculation of degree of security for all of the security goals and consequently for the SRM of the web service by explicitly factoring the security goal attributes and also characteristics of logical model of SRM [4] into the evaluation process.

The validity of our approach is demonstrated through applying it to SRM of a typical online money transfer service (MTS), a service that offers money transfer to the beneficiary accounts. The remainder of the paper is organized as follows. Section 2 discusses related works. Section 3 presents our measurement model and introduces MTS as our running application. Section 4 describes the DS attributes and section 5 gives the details of evaluating the security for MTS. Finally, in Section 6, we conclude this paper and discuss future work.

2 RELATED WORKS

With development and utilization of web services, many researchers concern about the security of web services which leads to different evaluation models and frameworks from different perspectives. In [5] Zhang has proposed integrated security framework based on authentication, authorization, integrity and confidentiality factors besides integration of these mechanism to have more secure web services. Some researchers put forward the improvement of web service technologies, for instance, paper [6] focus on enhancing security of web services WSDL file and they proposed model for encrypting WSDL document to handle its security problems. Moreover, Li Jiang et al. in their work [7] state that mainly research in the area of web service concern on the security of web service rather than evaluation of its secureness, they proposed evaluation model which is based on STRIDE model that determine whether or not web service is secure. Gonzalez et al., in paper [8], offered sets of metrics to assess e-commerce website requirements in terms of security and usability by means of human computer interaction, their proposed evaluation model is based on GQM approach. Furthermore, in [9], author has proposed a secure measurement model that introduces different categories of security measurements and their corresponding factors in order to detect potential security defects. Wei Fu et al., in their work [10], developed web service security analysis tools that look through the source code and generates the dependency graph and through that it identifies unsafe methods and the spread of them which helps to make these methods invisible to outer users after web service being published.

Authors of [11] have proposed client transparent fault tolerance model for web serve which will recognize server errors and redirect requests to reserved backup server in order to reduce the service failures. Santos at el. [12] proposed fault tolerance infrastructure that adds an extra layer acting as proxy between client requests and service provider’s response to ensure client transparent faults tolerance. In paper [13] also the author has cared for uncertainty factors in the environment through partial satisfaction of goals in self-adaptive systems. Web services are required to operate with high level of security and dependability. Several studies proposed web service strategies in order address this issue. Merideth et al. [14] introduced “Thema” which is Byzantine Fault-Tolerance middleware system in order to execute the Byzantine Fault-Tolerance by capturing all requests and responses.

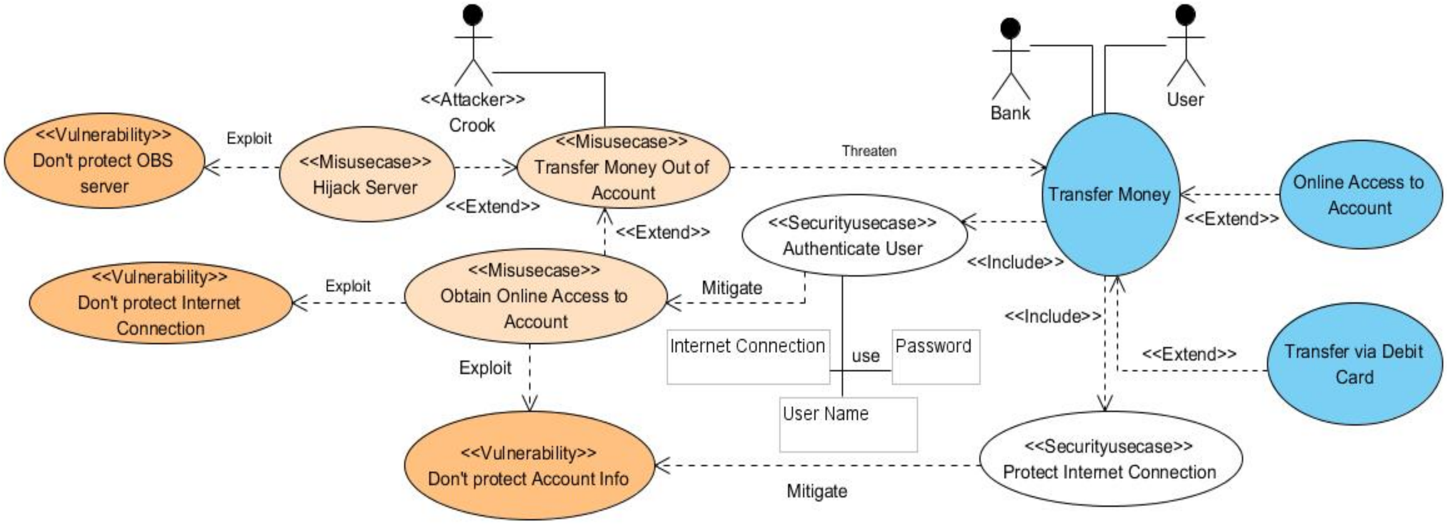

Figure 1. OBS' conceptual model in terms of use cases and misuse cases.

3 THE PROPOSED MEASUREMENT MODEL

3.1 Running Application

To illustrate the validity of our approach, we applied it to a case study provided in [15] describing an Online Banking System (OBS) as a security critical system (SCS). We have focused on the Money Transfer Service (MTS) in OBS.

OBS provides some standard banking services including money transfer service over the internet. The bank accounts are a tempting target for hackers. For this reason, MTS transactions must be protected to keep financial losses to a minimum. The availability of MTS is as important as the confidentiality and integrity. The MTS also has a server which should be protected from any possible misuse. In addition to that, an attacker may exploit the MTS' internal communication network to threaten the transactions.

MTS in addition should prevent unauthorized online access to the service. Thus, 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. MTS must offer reasonable assurance that their customers' accounts are secure. The main threat that concerns MTS is that an attacker will transfer money out of customers' accounts.

MTS as a web service relies on security concepts to work properly. Therefore, 1) maintaining integrity, 2) achieving a high level of confidentiality and 3) maintaining OBS available to the users, as the key features of security [3] are extremely important.

3.2 Methodology

Our proposed approach contains several steps. For a given security requirement model, first of all the security goals and requirements will be categorized in terms of the mitigation technique they are refined by. Afterward, the DS will be calculated for each security goal (requirement) based on its corresponding category attributes and formula. Note that all goals and requirements would be elicited from SRM of the target web service. The SRM is formally described with respect to the existing service requirement artifacts like attack trees [16] or use case and misuse case [17] diagrams. SRM is a tree-like model with "AND-OR" relations among security goals. Therefore, after calculating the degree of security for all of the security requirements so called leaves, the calculation will be propagated to the higher levels of the SRM based on the logical relation among security goals and also considering the mitigation technique the goal has refined through. In the last step, the Overall degree of security of the SRM will be calculated for the target web service.

3.3 Model Description

The SRM is supposed to reflect the security goals of the web service based on the use case model of the system illustrated in figure 1. Every security goal in SRM is refined through application of one of the four mitigation techniques mentioned in [18]. Based on the mitigation technique used to refine the goal, calculation of DS and attributes to be considered for this calculation may differ. On the other hand, some attributes should be taken into consideration to assess the goal either individually or as a part of SRM with respect to the category of mitigation it belongs to. These attributes include technical ability, impact, cost-of-implementation and flexibility of goal in the presence of security faults. TABLE 1 describes the proposed SMM in terms of these categories and attributes.

Table 1. Categories and Attributes in Proposed SMM

Mitigation Technique	*Attributes*
Add low level sub goals (ALG)	Cost of implementation (C)
	Technical Ability of goal (T)
	Impact of goal (I)
	Flexibility of goal (F)
Relaxation (RLX)	Sum of DSs of descendants (S)
	Production of DSs of descendants (P)
	Flexibility of goal (F)
Add High Level Goal (AHG)	Sum of DSs of descendants (S)
	Production of DSs of descendants (M)
	Flexibility of goal (F)
No refinement (NF)	-

For each goal in the SRM the DS values will be calculated based on the equation (1). Finally, the Overall Degree of Security (ODS) for the SRM of target web service will be calculated based on equation (2).

DS: Degree of security
T_i*:* Technical ability of goal i
I_i*:* Impact of goal i
C_i*:* Cost of implementation of goal i
F_i*:* Flexibility of goal i

$$\forall goal\ gi:\ DS_i$$

$$= \begin{cases} 0.5 \times (0.01 \times \dfrac{T_i \times I_i}{C_i} + F_i) \left| \begin{array}{c} 0 \le T_i \le 1 \\ 1 \le C_i \le 100 \\ 0 \le I_i \le 100 \\ 0 \le F_i \le 1 \end{array} \right. , gi\ is\ leaf \\ 0.5 \times (F_i + \displaystyle\sum_{all\ descendants\ k} DS_k\ ) , gi\ is\ OR - Node \\ 0.5 \times (F_i + \displaystyle\prod_{all\ descendants\ k} DS_k\ ) , gi\ is\ AND - Node \end{cases} \quad (1)$$

ODS: Overall Degree of security
$DOFT_i$*:* Degree of security of goal i
SEV_i*:* Severity of the threat which is mitigated by goal i

$$ODS = \frac{\sum_{i=1}^{n} DS_i\ \times SEV_i}{\sum_{i=1}^{n} SEV_i}, \qquad 0 < SEV_i \le 100 \quad (2)$$

4 SECURITYATTRIBUTES

In this section, the attributes taken into account for calculation of DS for each goal and also for the ODS will be discussed.

4.1 Technical ability (T)

Technical ability as one of the attributes for calculation of DS reveals the ease of implementing the goal in the following stages of the development in terms of complexity of the goal and existence of professions in the development team. In fact the Technical ability can be calculated using equation (3). Technical complexity of the implementation in the equation (3) also can be calculated based on any acceptable method for calculation the program complexity. However, since it is required to calculate the complexity in the requirement engineering stage for our proposed measurement model, using the techniques like Albresht [18] which are capable of calculationg the complexity in the early stages of development are adviced. Nonetheless any method or technique capable of doing this calculation based on the SRM is applicable. Technical ability as given in equation (3) is a number between zero and one.

T_i: Technical ability of Goal i
TCI_i: Technical Complexity of Implementation of goal i

$$T_i = \frac{1}{TCI_i}, \qquad 1 < TCI_i \leq 100 \tag{3}$$

4.2 Impact (I)

Impact is another attribute for calculating the DS of security goals in requirement model of the web service. This attribute reflects the efficiency of the mitigation constructed by the security goal. On the other words, it describes to which extent the security goal is able to mitigate the corresponding security threat. This parameter takes a value between zero and one hundred which will be specified by the security expert. Security expert can either be a member of the development team or an external security expert.

4.3 Cost of Implementation (C)

Cost is one of the main factors for evaluation the security requirements. Sometimes a security requirement can make a great contribution to the security of the service but the cost of implementation does not allow the development team to implement it. On one hand cost of development is one of the key features of web service market. So less development cost contributes to more profit and keeping abreast of the technology changes in the web market. On the other hand the extent to which the security is critical for a web service specifies the amount of budget which can be spent on security enhancements. The value for cost will be specified by development team. This can be used for calculation of DSs.

4.4 Flexibility (F)

Since it is not always possible to completely satisfy the goals, sometimes we need to accept the partial goal satisfaction [12]. We address this partiality in terms of the *relaxed* attributes in RELAX statements. Accordingly, we benefit from fuzzy temporal logic as a semantic for our applied syntax to take the security faults into account during the RE process [18]. This way we can integrate the fault tolerance into the target system's SRM. If partial satisfaction of the security goal is acceptable, we RELAX the goal. We apply this technique when threats can be partially mitigated. In this case, we add flexibility by explicitly factoring the security faults into the SRM. This contributes to a fault tolerant model for the target system which can resist in the presence of unavoidable security faults.

According to the proposed model, we calculate the flexibility for each goal based on the category it belongs to. Basically, flexibility of the goal depends on the mitigation technique it has been derived by. Calculations of flexibility for all of the categories are given in equation (4). As it is depicted in equation (4), measuring the DS at the proposed SMM , takes the fuzziness of RELAX statements into account by incorporating the membership function of corresponding fuzzy set into account for calculation of flexibility of the goal. This will be applied only on goals belonging to the RLX set.

F_i: Flexibility of goal i
gi: Goal i

$$F_i = \begin{cases} 0.2 \quad , g_i \in AHG \\ M\ (\overline{\Delta}(g_i) - OPT_i)\ , g_i \in RLX \\ 0.1\ , gi \in ALG \end{cases}$$

$$RLX = \{gi | RELAX - ation\ is\ used\ to\ derive\ gi\}$$

$$\overline{\Delta}(g_i) = \textstyle\sum_{all\ k\ mesurements} \frac{\Delta_k(g_i)}{k}$$

$$\Delta_k(g_i) \\ = \ Measured\ value\ for\ goal\ i\ in\ k_{th}\ measurement \\ In\ the\ presence\ of\ security\ faults$$

$$OPT_i = Optimal\ Value\ for\ Satisfaction\ of\ goal\ g_i \\ |\ M(\Delta_k(g_i) - OPT_i) = 1,\ if\ \Delta_k(g_i) = \ OPT_i$$

$$M\ (x) = MembershipFunction\ of\ fuzzy\ set\ of\ S \\ |\ M(x) \rightarrow S\ , M(0) = \ 1$$

$$S = \{\ (x_i, M(x_i\ ))| M(x_i)\ \in\ [0,1]\ , x \in \mathbb{R}\} \tag{4}$$

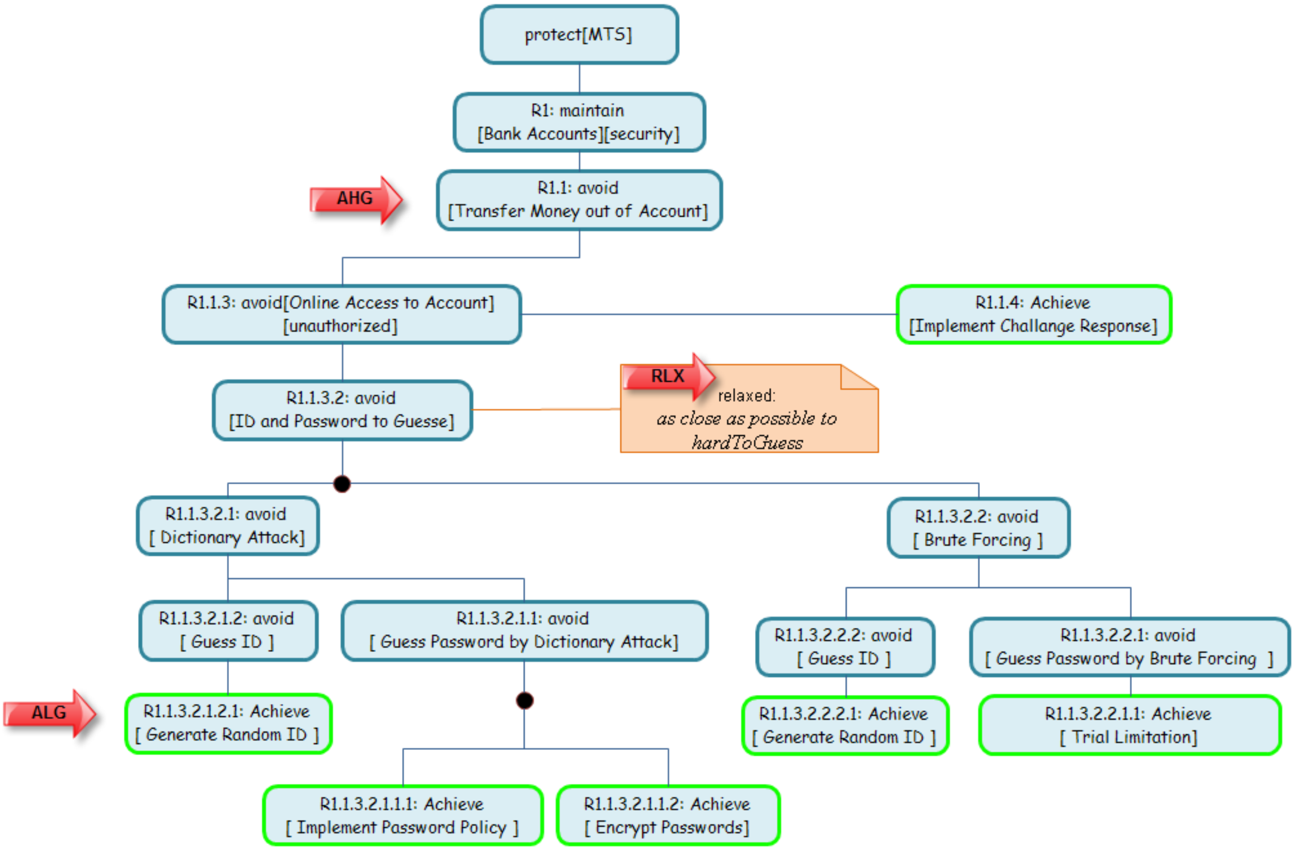
protect[MTS]
R1: maintain [Bank Accounts][security]
AHG
R1.1: avoid [Transfer Money out of Account]
R1.1.3: avoid[Online Access to Account] [unauthorized]
R1.1.4: Achieve [Implement Challange Response]
R1.1.3.2: avoid [ID and Password to Guesse]
RLX
relaxed: as close as possible to hardToGuess
R1.1.3.2.1: avoid [Dictionary Attack]
R1.1.3.2.2: avoid [Brute Forcing]
R1.1.3.2.1.2: avoid [Guess ID]
R1.1.3.2.1.1: avoid [Guess Password by Dictionary Attack]
R1.1.3.2.2.2: avoid [Guess ID]
R1.1.3.2.2.1: avoid [Guess Password by Brute Forcing]
ALG
R1.1.3.2.1.2.1: Achieve [Generate Random ID]
R1.1.3.2.2.2.1: Achieve [Generate Random ID]
R1.1.3.2.2.1.1: Achieve [Trial Limitation]
R1.1.3.2.1.1.1: Achieve [Implement Password Policy]
R1.1.3.2.1.1.2: Achieve [Encrypt Passwords]

Figure 2. SRM for MTS. (Junction points represent AND-relations while their absence means OR-relation)

A fuzzy set is a set whose elements have degrees of membership. Fuzzy set theory permits the gradual measuring of membership of elements in a fuzzy set, which is described using the membership function $M\ (S, x)$ in the range of real numbers [0, 1]. In other words, a fuzzy set is a pair (A, x) where S is a set and $M(A, x) \rightarrow [0,1]$ captures the degree of membership of A degree of membership of

5 APPLYING THE PROPOSED SMM TO MTS

In this section we apply the proposed SMM to the MTS through the following steps.

5.1 Step 1: Categorization of All Goals

Step 1 is to categorize the security goals in SRM based on the mitigation technique they have been derived by. As we discussed before we have four different mitigation techniques. By the end of the categorization process, no requirement will go under the category of the NF. This is because no requirement is derived by NF mitigation. An excerpt of the SRM for MTS is given in figure 2. The top-level security goal is to protect the MTS against possible attacks (i.e., Protect [MTS]). MTS is developed through several steps. Firstly we initiate the SRM with refinement of the top-level goal to protect the service. As a web service MTS also should be reliable and available to users. From identified assets we can specify the systems security goals in the highest-level of the SRM to protect the assets. The SRM may include other security requirements too. But in this paper we only concentrate on one of these goals (R1) to apply the proposed SMM on. At level two of the SRM we also have reduced the goals to only R1.1. This means for instance to maintain security of bank accounts (R1) in SRM includes other security goals which we have eliminated them to simplify the model for applying our proposed SMM. To categorize the goals in SRM we look into formal specification of SRM to find about the mitigation technique the goal is introduced by. Otherwise it might be difficult and subjective to categorize some of the goals as high level or low level goals. Normally high level goals are the goals which adding them to the model leads to radical changes on the behavior of the target service. Consider the situation in which the ID and Password are guessed by the attacker and the MTS cannot tolerate this security violence. In this case, we have to add redundant behavior in terms of high level security goal(s) to tolerate the threat. As it's depicted in figure 2, we may add supplementary authentication mechanisms like challenge response as high-level security goals to avoid unauthorized access to accounts in case of violation of R1.1.3.2. However, this new goals represent new behavior and the closer to the top-level goal they are, the greater the cost of implementation would be. The new goal is OR-ed with the other high level goals. As it is shown, the definition of high or low is comparative. Better said, we call a goal as a high-level goal when adding it to the system's SRM will cause radical changes in the specification of the original security requirement model. We have listed the categorized security goals of SRM in Table 2 as follows. As it is depicted in the table 2, we only have one RELAXed [19] requirement (R.1.1.3.2) for the target web service.

Table 2. Categorized Security Goals of MTS

Category	*Goal / Requirement*
Add low level sub goals (ALG)	R1.1.3.2.1.1.1, R1.1.3.2.1.1.2, R1.1.3.2.1.2.1, R1.1.3.2.2.1.1, R1.1.3.2.2.2.1
Relaxation (RLX)	R1.1.3.2
Add High Level Goal (AHG)	R1
	R1.1
	R1.1.3, R1.1.4
	R1.1.3.2.1, R1.1.3.2.2
	R1.1.3.2.1.1, R1.1.3.2.1.2, R1.1.3.2.2.1, R1.1.3.2.2.2
No refinement (NF)	-

5.2 Step 2: Calculation of DS for Category ALG

In this step we calculate the DS for the low level requirements (leaves) in SRM. The calculations are performed based on equation (1) and listed in the table 3 as follows. For example degree of security for the low level goal of R1.1.3.2.2.1.1 which brings about to limitation of number of password trials, is equal to 0.122 which is the highest among the other low level goals in SRM. Although enforcing encryption contributes to an acceptable level of mitigation but due to the comparatively low technical ability and high cost can contribute only to 0.0535 of DS which is the lowest among all DS's in Table 3.

Table 3. Calculation of Ds for Category ALG

Requirement	*C*	*T*	*I*	*F*	*DS*
R1.1.3.2.1.1.1	30	0.7	90	0.1	0.06050
R1.1.3.2.1.1.2	50	0.5	70	0.1	0.05350
R1.1.3.2.1.2.1	5	0.9	30	0.1	0.07700
R1.1.3.2.2.1.1	5	0.9	80	0.1	0.12200
R1.1.3.2.2.2.1	5	0.9	60	0.1	0.10400
R1.1.4	20	0.9	90	0.1	0.07025

5.3 Step3: Calculation of DS for Categories AHG and RLX

In this step we calculate the DS for high level requirements in SRM. The calculations are performed based on equation (1) and listed in the table 4 as follows. In order to calculate the DS for AHG goals, we need to firstly calculate the DS for ALG goals as we did in Step 2. Then we propagate the calculated values into the higher levels of the SRM and recalculate the higher level goals' DS by factoring the flexibility factor into the calculation. The flexibility factor as we described in section 3 will be calculated based on equation (4).

Concomitantly with calculation of DOF for high level goals, we calculate the DS for RELAXed goals. As we discussed before and based on equation (4), measuring the DS for RELAXed goals in proposed SMM , takes the fuzziness of RELAX statements into account by incorporating the membership function of corresponding fuzzy set into account for calculation of flexibility of the goal. This will be applied only on goals belonging to the RLX category. How to propagate the calculated DS to higher levels of the model depends on the relation among nodes in logical model of SRM. If the node in SRM (goal) is OR node, then the DS for that node will be calculated based on sum of the descending nodes. Otherwise if it is AND node, the DS will be calculated based on production of the descending nodes.

Table 4. Calculation of DS for Categories AHG and RLX

Category	*Requirement*	*S*	*P*	*F*	*DS*
AHG	R1	0.28087	-	0.2	0.24043
	R1.1	0.36174	-	0.2	0.28089
	R1.1.3	0.52347	-	0.2	0.36174
	R1.1.3.2.1	0.24019	-	0.2	0.22006
	R1.1.3.2.2	0.31300	-	0.2	0.25650
	R1.1.3.2.1.1	-	0.00324	0.2	0.10162
	R1.1.3.2.1.2	0.07700	-	0.2	0.13850
	R1.1.3.2.2.1	0.12200	-	0.2	0.16100
	R1.1.3.2.2.2	0.10400	-	0.2	0.15200
RLX	R1.1.3.2	-	0.05645	0.85	0.45322

We have RELAXed [19] the goal R1.1.3.2 in by assigning the RELAX statement of ‘as many as possible’ to the ‘*relaxed’* attribute of the requirement R1.1.3.2. So, R1.1.3.2 will be described as follows:

“R1.1.3.2: OBS shall generally avoid [ID and Password to Guess] as close as possible to hardToGuess”

The value ‘hardToGuess’ is a constant value representing the optimum value for difficulty of guessing password and ID. ‘hardToGuess’ is the optimum value not definitely the maximum value. On the other words, difficulty of guessing ID and password might be less than the maximum value while it’s still optimal. This is explained in terms of fuzzy nature of RELAX semantic:

“AG ((Δ (avoid ID and Password to Guess) – hardToGuess) ∈ S)”

Where S is a fuzzy set whose membership function has value 1 at zero (m (0) = 1) and decreases continuously around zero. *“Δ (avoid ID and Password to Guess)”* represents the hardness of guessing the ID and password which will be compared to ‘*hardToGuess*’. It means although we cannot accurately measure the difficulty of guessing the ID and password for OBS, the system model should use the capabilities of security resources for providing a best effort at protecting ID and password from attacker. In order to calculate the DS for RELAXed goal of R1.1.3.2, we need to both calculate the DS for its descendants and consequently calculate the S or P parameters and also the flexibility of the goal. To calculate the flexibility of the goal for R1.1.3.2 we need to calculate the membership of the value $(\,\overline{\Delta}(R1.1.3.2\,) - hardToGues)$ as $M\,(\,\overline{\Delta}(R1.1.3.2\,) - hardToGues)$ based on the equation (4). We consider $hardToGues = 50$ for R1.1.3.2 which means the optimum difficulty value to guess ID and password is equal to 50. Through checking the MTS model against goal R1.1.3.2 of MTS captured by SRM and in the presence of security faults, we can calculate the $\overline{\Delta}(R1.1.3.2)$ for a specific number of running the model checker. In our running example we consider $\overline{\Delta}(R1.1.3.2) = 35$ for R1.1.3.2. So we need to calculate the $M\,(\,-15)$ based on the membership function. We define the membership function for satisfaction of goal R1.1.3.2 in equation (5) as follows:

$$M\,(\,\overline{\Delta}(R1.1.3.2\,) - hardToGues) = 1 - \left|\frac{\overline{\Delta}(R1.1.3.2\,)-50}{100}\right| \qquad (5)$$

From the equation (5) we have: $M\,(35\,) = 0.85$ so the value for flexibility of R1.1.3.2 will be equal to 0.85 according to the equation (4). Consequently we can calculate the DS for the R1.1.3.2 after propagation of previously calculated DS values for its descendants. The results are listed in Table 4. As you can see in the Table 4, for AND nodes in the SRM we propagate the production of descendants so the S attribute which is sum of the DSs of descendant nodes is left blank in the table. For OR nodes also the P attributes are left blank because we propagate the sum of DSs of descendants to calculate. If there is only one child for a node in the logical model of SRM, we can consider it either as an OR node or an AND node. In our running example we considered those as OR nodes. The example for this kind of node in SRM of MTS is R1.1.3.

Step 4: Calculation of ODS for the MTS

In this step we calculate the overall degree of security for the target web service of MTS. The calculation is performed based on equation (2) as follows. As you can see in the equation (2), in order to calculate the ODS for the SRM, we need to identify the severity of faults the security goals in SRM mitigate. In our running example (MTS) we assume the severity of faults as is listed in Table 5. Severity of faults are assumed to be specified by security experts and ranged from zero to one hundred. Based on the results in Table 5 we can calculate the ODS as follows:

$$ODS = \frac{\sum_{i=1}^{n} DFT_i \times SEV_i}{\sum_{i=1}^{n} SEV_i} = \frac{195.11327}{1035} \cong 0.189$$

The total degree of security for the MTS is approximately equal to 0.189 which means if we develop the target web service for MTS based on the specification given by SRM and current model of the system, the MTS will be able to tolerate the security threats to the extent of 0.189. The higher the ODS is the more tolerant the target web service would be in the presence of security faults.

Table 5. Calculation of ODS

Category	*Requirement*	*DS*	*SEV*	*DS×SEV*
AHG	R1	0.24043	100	24.04340
	R1.1	0.28089	80	22.46945
	R1.1.3	0.36174	75	27.13022
	R1.1.3.2.1	0.22006	65	14.30385
	R1.1.3.2.2	0.25650	65	16.67250
	R1.1.3.2.1.1	0.10162	65	6.60520
	R1.1.3.2.1.2	0.13850	40	5.54000
	R1.1.3.2.2.1	0.16100	65	10.46500
	R1.1.3.2.2.2	0.15200	40	6.08000
RLX	R1.1.3.2	0.45322	70	31.72558
ALG	R1.1.3.2.1.1.1	0.06050	65	3.93250
	R1.1.3.2.1.1.2	0.05350	65	3.47750
	R1.1.3.2.1.2.1	0.07700	40	3.08000
	R1.1.3.2.2.1.1	0.12200	65	7.93000
	R1.1.3.2.2.2.1	0.10400	65	6.76000
	R1.1.4	0.07025	70	4.91750

Figure 3 presents all the process required from categorization of all the goals to calculation of overall degree of security for the money transfer system.

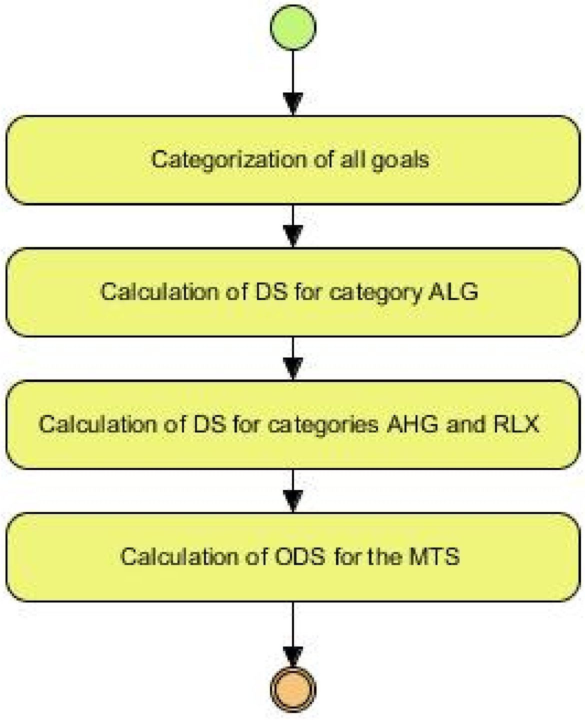
Categorization of all goals
Calculation of DS for category ALG
Calculation of DS for categories AHG and RLX
Calculation of ODS for the MTS

Figure 3. Steps required for calculation of ODS

6 CONCLUSION AND FUTURE WORKS

In this work we proposed a measurement model for evaluating security in security requirement model of the web services. Our proposed approach takes the security requirement model of the system as the input and measures degree of security in security requirements based on mitigation techniques they are refined through. The proposed model also takes into consideration attributes such as cost, technical ability, impact and flexibility of the security countermeasures to measures security of the target service. Consequently the overall degree of security can be calculated and the evaluation results can used to improve the security of the web service. To demonstrate the validity of our model, we have applied it to a typical money transfer service as our running application.

REFERENCES

1. Haley, C.B., Moffett, J.D., Laney, R., Nuseibeh, B.: A framework for security requirements engineering. In: Proceedings of the 2006 international workshop on Software engineering for secure systems, vol. Shanghai, pp. 35--42. (2006)
2. Mead, N.R., Hough, E.D.: Security Requirements Engineering for Software Systems: Case Studies in Support of Software Engineering Education. In: Software Engineering Education and Training, 2006. Proceedings. 19th Conference on, pp. 149--158. (2006)
3. Avizienis, A., Laprie, J.C., Randell, B., Landwehr, C.: Basic concepts and taxonomy of dependable and secure computing. In: Dependable and Secure Computing, IEEE Transactions on, vol. 1, no. 1, pp. 1--33. (2004)
4. Mougouei, D., Moghtadaei, M., Moradmand, S.: A Goal-Based Modeling Approach to Develop Security Requirements of Fault Tolerant Security-Critical Systems, in: Proceedings of 4th International Conference on Computer and Communication Engineering, Malaysia, pp. 200-205. (2012)
5. Zhang, W.: Integrated Security Framework for Secure Web Services. In: Intelligent Information Technology and Security Informatics (IITSI), Third International Symposium on, pp. 17--183. (2010)
6. Mirtalebi, A., Khayyambashi, M.R.: Enhancing Security of Web Services against WSDL Threats. In: Emergency Management and Management Sciences (ICEMMS), 2nd IEEE International Conference on, pp. 920—923. (2011)
7. Jiang, L., Chen, H., Deng, F. A Security Evaluation Method Based on STRIDE Model for Web Service. In: Intelligent Systems and Applications (ISA), 2010 2nd International Workshop on, 2010, pp. 1--5. (2010)
8. Gonzalez, R.M., Martin, M.V., Munoz-Arteaga, J., Alvarez-Rodriguez, F., Garcia-Ruiz, M.A.: A measurement model for secure and usable e-commerce websites. In: Electrical and Computer Engineering, 2009. CCECE ’09. Canadian Conference on, pp. 77--82. (2009)
9. Lai, S.T.: An Interface Design Secure Measurement Model for Improving Web App Security. In: Broadband and Wireless Computing, Communication and Applications (BWCCA), 2011 International Conference on, pp. 422--427. (2011)
10. Fu, W., Zhang, Y., Zhu, X., Qian, J.: WSSecTool: A Web Service Security Analysis Tool Based on Program Slicing. Services (SERVICES), IEEE Eighth World Congress on, pp. 179--183. (2012)
11. Aghdaie, N., Tamir, Y.: Client-transparent fault-tolerant Web service. In: Performance, Computing, and Communications, 2001. IEEE International Conference on, pp. 209--216. (2001)
12. Santos, G.T., Lung, L.C., Montez, C.: FTWeb: a fault tolerant infrastructure for Web services. In: EDOC Enterprise Computing Conference, 2005 Ninth IEEE International, pp. 95--105. (2005)
13. Cheng, B., Sawyer, P., Bencomo, N., Whittle, J., A Goal-Based Modeling Approach to Develop Requirements of an Adaptive System with Environmental Uncertainty. In: Model Driven Engineering Languages and Systems, vol. 5795, A. SchÃ¼rr and B. Selic, Eds. Springer Berlin / Heidelberg, pp. 468--483. (2009)
14. Merideth, M.G., Iyengar, A., Mikalsen, T., Tai, S., Rouvellou, I., Narasimhan, P.: Thema: Byzantine-fault-tolerant middleware for Web-service applications. In: Reliable Distributed Systems, 2005. SRDS 2005. 24th IEEE Symposium on, pp. 131--140. (2005)
15. Edge, K.S.: A framework for analyzing and mitigating the vulnerabilities of complex systems via attack and protection trees. Air Force Institute of Technology, Wright Patterson AFB, OH, USA. (2007)
16. Edge, K.S., Dalton, G.C., Raines, R.A., Mills, R.F.: Using Attack and Protection Trees to Analyze Threats and Defenses to Homeland Security. In: Military Communications Conference, 2006. MILCOM 2006. IEEE, pp. 1--7. (2006)
17. Sindre, G., Opdahl, A.L.: Eliciting security requirements by misuse cases. in Technology of Object-Oriented Languages and Systems, 2000. TOOLS-Pacific 2000. Proceedings. 37th International Conference on, 2000, pp. 120--131. (2000)
18. Cheng, B., Sawyer, P., Bencomo, N., Whittle, J.: A goal-based modeling approach to develop requirements of an adaptive system with environmental uncertainty. In: Model Driven Engineering Languages and Systems, A. Schürr and B. Selic, Eds. Springer Berlin / Heidelberg, pp.468--483. (2009)
19. Whittle, J., Sawyer, P., Bencomo, N., Cheng, B., Bruel, J.M.: RELAX: a language to address uncertainty in self-adaptive systems requirement. In: Requirements Engineering, vol. 15, no. 2, pp. 177--196. (2010)