SECURITY VIGILANCE SYSTEM THROUGH LEVEL DRIVEN SECURITY MATURITY MODEL

S. K. Pandey

Department of Information Technology, Board of Studies
The Institute of Chartered Accountants of India (Set up by an Act of Parliament), Noida-201 309, INDIA
E mail: santo.panday@yahoo.co.in

ABSTRACT

Success of any software system largely looms upon its vigilance efficiency that prompts organizations to meet the set of objectives in the arena of networks. In the highly competitive world, everything appears to be vulnerable; information system is also not an exception to this fact. The security of information system has become a cause of great concern. On the contrary, till time the software security engineers are trying hard to develop fully protected and highly secured information systems but all these developments are at nascent stages. It is quite revelling that in the earlier research studies, little attention is paid to highlight an accurate status of the security alertness for developed software. Hence, keeping all these factors at the backdrop, this paper is an attempt to propose a holistic Security Maturity Model (SMM), in which five levels/stars have been developed, driven on the strength of the security vigilance occurring at the various stages for any software. SMM is in its conceptual stage; the detailed steps will certainly require time to be developed so that every software system can reap out the benefits of this model. To categorize/discriminate the level of potency, SMM will be highlighted through appropriate ranking/star system. It is hoped that if SMM will be followed in its true letter and sprit; undoubtedly, this will restore the clients' trust and confidence on the software as well as their corresponding vendors. Moreover, this will also enable software industry to follow transparent and ethical practices.

Keywords

Security Vigilance System, Security Maturity Model, SMM, Security Stars, Security Levels.

1. INTRODUCTION

With the rapid advances in ICT, the computing and communication devices are having various components in the form of software. Everyday, millions of people perform their business transaction through internet driven operations, ATM, mobile phone; they send email & e-greetings, and use word processing and spreadsheet for their routine affairs. For developing software, various methodologies/techniques are taken into consideration under the head of software engineering. Software engineering is the application of a systematic, disciplined, quantifiable approach to the development, operation, and maintenance of software, and the study of these approaches; that is, the application of engineering to software (Wikipedia, Software engineering). Software Engineering technologies appear to support, and demand as well, the sufficient level of security assurance in software development projects.

DOI : 10.5121/ijcseit.2012.2202

The issue pertaining to security surfaced for the first time in 1970s with report of earliest known intrusion in 1977, first spam email in 1978, earliest large-scale identity theft in June 1984 and attack of first ever known computer virus reported in 1987. During 1980s and 1990s, many international banks were targeted by crackers and hackers. In 1995, U.S. Department of Defense computers were attacked roughly 250,000 times. In 1996, hackers alter websites of the U.S. Department of Justice in August, CIA in October, and U.S. Air Force in December. In 2001, Microsoft becomes victim of Denial of Service attacks. In May 2006, a Turkish hacker successfully hacked 21,549 websites (Kizza, 2008). In March 2008, around 20 Chinese hackers claim of gaining access to the world's most sensitive sites, including Pentagon. In April 2009, Conficker, a worm infiltrated billions of PCs worldwide including many government-level top-security computer networks (Wikipedia, Timeline of computer security hacker history).

While trying to identify and analyze the reasons behind the cause of security breach, one can generally put blame entirely on virus attack, denial of service, spam mail etc. But, if we introspect in true sense, we may find ourselves biased; while analyzing the facts, we intend to forgo a very important and real fact, which is one of the most important factors in software security breach, and, that is really disheartening, bad software, which is actually behind every security problem and malicious attack (Raman, 2006) (Pandey & Mustafa, 2010) targeting those individual security threats and providing solution for those attacks, if we also put focus on the security aspect of software, we can surely build a more robust and reliable software in totality (Nhlabatsi et al., 2008).

In the fast changing world of software security system, a few research studies have been attempted (Carnegie Mellon University, 2003). However, the efforts in comparison with the place of demands in the context of assurance for secure software are far away from the desired and needs a focused attention on emergent basis. In literature, there is not any process/framework/model, which can assess the accurate security level for software, ready to be deployed. Companies develop and sell software without having a concrete status of security in software. Paradoxically, clients also procure software in dark without knowing the security maturity level/s. To address these emergent issues of IT Industries as well as their clients/users, a model, SMM is proposed in the paper. The model proposes five levels/stars based on the maturity of the security vigilance during various stages for any software.

Beyond this introduction on the background details, the remainder of this paper is organized as follows. Section II describes ‘Security Maturity Model (SMM)’. Possible mechanisms for assessment of these levels are discussed in Section III, while Experts’ Review and Discussion about the proposal is discussed in Section IV. Finally, ‘Conclusions and Future Works’ are given in Section V.

2. SECURITY MATURITY MODEL (SMM)

The proposed model, SMM is a process maturity model. It is focussed on the implementation of the security starting from the requirements phase till the deployment and maintenance. One of the most important aspects of this model is that the model is *process independent*; it does not dictate its own process for any activity. Organizations are free to adapt any of the existing approaches or best practices for their different activities. SMM will only guide them about the security levels with reference to a particular methodology and accordingly, it will also provide the final star rating. For example, if an organization is using XYZ method for developing security requirements in the requirements phase, and finally prepare the SRS; SMM will provide security star/s for the final output i.e. SRS and it will not suggest any of its own methodologies. The proposed model, SMM has five maturity levels, which are discussed as follows:

- **One Star: Elementary Level:** This is the first and minimal level maturity of the security. SMM strongly recommends that all the software must possess one star to survive in the cyber space; otherwise they will be highly insecure and their security may be compromised at any given point of time. For this, the tools/techniques followed by the development companies starting from the requirements phase till deployment and maintenance must be analyzed.

- **Two Stars: Intermediate Level:** To have a compliance of the two star security assurance of SMM, some more security specific tools/techniques will be required to be adapted by the organizations for more secure software development.

- **Three Stars: Post-Intermediate Level:** At this level, security must be planned and implemented very preciously in all the processes at every stage of the development life cycle. Very focused attention will be required by all the team members from the inception itself for building a software, which should be able to possess three stars.

- **Four Stars: Advanced Level:** This is an advanced level of the security. For the development of four stars secure software, all the individuals involved in the different processes must be aware with all the latest developments in terms of their tools/techniques used for various activities in the SDLC.

- **Five Stars: Premium Level:** This is the final as well as five stars level in which the development organization will offer the software with maximum achievable security. Although, we know that there is nothing 100% secure in the world; but after having five stars, it will be presumed that the software will be secure at least up to 99.9999%.

3. POSSIBLE MECHANISMS

To assess these star levels, we propose that security should be taken care in each of the generic phases of the SDLC. For each phase, all the possible tools/techniques and best practices should be collected. In addition, these must be analyzed in terms of the security. In this way, first of all, the security stars will be assigned to the final output of each phase, and finally, to the software as a whole. A pictorial representation of the same is given in Fig. 3.1.

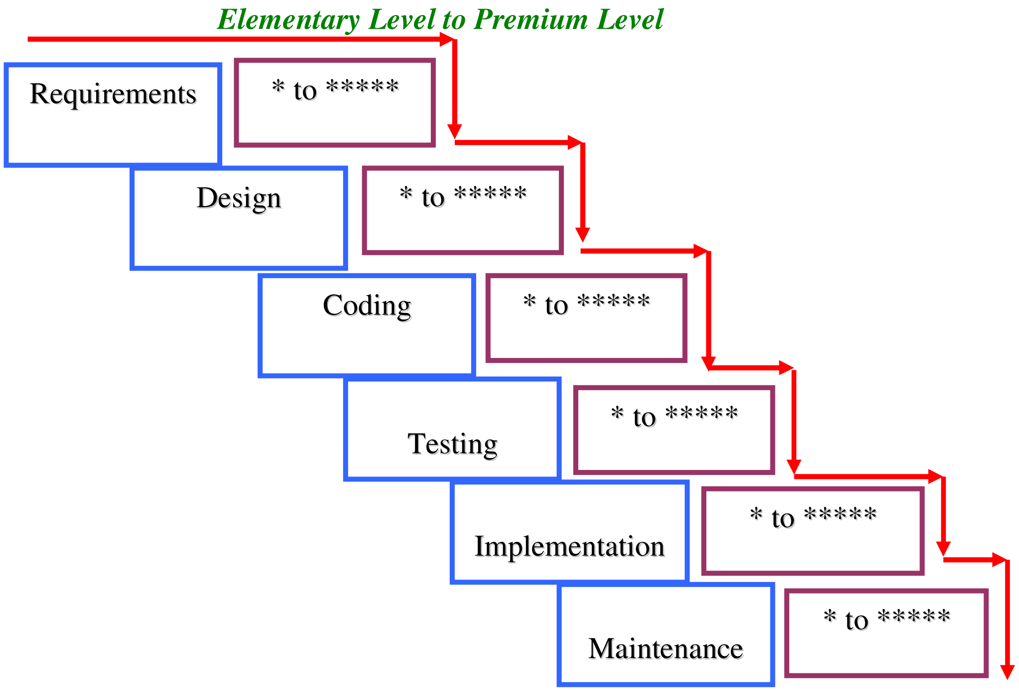

Fig. 3.1: Security Stars for SDLC

As we discussed earlier, SMM is at the foundation level presently; hence, a lot of work is yet to be accomplished for determining the security stars with respect to the different activities for each phase of the SDLC. Although, SMM is primarily intended for the improvement in the maturity levels of the security, but it may also support a wide variety of enhancement activities. This will help in obtaining a benchmark of actual practice related to security for any software. In addition, this will create and support a momentum for secure development practices and finally, of course a secure software. Another important benefit is that the business will be transparent because before signing the contract, clients will be asked that 'what is their need in terms of security'; 'how many stars' complaint software they need?' depending upon their requirements, cost will be assessed by the development companies. On the other hand, companies will also be bound to provide the security to the desired stars levels. In this way, SMM will facilitate client/s and development company/ies both in terms of building their mutual trust and confidence with each other.

4. EXPERTS' REVIEW AND DISCUSSION

Proposal of any model is subject to the experimental validation and analysis of the results. There must be some experimental data, which should show the utility of the proposal. As we said earlier that at this stage, SMM is only a conceptual model; its validation on real life projects is not feasible. Therefore, it was decided to take the help and guidance of experts' feedback on the relevant issues by designing a feedback form. The feedback was collected on the following issues:

- SMM's relevance to the purpose;
- Analysis of the SMM under the following heads:
    - Importance and appropriateness of the proposed idea/concept;

  - Relevance of the model;
  - Potential utility for evaluation process;
  - Proposed mechanisms;
  - Relevance of all the star levels;
  - Clarity of activities;
  - User-friendliness; and
  - Scrupulousness of the Model.
- Overall recommendation.

SMM document along with the review form was sent to the twenty experts from the varied fields' viz. academia, industry, scientific organizations, educational institutions, research bodies, government organizations. But, our emphasis was primarily based on the software development companies. Really, this was a daunting task to have the feedback from the experts. It was completed by personal interactions with the experts by having 2-3 meetings in which the complete model was discussed in detail along with future strategies. However, after a lengthy exercise, we were able to have duly filled feedback forms from the twelve experts only. However, two experts provided the feedback only on a point, namely 'Potential utility for evaluation process' exclusively; in this way, for this point, total feedback was given by fourteen experts. The duly filled review forms given by various experts were compiled and a summary of the same is given as follows:

- ***SMM' Relevance to the purpose:*** All the experts found the proposed work relevant to the current need in terms of security.
- ***Analysis of the SMM:*** The following chart has been drawn to show the ratings given by individual expert, assigned to various parameters given in the review form.

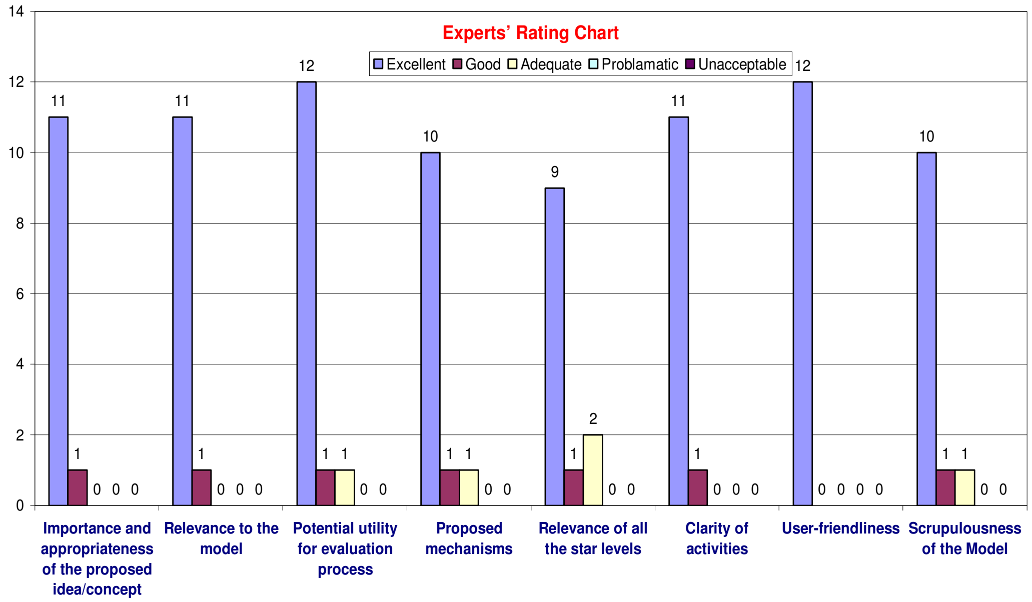

Figure 4.1: Experts' Rating Chart

- ***Overall Recommendation:*** All the experts accepted the research work as an important contribution, which needs the detailed work and effective practical implementation.

Observations given by the various experts reveal that the proposed conceptual model, SMM is incredibly relevant for the assessment of security assurance of any software. Most of the experts also urged that if it is developed with all the detailed steps, it will be a great work for the ICT community. However, some experts were also of the opinion that a strong validation of the model with detailed steps on a very large sample size will be required for accepting the SMM as a reputed as well as worldwide practice.

5. CONCLUSIONS AND FUTURE WORKS

It is very imperative to note here that SMM recognizes the need of secured development life cycle and supports the same through its security maturity stars at different stages. Experts' opinion is also taken on the related issues and the same is compiled in a proper way. The summary reveals that this may be a very useful and globally accepted model if all the steps/sub-steps is developed appropriately. However, a very strong support of experimental validation will be needed for the standardization of the model.

Future work related with SMM may be to study the detailed methodologies of security assurance for each of the generic phases of the SDLC. For this, an in-depth study and analysis of every activity and its related tools, techniques, best practices will be required. Then only, stars can be assigned to the overall output of a phase and finally, to the software, ready to be deployed. All these tasks are really, very stimulating. But, on the other hand, research community has the potential to come up with the solutions of the same. Hope for the best!

REFERENCES

[1] Carnegie Mellon University (2003, June). Secure Software Engineering- Capability Maturity Model. Description Document Version 3.0.

[2] Kizza Joseph Migga. (2008). *A guide to computer network security*. (pp. 112-115). Springer.

[3] Nhlabatsi A., R. Laney, B. Nuseibeh. (2008). Feature interaction: The security threat from within software systems. *Progress in Informatics* (5), 75-89.

[4] Pandey S. K. and Mustafa K. (2010, July). Recent advances in SRE research, *International Journal of Computer Science and Engineering*, 2(4), 1079-1085.

[5] Raman Jari. (2006). *Regulating secure software development: Analyzing the potential regulatory solutions for the lack of security in software*. (p. 2). Lapland University Press.

[6] Wikipedia. Software engineering. Retrieved April 5, 2009, from http://en .wikip edia.org/wiki/Software_engineering

[7] Wikipedia. Timeline of computer security hacker history. Retrieved May 23, 2008, from http://en.wikipedia.org/wiki/Timeline_of_computer_security_hacker_History

Author

Dr. Santosh K. Pandey is presently working as a Faculty (Executive Officer) in the Department of Information Technology, Board of Studies, The Institute of Chartered Accountants of India (Set up by an Act of Parliament) New Delhi. Prior to this, he worked with the Department of Computer Science, Jamia Millia Islamia (A Central University) New Delhi. He has a rich Academics & Research experience in various areas of Computer Science. His research interest includes: Software Security, Requirements Engineering, Security Policies and Standards, Software Engineering, Access Control and Identity Management, Vulnerability Assessment etc. Currently, he is working in the areas of Software Security and Requirements Engineering. He has published around 38 high quality research papers in various acclaimed International/ National Journals (including IEEE, ACM and CSI) and Proceedings of the reputed International/National Conferences. He has been nominated in the board of editors/reviewers of various peer-reviewed and refereed Journals. In addition, he has also served as a Program Committee Member of several reputed conferences in India as well as abroad. He has also been designated in various academic/research committees by the government organizations as well as software companies as a subject expert. His one of the research papers was adjudged as the Best Paper in the National Conference on IT-Present Practices and Challenges held at New Delhi during Aug 31- Sep 1, 2007.