Review Comments Prince Thomas

----------------------- REVIEW 1 ---------------------

PAPER: 10

TITLE: Security Evaluation

AUTHORS: Prince Thomas

Overall evaluation: 0 (borderline paper)

----------- Overall evaluation -----------

Summary:

Chapter 2 gives an idea and insights about security metrics and why these are important to use. The next chapter describes security patterns and their evaluation. It also describes methods and tools to test vulnerabilities in software. To wrap it up a case study is presented which show some of the previously described methods. The last chapter then the quantitative evaluation. Different methods for systematic software penetration or attacks are discussed, as well as their advantages and disadvantages.

Positive aspects:

The paper gives a nice overview on methods and tools for software security evaluation.

Its logically structured.

General Issues:

Some things which could be a list are in continuous text which makes it hard to read, because of all the commas, hyphens and colons.

Some sentences tend to get long (3-4 lines).

Prince Thomas Comments: Fixed most of that's possible.

Specific Issues:

Goals/Aims:

The goal is to give a deeper insight into software security evaluation and its aspects. Explaining challenges and reason why doing security evaluation.

Presentation:

Title: Maybe be a little more specific, 'Security Evaluation' of what or in which field?

Prince Thomas Comments: It's for software field, but since this paper is a part of non-functional aspects of software engineering, I didn't mention it specifically..

Abstract: Good

Key Words: Maybe add 'Software' somewhere.

Prince Thomas Comments: Taken care.

Introduction: Good

Conclusion: In the second paragraph: 'There are so many [...]' -> bad phrasing. Due to all the enumerations it is hard to get into a 'reading flow'.

Prince Thomas Comments: Taken care.

Length:

3.5 and 4.5 could be a little bit longer and more detailed, since a lot of things are described in the corresponding chapters (3.1-3.4 and 4.1-4.4). Just to wrap it up.

Prince Thomas Comments: Those subsections are combined to a section to give a better clarity.

Research Methods: Clear

Clarity:

Figure 6 is hard to follow.

Prince Thomas Comments: Changed the representation with enough details.

Result Presentation:

Figure 3 is not a cycle as stated in the description.

Prince Thomas Comments: Taken care.

Figure 5 doesn't give me any information.

Prince Thomas Comments: Gives an idea about 'AND' and 'OR' nodes.

Citations:

Reference style is not consistent

Prince Thomas Comments: Because of different kind of refrences.

Goal/Aim reached:

Each chapter describes methods and concludes them. The conclusion could be a little bit longer (see Length).

Prince Thomas Comments: I feel its sufficient. I will discuss with supervisor and will change accordingly.

Other Issues:

In 3.2 make a list or similar for the 10 principles.

Prince Thomas Comments: Taken care.

Be consistent with enumerations. Currently some of them are continuous text some use bold text with '-' some with ':'.

Page 11, Sentence 1 doesn't make sense to me.

There are errors with spaces before/after colons/brackets/dots/...

Prince Thomas Comments: Taken care.

--------------------- REVIEW 2 ---------------------

PAPER: 10

TITLE: Security Evaluation

AUTHORS: Prince Thomas

Overall evaluation: 2 (accept)

----------- Overall evaluation -----------

1. Summary of the paper

The paper talks about why software security is important (continue to function correctly under attack) and why is it important in modern software systems. The author emphasizes on significance of measuring and assessing software security, because secure software is a must. Furthermore, it elaborates on how security metrics aid developers in securing their software product. For example, which configuration change is the most effective to increase parameters relevant for the trustworthiness of a software products. It evaluates web security on the use case, where automated attack of web application is studied. It talks about what are software security metrics and security evaluation techniques. In the 2nd chapter it elaborates more on importance of Security Metrics and how are they are classified. Different quantitative Security evaluation techniques are presented such as Combinatorial methods and State-Based Stochastic Methods, where system is expresses as a finite state machine. Case study is given evaluating security mechanisms in the context of web applications.

2. Positive aspects

The language in the paper is comprehensive and easy to read. The author uses proper constructs and the work is not boring to read. The paper gives motivation why software security is an important aspect in Modern software. The rest of the paper follows and builds upon Abstract and Introduction subsection and gives the suggestions on how to tackle issues presented in these subsections.

3. General issues

Format: On page 5, "Static: Static, or pre-deployment, security metrics are developed to be measured before the assessed target enters operation. Dynamic: Dynamic, or run-time, security metrics are those developed to be constantly measured, during the operation of the target being evaluated." Looks better if you write "Static, or pre-deployment, ...", delete "Static: Static, or pre-deployment ..."

Prince Thomas Comments: Taken care.

Language: Abstract: The 2nd sentence sounds boring, since you used two times for the sentence subject the same word "Security Evaluation". "Security Evaluation basic step in achieving this goal for any organization. Security Evaluation is particularly important because of the rapidly changing environment of the information security system or the operation system."

Prince Thomas Comments: Taken care.

"Metrics is a measurement standard which denes what is to be measured, how to be measured and helps the security practitioners to manage the product efficiently. Security metrics is the powerful tool that helps security practitioners to integrate security features into their system. The security metrics are gaining lot of significance now a days because with the help of the data obtained from them software security decisions can be taken and which in turn helps the software developers to secure their software product."

Prince Thomas Comments: Taken care.

Same as in my first comment, you are using the same verb way too many times. Here in all 3 consecutive sentences you use verb aid".

Prince Thomas Comments: Taken care.

Check other grammar and spelling mistakes.

Prince Thomas Comments: Taken care.

Structure: In the Conclusions section, you should give a future work based on the work in your paper.

Prince Thomas Comments: Future scope of the work is mentioned in abstract manner.

4. Specific issues

Goals/Aims: In the Introduction section, you stated what is the current problem, however, you need to introduce the solution to this issue, to emphasize the relevance of your paper.

Prince Thomas Comments: It seems fine.

Length: In subsection 3.1 you mention all the Security Patterns for Qualitative Security Evaluation, instead you should explain only ones that are relevant to your methodology.

Prince Thomas Comments: All of them are measured to give the author an idea about the valuable security patterns which will help in exploring further.

Clarity: In subsection 3.2, rather than just citing and listing qualitative criteria for evaluation of security pattern, try to elaborate more on this topic. For example, try to extend the part which talks about what is significance of these qualitative criteria, why are they better than the others?

Prince Thomas Comments: Idea was just to give a short overview as it's not really part of the research.

Result presentation: You have figure 4, for your case study, however in the text of subsection 3.4 you should give more detail about this picture. Keep in mind that a reader should be able to find more details about your figure in the text.

On page 7, you wrote: "Penetration testing is the next step after vulnerability assessment.", however in Figure 3, Penetration Testing is the step after information Analysis and Planning.

Prince Thomas Comments: All the 4 steps constitute the part called vulnerability assessment.

Research methods: In subsection 3.4 give more information on how are results produced from the use-case scenario.

Citation: 1) On page 6: "Spyros T. Halkidis, Alexander Chatzigeorgiou and George Stephanides in their paper "A qualitative analysis of software security patterns" [6] had mentioned three set of qualitative criteria for evaluation of security pattern.", when you cite someone else's work you do not need to write all of the author names. Use something like Researchers in [6] have demonstrated that

Prince Thomas Comments: Taken care.

2) In subsection 4.2, you explain the definition of these methods, however, is this really your own idea, or it's a definition from some other book or paper. If not cite the source.

Prince Thomas Comments: Framed with my own words.

5. Other issues

Page 1, twitter should be written with capital t.

On page 2, "now a days" must be written together "nowadays". You also used this verb on page 1, try to use some other word instead.

"Brief description about software", this is wrong it "description about ..." is wrong, should be "description of ....".

"model based" is one word, should be "model-based".

"describes about the qualitative" should be without word "about": "describes the qualitative"

"from them software security" what is "them" trying to tell here? Did you mean to use "the"?

Prince Thomas Comments: All points were relevant and have been taken care.

----------------------- REVIEW 3 ---------------------

PAPER: 10

TITLE: Security Evaluation

AUTHORS: Prince Thomas

Overall evaluation: 2 (accept)

----------- Overall evaluation -----------

1. Summary of the paper:

The paper gives an overview about software security evaluation. It specifies the significance of software security and provides a detailed study on the security metrics used in the research to quantify the metrics for security evaluation. The paper elaborates further on qualitative and quantitative security evaluation approaches in detail.

2. Positive aspects:

The paper gives a very detailed overview of security evaluation. Qualitative and quantitative security evaluation approaches are explained clearly with case studies and examples.

3. General aspects:

1. Figures need to be in vector graphics format.

2. Capitalization of letters needs to be corrected at various places in the paper. (for example, "in Modern software development", "social network Web site", "Several vulnerability databases", "and Race conditions" etc)

Prince Thomas Comments: Taken care (All points).

4. Specific aspects:

1. Please provide a tabular comparison of evaluation in the results for better clarity.

2. "Representation of an AND node OR node is given in Fig.5." needs to be corrected.

3. In section 3.2, 10 guiding principles for building secure software are listed. This can be numbered to make it more readable.

4. In Section 4, please add a sentence on what is detailed in subsection of it to add better clarity, to describe the aspects considered in the evaluation and its relevance.

5. In Section 3, please add a sentence on what is detailed in subsection of it to add better clarity. For example, it was not clear on why the VAPT based security evaluation is performed.

Prince Thomas Comments: Taken care (All points).

5. Other issues:

1. Punctuation issues/Typo: "dynamic:"

2. Typo: "systematic ay" needs to be corrected to systematically.

Prince Thomas Comments: Taken care (All points).