FACULTY OF INFORMATION TECHNOLOGY CTU IN PRAGUE

Supervisor's statement of a final thesis

Student:	Bc. Ondřej Lauer
Supervisor:	Mgr. Jakub Růžička
Thesis title:	Security Analysis of Applications Using Smart Contracts
Branch of the study:	Computer Security

Date: 26. 5. 2019

Evaluation criterion:	*The evaluation scale: 1 to 4.*
1. Fulfilment of the assignment	*1 = assignment fulfilled,* ***2 = assignment fulfilled with minor objections,*** *3 = assignment fulfilled with major objections,* *4 = assignment not fulfilled*

Criteria description:
Assess whether the submitted FT defines the objectives sufficiently and in line with the assignment; whether the objectives are formulated correctly and fulfilled sufficiently. In the comment, specify the points of the assignment that have not been met, assess the severity, impact, and, if appropriate, also the cause of the deficiencies. If the assignment differs substantially from the standards for the FT or if the student has developed the FT beyond the assignment, describe the way it got reflected on the quality of the assignment's fulfilment and the way it affected your final evaluation.

Comments:

The thesis sets up the following objectives: 1. An introduction to applications utilizing smart contracts; 2. Proposal of a framework for security analysis of such applications; 3. demonstration of employment of the developed framework on a sample product (VETRI, https://vetri.global/), identification of vulnerabilities and their remedies. All of the above with an emphasis on smart contract-related components.

The difficulty of the assignment is corresponding to the requirements put on a Master's degree student as it's concerned with a current (and therefore lesser-researched) topic, hence it requires inventiveness on his part.

Regarding the overall fulfillment of the assignment, I give grade B (2). I believe that the 1st and 2nd goals were elaborated without any significant remarks, the 3rd objective is then recalled and discussed in more detail in the sections below.

Evaluation criterion:	*The evaluation scale: 0 to 100 points (grade A to F).*
2. Main written part	*80 (B)*

Criteria description:
Evaluate whether the extent of the FT is adequate to its content and scope: are all the parts of the FT contentful and necessary? Next, consider whether the submitted FT is actually correct – are there factual errors or inaccuracies? Evaluate the logical structure of the FT, the thematic flow between chapters and whether the text is comprehensible to the reader. Assess whether the formal notations in the FT are used correctly. Assess the typographic and language aspects of the FT, follow the Dean's Directive No. 26/2017, Art. 3. Evaluate whether the relevant sources are properly used, quoted and cited. Verify that all quotes are properly distinguished from the results achieved in the FT, thus, that the citation ethics has not been violated and that the citations are complete and in accordance with citation practices and standards. Finally, evaluate whether the software and other copyrighted works have been used in accordance with their license terms.

Comments:
The structure of the text is simple and evident. (In a good way.) There's a logical continuity of individual chapters, which strictly adhere to the assignment and do not contain redundant information.

The reader is first introduced to the basic concepts around smart contracts, followed up by a list of most common vulnerabilities in components that are typically used in smart contract (and/or decentralized) applications. The 'Smart contract application testing framework' chapter then summarizes and concludes the theoretical part with a checklist for developers containing vulnerabilities, type of security testing and proposed testing tools (including a column denoting whether the vulnerability made it to the scope of the VETRI penetration testing as part of this thesis). The practical part describes the high-level architecture of the VETRI ecosystem, (correctly) identifies all blockchain use-cases at that time, covers the process and results of (only automated) analyses of the main components, and briefly describes the remedies for the identified vulnerabilities and the limitations of the chosen approach.

Because of the high time requirements of a full-blown security analysis of the VETRI ecosystem, not all theoretical findings from the first part of the text were put to practice. The hands-on testing in the practical part is restricted to automated analyses only, utilizing third-party tools. There was unfortunately no time left for an audit /external examination of the architecture and/or manual testing which could bring more useful and actionable results for the authors of the application. Without detailed insight into the individual components of the ecosystem (study of the documentation and architecture of the components in order to find viable attack vectors), the outcomes of the testing are not very information-rich and lack a needed context in some of the cases. On the other hand, I would like to stress out that I don't see the lack of identified vulnerabilities as an issue because the quantity of the findings should not be used as measure of quality of a security testing engagement.

Concerning the factual accuracy, language and literature, I found no major shortcomings when reading the text. The author of the thesis quotes primarily from online resources, which seems understandable, given the novelty of the subject matter. The proposed security framework is based on industry-recognized standards (in the case of smart contracts, it's based on emerging standards).

Personally, I would 'push through' more articles from peer-reviewed journals. Nevertheless, the author quotes several relevant articles (see the Bibliography section), so I don't consider this as a drawback but as a personal note.

Evaluation criterion:	*The evaluation scale: 0 to 100 points (grade A to F).*
3. Non-written part, attachments	*100 (A)*

Criteria description:
Depending on the nature of the FT, comment on the non-written part of the thesis. For example: SW work – the overall quality of the program. Is the technology used (from the development to deployment) suitable and adequate? HW – functional sample. Evaluate the technology and tools used. Research and experimental work – repeatability of the experiment.

Comments:
Configurations, scope of the performed tests, command line inputs and most significant outputs of the used vulnerability scanning tools are documented directly in the main text. Full reports of third-party tools are available in the appendix of the thesis. (The more extensive results of the MobSF analyzer can be found on the enclosed CD.)

The VETRI ecosystem was analyzed when it it was still under active development and an emphasis was placed on non-disclosure of sensitive information (even though the application will be open-sourced in the future). Therefore the level of documentation of the carried out tests seems adequate.

The scope of the performed security testing is discussed below and is not reflected in this point's evaluation.

Evaluation criterion:	*The evaluation scale: 0 to 100 points (grade A to F).*
4. Evaluation of results, publication outputs and awards	*65 (D)*

Criteria description:
Depending on the nature of the thesis, estimate whether the thesis results could be deployed in practice; alternatively, evaluate whether the results of the FT extend the already published/known results or whether they bring in completely new findings.

Comments:
As mentioned above, the proposed security framework is based on industry-recognized (or emerging) standards. Therefore the thesis can be used by information security specialists or software developers as a general introduction to the topic of applications using smart contract.

I gave the lower score because of the high-level detail of the practical part of the text and narrow scope of the performed tests, which makes the employment and interpretability of the results more difficult for the developers of the application and readers of the text. I believe that because of that the usefulness of the developed framework was not demonstrated in its full force.

Manual architecture and/or architecture review of selected components - e.g. communication with the VETRI sidechain via the available interfaces or manual interaction and deployment of the smart contracts seeking for logical flaws - would increase the focus of the performed tests (automated analysis may test strings of irrelevant programming languages, contain REST rules instead of GraphQL that's used in the VETRI ecosystem, don't examine /audit business logic from security perspective or private key management etc.) and could perhaps even enrich the the aggregated resources in the theoretical part with some new findings.

Even the author of the thesis points out that a complete analysis of the VETRI ecosystem goes beyond the defined scope of work, however, I believe that in case of targeting one particular area (see above), it would be possible to perform simple non-automated tests that could potentially bring several suggestions regarding the architecture or non-critical vulnerabilities.

Evaluation criterion:	*The evaluation scale: 1 to 5.*
5. Activity and self-reliance of the student	*5a:* ***1 = excellent activity,*** *2 = very good activity,* *3 = average activity,* *4 = weaker, but still sufficient activity,* *5 = insufficient activity* *5b:* ***1 = excellent self-reliance,*** *2 = very good self-reliance,* *3 = average self-reliance,* *4 = weaker, but still sufficient self-reliance,* *5 = insufficient self-reliance.*

Criteria description:
From your experience with the course of the work on the thesis and its outcome, review the student's activity while working on the thesis, his/her punctuality when meeting the deadlines and whether he/she consulted you as he/she went along and also, whether he/she was well prepared for these consultations (5a). Assess the student's ability to develop independent creative work (5b).

Comments:
Ondřej actively participated in work planning and setting up a timeline, requested missing documentation, consulted the thesis regularly, discussed and incorporated provided feedback and stuck to the agreed on deadlines. He was able to work independently with the provided documentation, source code and security testing tools. Since most of the technology stack in the VETRI project was new to him, Ondřej also demonstrated his ability to quickly find his feet in a new topic.

Evaluation criterion:	*The evaluation scale: 0 to 100 points (grade A to F).*
6. The overall evaluation	*85 (B)*

Criteria description:
Summarize which of the aspects of the FT affected your grading process the most. The overall grade does not need to be an arithmetic mean (or other value) calculated from the evaluation in the previous criteria. Generally, a well-fulfilled assignment is assessed by grade A.

Comments:
By and large, I think the thesis fulfilled its objectives. I praise the choice of a current and less explored topic and the student's ability to guide the reader through the basic concepts (including security) around smart contracts and how they fit in the broader architecture of a typical application software utilizing them. I also believe that the security checklist that concludes the theoretical part can serve well to developers or information security specialists and should be made public as an intro-level tool for those who are not versed in smart contracts or even decentralized applications.

Even though the scope of the theoretical part of the thesis meets the requirements, I decided to grade this thesis B (2) because of the practical part that could be improved via detailed analysis of one particular component of the ecosystem (the most component that fits the aim of the thesis is likely the VETRI sidechain) and/or manual tests exposing how an attack vector via the infrastructure or an interface (mobile and web applications in case of VETRI) can potentially affect the blockchain /smart contract component, which could better illustrate the usefulness of the created security framework and particularities of testing apps using smart contracts (in contrast to a typical client-server architecture).

Signature of the supervisor: