188.959 Software Security VU 2,0h

Final Exam Retake

June 17^{th}, 2020

Instructions

Please read the instructions BEFORE you start writing!

1. For calculations, write the complete calculation. Your solution needs to be comprehensible.
2. Read the questions carefully. Your answer should include only relevant information.
3. Try to keep your answers short.
4. You may answer in either English or German.
5. You can get up to **28 points** for this exam.
6. Whenever you answer a question, you are not allowed to copy text from websites, lecture slides or other students verbatim, except when the question explicitly tells you to. Otherwise use your own words for your answers.
7. Screenshots or images of answers are not allowed as submission.
8. Upload your questions as pdf file to TUWEL and include your name and student ID on the first page of the document.
9. Make sure that you reference the question numbers in your answers.
10. You have 2 and a half hours to upload your answers, i.e. until 17:30.

1. **(3pt) Consider the problem of testing a TLS implementation. Which combinatorial structure lends itself for event-focussed in this setting naturally? Explain your reasoning in detail.**

2. **(2pt) Explain the abstract concept of a fingerprint and give two concrete examples from two different domains.**

3. **(2pt) Give two examples illustrating that there are (potential) issues to be considered when using some form of a (digital or analog) "fingerprint" in practice.**

4. **(2pt) Tracking or fingerprinting users is often associated with a negative connotation. In constrast, give an example where these activities work "on behalf" of a user (i.e., in a positive sense) and describe the reasoning behind it in detail.**

5. **(1pt) Give an example how tracking or fingerprinting could be used in practice for some specific purpose. Explain in detail.**

6. **(2pt) What is "history fingerprinting" and describe one corresponding attack.**

7. **(1pt) Give the definition of a test oracle and provide one for testing the authentication functionality of a website, where the oracle has the form of a requirement.**

8. **(2pts) Explain how black-box testing and white-box testing are applied to penetration testing. Which are their respective goals?**

9. **(3pts) Explain two testing methods and describe how these can be applied to cross-site scripting (XSS).**

10. **(3pts) Assume you are given a combinatorial attack grammar for XSS having k types and g derivation rules per type to form an attack vector. Which of the following is more cost effective in terms of combinatorial testing. Adding more types or more derivation rules per type in the grammar? Justify your answer. (Hint: For an SUT with x variables and y possible values per variable, the number of test cases in combinatorial testing is proportional to $y^t \log x$.)**

11. **(3pts) Describe two testing methods for TLS/SSL implementations.**

12. **(4pts) You are given the following (sample) configuration options for a TLS Cipher Suite:**

Sample Test Suite for TLS Cipher Suite Registry		
Key Exchange Algorithm	**Encryption Algorithm**	**MAC**
RSA	3DES	MD5
RSA	AES	SHA
DCH	3DES	SHA

Has combinatorial testing been employed to generate the test suite? Justify your answer.