188.959 Software Security VU 2,0h

Final Exam

June 10^{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 **25 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. **(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.**

2. **(2pts) Explain what is security testing and penetration testing. How they differ?**

3. **(2pts) Explain how black-box testing and white-box testing are applied to penetration testing. Which are their respective goals?**

4. **(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 $y^t \log x$.)**

5. **(3pts) Which testing method is more likely to cover the input space for X.509 certificate generation? CoveringCerts or Frankencerts? Justify your answer.**

6. **(2pts) Describe two testing methods for TLS/SSL implementations.**

7. **(3pts) 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	SHA256
ECDCH	3DES	SHA256
ECDCH	AES	MD5

Which testing method is most likely to have been employed to generate the test suite? Justify your answer.

8. **(2 pt) In an abstract fingerprinting setting:**

   a) **Describe the terms entity and properties.**

   b) **Describe all the relationships that exist between entities and properties; as well as important characteristics of these relationships in a fingerprinting problem.**

9. **(2pt) Give an application of sequence covering arrays, preferably in software security, and explain their properties in this regard.**

10. **(2pt) Describe in your own words the problem of browser fingerprinting.**

11. **(3pt) List and describe two approaches that can be used for browser fingerprinting.**

12. **(1pt) List two ways in which browser fingerprinting or tracking in general could be used in practice.**

13. **(2pt) The TLS protocol 1.2 allows client/server applications to communicate "securely" with each other.**

    a) **Give one security property that TLS ensures.**

    b) **The TLS handshake consists of messages. Choose one such message and describe it.**