COMP2700 Assignment 2 - Assessment Guidelines

Version 2022-10-13

This assignment has 4 challenges. For each challenge, you are required to submit two components:

- The artefact component (10%): The artefact for each challenge is the flag associated with the challenge: The flags must be submitted through the 'Assignment 2 -- Artefact' quiz link on Wattle. No other forms of submissions are allowed. This will be marked automatically on Wattle. The artefact component accounts for 10% of the total mark for this assignment.

- The report component (90%): For each challenge, you are required to explain in detail your exploration of the challenge, the analysis of its vulnerabilities, and the exploitation steps to obtain the flag that are reproducible. The report component must be submitted through Turnitin using the 'Assignment 2 -- Report' link on Wattle. The report component accounts for 90% of the total mark for this assignment.

Note that unlike Assignment 1, the challenge files for Assignment 2 are not available for download publicly. Instead, they are embedded in the questions in the “Assignment 2 – Artefact” quiz on Wattle, and the student can only view these files after the start the quiz on Wattle. Each student is assigned a unique set of challenges. You are not allowed to share your uniquely assigned challenge files with others, as this can be considered as an act of collusion. This also means that a student who submitted a report without having actually started the quiz will be given 0 mark, and an academic misconduct investigation will be initiated, as it indicates that they may have obtained the challenge files through colluding with another student.

Artefact assessment

The artefact (flag) for each challenge will be marked automatically on Wattle, by an exact match. The flag has the form flag{<some-text>} where <some-text> consists of two or more English words separated by -, for example, flag{hello-world}. Note that you need to include the tag flag{} in your answer, so if the flag you obtained is flag{hello-world} then enter exactly flag{hello-world} in the provided answer box.

The auto-marking on Wattle will be reviewed manually in case there is a mismatch. Minor typos, such as using ‘_’ instead of ‘-‘, or additional spaces, are permissible and will be marked correct manually.

A flag submission for a challenge that is not followed by a report component explaining how the challenge was solved will be given 0 mark.

Report assessment

The report component is required for each challenge.

In general, your report should contain two main components for each challenge:

- An explanation of the vulnerabilities you discovered and how you discovered them. This is where you document your analysis of the problem, e.g., analysis of the design of the relevant cryptographic functions and/or source code, analysis of the provided plaintext/ciphertext, and/or the tests you've done to confirm your hypotheses about the vulnerabilities you found.
- Your attack strategy. Having discovered the vulnerabilities, how do you plan to obtain the flag? Describe your overall strategy, and the reasoning behind it, e.g., why do you think that particular strategy would work? Then map it to the concrete steps you need to do and how they translate into your exploitation steps. You need to explain all these components in some detail, so that the assessor can reproduce your exploitation if needed. If you use computer programs to automate parts of your attack, please list the code in the report. However, code alone is not a substitute for clear explanation in English. Code dumping, without any explanations in English accompanying the code, will not get you any marks.

Your report should be written clearly – pay attention to readability of your report, spelling and grammar, clarity of texts (e.g., if you post screenshots, make sure the important details are clearly readable), etc. A badly typeset report may attract a deduction of up to 5% of the total report mark.

For each challenge, there can be one or more key components that lead to the exploitation. Your report will be assessed against the completeness of your analysis with respect to these key components. If a challenge can be solved in more than one way, you only need to explain the key components for your chosen solution.

Restrictions on the exploitation methods: The challenges for this assignment must be solved using analytical means, without using brute force search on the key space (in the case where the challenge is related to encryption/decryption or computation of message authentication code with a secret key), or in the case of hash functions, without using brute-force search on the output of a hash function to find a second pre-image. Your solutions must be reproducible, so make sure you include key steps required to reproduce the flag. If a challenge comes with an `oracle` that prints the flag (when a correct input is provided), you are not allowed to exploit software vulnerabilities in the oracle program to obtain the flag; this is an assignment on cryptography, not software security. Any flag obtained through exploiting software vulnerabilities in the oracle program will be considered invalid and will get 0 mark.

Length of the report. Your report (containing explanations for all the challenges) should not exceed 3000 words, excluding figures, tables, code and output generated by programs. This is not a hard limit but keep in mind that reports that are exceedingly long will delay the release of your assignment marks.

To give you some ideas of the level of details we expect to see in the report, an example problem and the report containing a solution for that problem, is provided on Wattle (see the file ‘ass2_example.zip’ on Assignment 2 page on Wattle).

Late submissions
No late submissions are allowed without a prior approval from the convener of the course.