APPENDIX C: CONSENT FORM

I, the undersigned,

declare hereby that I, as a participant in a research project in the Department of Electronics and Information Systems under direction of Professor Bjorn De Sutter at Ghent University,

(1) have been informed about the research objectives, the questionnaires I will be asked to fill in, the tasks that I will encounter during the research and that I was given the opportunity to receive further information if desired;

(2) will participate out of free will in the research project;

(3) will participate pseudonymously, which means I will be randomly assigned a participant number electronically, and my personal information such as name and gender will not be collected;

(4) give informed consent to the researchers to record my activities while performing reverse engineering tasks on a virtual machine using the provided data collection software, store my data confidentially, and process and publish my data (as aggregated results or limited samples of individual data) in pseudonymized form;

(5) am aware of the option to stop my participation in this research at any moment in time without having to provide any reason;

(6) know that participating or stopping my participation in the research has no negative consequences of any kind for me;

(7) know that my choice of participation will not be impact my grade, my relationship with the course instructor/teaching assistants in any way;

(8) am aware of the option to ask the researcher(s) for a summary of the results after the study is finished and the results are known;

(9) am aware that UGent is the responsible entity with regards to the personal information collected during the study. I am also aware that the data protection officer can give me more information about the protection of my personal information. Contact: prof. Bjorn De Sutter.

A Priori Questionnaire (Sample)

During the actual experiment, this will be completed online after participants sign the consent form online pseudonymously and receive their participant number, right before their actual participation starts. The questionnaire will consist of the following questions:

1. Your participant number:
2. For how many year(s) have you been programming?
3. For how many year(s), if any, have you been programming for larger software projects, e.g., working in a company, major class projects?
4. Excluding the assignments in the SHP course, how experienced are you with C?

   1: I have very little or no experience and have only written a few lines or snippets of C code not involving pointers.

   2: I have some experience and have written a few lines or snippets of C code, some of which did involve pointers.

   3: I am comfortable with basic C programming and completed some small or medium programming projects in C.

   4: I am very familiar with C and have completed a big project with it.

   5: I am proficient in C and would be comfortable to teach a class about C programming.
5. Excluding the assignments in the SHP course, how experienced are you with x86 assembly language?

   1: I never studied any assembly before.

   2: I never studied x86 assembly before.

   3: I studied (i.e., read and possibly wrote) a limited number of small x86 fragments in isolation, e.g., as part of a computer architecture course.

   4: I studied (i.e., read and possibly wrote) lots of x86 assembly code before, including non-trivial whole functions.
6. On a scale of 1 to 5, which of the following statements best matches your x86 binary code reverse engineering experience excluding the assignments in the software hacking and protection (SHP) course?

   1: I have no additional software reverse engineering experience.

   2: I have tried to reverse engineer small code function/snippets on a couple of occasions.

3: I have tried to reverse engineer larger code fragments.

4: I have worked on many reverse engineering challenges on my own and am familiar with multiple tools.

5: I have (semi-)professional experience with x86 reverse engineering and can perform complicated tasks.

7. Excluding the assignments in the SHP course, how experienced are you with IDA Pro or/and another comparable disassembler such as Binary Ninja or GHIDRA? (For the sake of clarity: objdump is not a comparable disassembler.)

   1: I have never used any such disassembler.

   2: I have used it once or a couple of times.

   3: I have limited experience with it, e.g., took another course that uses them occasionally.

   4: I have lots of experience with it, e.g., completed several medium-level software hacking challenges with them.

   5: I am already very familiar with it and can use advanced features to complete challenging tasks.

8. Excluding the assignments in the SHP course, how experienced are you with GDB or other similar assembly-level debugging tools?

   1: I have never used any such debugger.

   2: I used it occasionally for a class or personal project.

   3: I have some experience with it, e.g., took a programming class that uses them regularly.

   4: I have lots of experience with it, e.g., use it regularly for a major software project or job/internship.

   5: I am very familiar with it and can use advanced features to complete challenging tasks.

9. How experienced are you with software obfuscation techniques deployed on natively compiled software (i.e., C/C++)?

   a. Have you studied obfuscated binary code outside the SHP course? No – a couple of times - extensively

   b. Have you studied obfuscated binary code outside the SHP course? No – a couple of times – extensively

c. Have you tried to deobfuscate code outside the SHP course? No – a couple of times – extensively
d. Have you used automated deobfuscation tools outside the SHP course? No – a couple of times – extensively
e. Have you used obfuscators outside the SHP course? No – a couple of times - extensively

Post Questionnaire (Sample)

After completing the assigned tasks, the participants will fill in a second online questionnaire, again pseudonymously, with the following questions:

- Your participant number:
- For each of the tasks you worked on, list, in chronological order, the reverse engineering techniques that you attempted and the subgoals that you tried to reach with each technique, and whether or not those steps were successful. Listed items should be of the form *<used technique/tool> to <goal>, successful | not successful*. An example of an item on the list could be "used debugger to find location of checksum computation, not successful".