Ethical Committee OS3 Procedures

Version 1.0

Jeroen van der Ham

22nd May 2014

1 Introduction

We believe it is essential for our students to get experience with real world security issues. This experience is highly valued in the field. We also believe that in the increasingly connected world, possible problems will increase with possibly severe impacts. In order to contain the impacts of our findings, we have defined the following procedure for project proposals during the SNE Master.

2 Procedure

Students must write an ethical analysis as part of their project proposal, which should identify risks, possible impact and mitigation.

The teacher of the course evaluates the projects goals and the ethical analysis paragraph and categorises the projects in four different levels:

Green There is no possibility of ethical issues in this project.

Examples are offline analysis of very specific tools, or projects where no possibility exist to access sensitive data of third parties.

Yellow There is a small possibility of ethical issues.

Examples are offline analysis of tools or operating systems, where an issue may allow others to gain access to sensitive data.

Orange There is a real possibility of ethical issues.

Examples are research using personally identifiable information, obtained with prior permission, or sandbox analysis of important secure applications.

Red There are clear ethical issues in this research.

Examples are research where (for whatever reason) personally identifiable information is obtained without prior permissions, or online analysis of applications involving third parties.

An overview of the projects and their indicated levels is submitted to the ECOS3 for evaluation. The projects with *Green* and *Yellow* rating can continue directly. The *Orange* and *Red* ratings are discussed in the ethics committee OS3 (ECOS3) within 2 workdays.

If a *Red* level project is still desired by the ECOS3, this is submitted for consideration with description and explanation to the Ethical Committee Information Sciences (ECIS), and can only continue with their approval. The ECIS will answer within one week.

If a student feels that his/her project is unrightfully stopped by the ECOS3, the student can escalate the issue to the ECIS. The student will submit a written argumentation to ECIS describing the case and argues why the project should not be stopped or labelled with a lower level. In this case the ECIS will also answer within one week.

Periodically an overview of all projects and their levels is submitted to the Ethical Committee Information Sciences. This overview contains the course and projects, their associated level, with a short argumentation for this level. This overview is also archived for later reviewing possibilities.

Yellow, Orange and Red level projects that are undertaken get subsequently increasing supervision by the teacher and lab assistants.

3 Issues and Findings

Any ethical issues (privacy, security, etc.) found by the students during the projects are immediately signalled to the teacher. The teacher submits serious issues directly to the ECOS3. These issues are kept secret until permission has been given by the teacher or ECOS3.

It is possible that due to findings in the project, the level of the project is changed. For most levels this only has implications on the supervision intensity. Should this result in a *Red* level, the project is paused immediately until ECOS3 has examined this, and discussed this with ECIS. The project can then only go ahead with their permission.

If applicable, a responsible disclosure procedure (RDP) is started as soon as possible using the National Cyber Security Centre (NCSC) guideline[1, 2]. This RDP is performed by the ECOS3. During the initial contact ECOS3 will insist on a written indemnification clause. The ECIS is informed of the issue and the responsible disclosure procedure.

4 Committee Members

The ECOS3 consists of:

Programme Director Karst Koymans

Security Track Coordinator Jaap van Ginkel

Ethics Advisor Jeroen van der Ham

References

[1] National Cyber Security Centre *Policy for arriving at a practice for Responsible Disclosure*. URL `https://www.ncsc.nl/binaries/en/current-topics/news/responsible-disclosure-guideline/1/Responsible%2BDisclosure%2BENG.pdf`.

[2] National Cyber Security Centre *Responsible disclosure*. URL `https://www.ncsc.nl/english/security`.