The Supervision of Research Projects Entailing Computer risks within an Academic Context : The Case of Ecole Polytechnique de Montréal

Céline Roehrig[1], José Fernandez[2]

[1]M.A., Advisor to the Dean, Research and Innovation, École Polytechnique de Montréal, Canada
[2]Dept. of Computer and Software Engineering, École Polytechnique de Montréal, Canada

celine.roehrig@polymtl.ca[1], jose.fernandez@polymtl.ca[2]

Abstract

— Information systems security aims to protect information assets, including data, computer systems and computing services, in terms of confidentiality, integrity and availability. The increasing use of information systems in society has led to growing concerns about the security of such systems in recent years. As a result, École Polytechnique de Montréal has encouraged continued research efforts in this field for many years. The institution nevertheless also recognized the risks that this type of research might entail, particularly those research projects pertaining to the study of malicious computer programs (e.g. viruses), the study of vulnerabilities and the study of tools and methods used by malicious actors targeting information assets, or the use of data collected to support research efforts related to the use of actual computer systems. In early 2009, École Polytechnique de Montréal implemented a procedure aimed at supervising the conduct of such research projects. This procedure, the first of its kind within a university context in Canada, aims to provide guidelines for the conduct of research projects which could either i) stop or damage the institution's computer infrastructure, that of its partners or any other entity/individual; ii) damage the institution's information assets, those of its partners or any other entity/individual; iii) incur financial losses to the institution, one its partners or any other entity/individual; iv) affect the availability, the integrity or the confidentiality of the institution's data, that of its students, collaborators or any other entity/individual; v) be harmful to the reputation of the institution or that of one of its collaborators. This paper presents the objectives of this procedure, its underlying principles and the chosen approach to supervise the conduct of such research projects.

Index Terms— Computer risks, Information Systems Security, Research projects, Procedure.

Introduction

Information systems security aims to protect information assets, including data, computer systems and computing services, in terms of confidentiality, integrity and availability. While the benefits of carrying out computer security research can be great, there are also major risks associated with conducting this kind of research, particularly within academia. Indeed, these projects may involve confidentiality and responsible disclosure issues which are associated with the discovery of unknown vulnerabilities or unknown attack types, the use of collections of live malware, or the use of network capture data for testing purposes. They may also involve system and network integrity as well as availability issues associated with experimentation with live malware or synthetic malware-like proof-of-concept code. In an academic context, these risks must be weighed against the sacrosanct academic freedom of researchers but also against the ultimate benefit that these research projects are likely to bring to society.

In recent years, computer security research efforts increased substantially at École Polytechnique de Montréal (Polytechnique) with the appointment of new researchers in that field as well as the establishment of a new experimental facility. Primarily at the request of the researchers active in that field and under the auspices of the Dean of Research and Innovation, a task force was setup to establish an institutional procedure to provide a framework for 1) the evaluation of the risks associated with computer security research projects, 2) the assessment of these projects' foreseeable advantages and disadvantages and 3) the establishment of adequate risk-mitigating measures. This procedure, which was adopted in early 2009, notably establishes and mandates a Computer Risks Evaluation Board (CREB) made of

university administrators, internal and external experts, and researchers from related fields to perform the aforementioned tasks. The procedure requires all researchers within the institution who conduct research that could impact the integrity of computer systems to submit an application to this board and to periodically report on the progress of their research project. This paper presents the objectives of this procedure, its underlying principles and the approach chosen to enforce it.

1. Research projects on information systems security and related risks

The increasing use of information systems in society has led to growing concerns about the security of information systems in recent years. As a result, and given that the design and operation of such systems as well as the protection of related information assets, are an integral part of computer engineering and software engineering in particular, Polytechnique has encouraged continued research efforts in this field for many years. The institution nevertheless also recognized the risks that this type of research might entail, particularly those research projects pertaining to the study of malicious computer programs (e.g. viruses), the study of vulnerabilities and the study of tools and methods used by malicious actors targeting information assets, or the use of data collected to support research efforts related to the use of actual computer systems.

The risks associated with these types of research activities are indeed manifold. Given the ubiquity and ever increasing interactions between our working and research environments, these research activities can have both operational and economic effects including:

- stop or damage the institution's computer infrastructure, that of its collaborators or any other entity/individual;
- damage the institution's information assets (e.g. computer systems, data, computing services), those of its partners or any other entity/individual;
- incur financial losses to the institution, one its collaborators or any other entity/individual;
- affect the availability, the integrity or the confidentiality of the institution's data, that of its students, collaborators or any other entity/individual;
- be harmful to the institution's reputation or that of one of its collaborators.

Given all these risks, and given the fact that neither the federal/provincial granting agencies nor the institution had clear rules governing the conduct of this type of research project, Polytechnique decided to implement a procedure which would explicitly describe the principles and practices it wished to promote with its researchers who conduct research efforts that involve or could potentially involve computer risks. This procedure, its rationale, scope, objectives, the principles it is based upon and the responsibilities it implies, as well as the certification procedure that was implemented to supervise the conduct of research projects involving computer risks are presented below. To our knowledge, this procedure is the first of its kind within an academic context in Canada.

2. Procedure rationale

The procedure that was implemented by Polytechnique aims to impose the highest ethical, integrity and diligence standards to the institution's researchers with a view to maintain and promote its respectability and credibility with the academic community, its partners and the public at large, without compromising the competitiveness of its research teams and the level of work they carry out. This procedure does however not exempt the targeted individuals to comply with all the relevant institutional policies, guidelines and rules including the policies pertaining to probity, the management of research funds, human research ethics and institutional data, the guidelines pertaining to the management of digital documents, to personal information and document disposal and the rules pertaining to the use and management of computing resources. In addition, professors must comply with the provincial and federal granting agencies policies and rules.The policy's primary objectives are the following:

∑ Describe the institution's expectations with regards to the projects conducted within the institution that involve or could potentially involve computer risks;

- Define the general principles that underlie the policy as well as its scope and inform the academic community about them;

- Raise the academic community's awareness and train the latter about the need to respect these principles and the norms that follow from them;
- Describe the duties and responsibilities of the concerned stakeholders;
- Set up a mechanism to assess the projects targeted by the procedure.

3. Frame of reference

The procedure that was implemented by Polytechnique primarily stems from 1) the need to supervise the conduct of research projects which involve or could potentially involve computer risks and 2) the absence of rules governing this type of research. Indeed, none of the federal granting councils nor any of Quebec's provincial granting agencies had any rules governing the conduct of such projects. Although the granting agencies impose strict requirements to the institutions that receive funding from them through the Memorandum of Understanding (MOU) on the Roles and Responsibilities in the Management of Federal Grants and Awards [1], particularly those projects that involve human subjects, animals or biohazards, they did not require research institutions to meet any particular requirements with regards to computer security. The procedure that is presented in this paper was consequently elaborated with a view to fill this gap. It therefore constitutes a complement to the institution's existing policies pertaining to

- probity, the management of research funds, human research ethics and institutional data,
- its guidelines pertaining to the management of digital documents, to personal information and document disposal, and
- its rules pertaining to the use and management of computing resources,

all of which were silent about the way those projects should be handled. At the time it was elaborated, no Canadian university had a similar procedure.

4. Scope of procedure

The procedure applies to all research projects, conducted or supervised by any researcher, which entail or could entail computer risks for Polytechnique's computer infrastructure, that of one of its collaborators or any other entity/individual, including those pertaining to:

- the study of malicious computer programs;
- the study of vulnerabilities and the utilization of commonly used computer systems' flaws;
- the study of tools and methods used by malicious actors targeting information assets;
- the use of data collected to support research efforts related to the use of actual computer systems.

Please note, that within the framework of the presented procedure, computer risks were defined as any scenario or event related to the use of information systems (those of Polytechnique or any other directly or indirectly connected information system that could potentially be affected), that could cause damages to its information assets or affect their relevant confidentiality, integrity or availability properties, that of its partners, or the general public.

Although computer risks can be classified, the institution chose not to do so within the framework of this procedure, due to the difficulty to foresee all possible scenarios. It was however agreed that the level of supervision would depend on the level of risk associated with each project submitted for evaluation.

5. Principles

A series of principles aimed at guiding researchers in the conduct of their research work and the Computer Risks Evaluation Board in its mission to evaluate those research projects that entail or could entail computer risks were enunciated. These principles are as follows:

Proportionality: this principle means that all research projects should be supervised according to the level of risk they may entail as well as the foreseeable advantages and disadvantages of the research project. This notably means that the predictable disadvantages should not be greater than the expected advantages. Moreover, no project should be undertaken unless the researcher can prove he/she has taken all the necessary precautions to avoid any damage

to the institution or third parties caused by the research project under his/her supervision. This also means that when a project entails significant computer risks, the CREB can request more frequent progress reports or refuse to allow the conduct of that project.

The respect for privacy and the protection of personal/confidential information means that researchers have to respect the privacy of individuals as well as all the applicable norms pertaining to the protection of personal or confidential information. They should be particularly cautious when accessing or diffusing such information.

Transparency means that those researchers whose projects entail or could potentially entail computer risks are required to inform the institution about the risks involved so the latter can be adequately managed. It also allows to advice those individuals about whom he/she wishes to use information, about the research project and to allow them to refuse granting access to their information.

The respect of purpose means that those researchers whose projects entail or could potentially entail computer risks must commit to respecting the targeted purpose. This principle is important in that it aims at preventing the research to drift from its original purpose and to prevent any form of abuse. This notably means that those researchers who, during the course of a project, identify other possible uses of the information/data to which they have access, should request the authorization of the CREB before orienting their work in any new direction.

5. Duties

The procedure recommends a sharing of the numerous and manifold liabilities and responsibilities pertaining to computer risks between the various stakeholders involved in the research process, including the researchers, the Computer Risks Evaluation Board, the Research Ethics Board and the Dean of Research and Innovation.

5.1 Researchers

Although liabilities are shared between all stakeholders, it was important for the institution to stress on the fact that the privilege of researchers to conduct the research activities of their choice also comes with the duty to conduct scientific and ethical research work. This also applies to the people he/she (co)supervises. In addition, the institution requires all research projects conducted or supervised by its researchers that might entail computer risks to not only be coherent with its mission, but also to comply with the procedure at hand and to be submitted for evaluation by the CREB before they can be undertaken. Researchers therefore have the duty to design research projects according to the principles and rules enunciated in the procedure.

A "joint responsibility" rule applies to projects carried out by undergraduate and graduate students within the framework of their program of study. On one hand, since the responsibility of supervising such projects lies with the professor, it is his/her duty to make sure that his/her student submits his/her project for evaluation to the CREB. On the other hand, the student must commit to respecting the project's methodological and ethical frame, to inform his/her research supervisor about the progress of his/her research work and about any difficulty encountered during the conduct of the project. Students are encouraged to actively participate in the preparation of the documentation to be submitted to the CREB and to stand up for his/her approach in front of the committee, together with his/her research supervisor, should it have any questions.

5.2 The Computer Risks Evaluation Board (CREB)

The CREB is the body that was set up by Polytechnique to proceed with the evaluation of projects that entail or could potentially entail computer risks conducted at Polytechnique or by its researchers. The CREB has the power to approve, modify or terminate any proposal or the pursuit of any research project that involves or could potentially involve computer risks. It must abide by the procedure at hand and provide adequate training to all the people whose work involves computer risks before the beginning of the research projects it approves. The CREB also has to advise and support Polytechnique researchers with relation to the present procedure or any question pertaining to computer

risks.

The CREB is made of at least four (4) members including :

- A professor or a researcher who is specialized in the field of computer or software engineering. This individual cannot be in conflict of interest with the project submitted for evaluation;
- The director of IT or a designated representative;
- A manager from the Research and Technology Transfer Office or the Research and Innovation Directorate;
- A person from the community connected to Polytechnique but who is not affiliated to it (e.g. an expert in computer security from the private or public sector or a non-profit organization.

One of these people presides the CREB. The quorum is made by at least 3 people. Additional members or substituting members can also be nominated if need be. In case of disagreement, the chairman's vote prevails. The nominations, including that of the chairman and the substituting members, are made by the Management Assembly, upon recommendation of the Dean of Research and Innovation. The members hold their mandate either for two or three years, so that they do not all come to an end at the same time. The mandates are renewable. A person who acts as secretary is also nominated by the Dean of Research and Innovation to support the work of the CREB.

Moreover, whenever the nature or the scope of a project requires a particular expertise or skill that the members of the CREB do not possess, the CREB can call upon an expert to help the committee in its evaluation. These experts can take part in the CREB's discussions according to the rules set up by the chairman, but they do not have the right to vote when such a vote is required.

5.3 The Research Ethics Board (REB)

Because in Canada the confidentiality of personal information and privacy of individuals within the framework of research projects are issues that are already protected by research ethics boards (REB), a tight collaboration between the CREB and the institution's REB was recommended. The institution's REB is the body which is in charge of evaluating those research projects which involve human subjects or the use of personal information. Consequently, projects involving computer risks but also human subjects or personal information must receive the approval of the REB following that of the CREB before they can begin. The REB will therefore help ensure that the projects meet the provincial and federal ethical requirements in terms of privacy, confidentiality as well as free and informed consent of human subjects to participate in these studies. Future projects could include the testing of computer security products involving human interactions, the analysis of network traffic involving both malicious activity and human-generated traffic, etc.

5.4 The Dean of Research and Innovation

The Dean of Research and Innovation is responsible for the elaboration, enforcement and updating of the present procedure. Any question pertaining to the procedure and any other related matter is also submitted to him/her. He/she is also responsible for its diffusion and promotion to the Polytechnique community and to stay aware of the evolution of ideas and practices in this field.

The Dean of Research and Innovation (or the person he/she designates) acknowledges receipt of all research projects to be evaluated by the CREB and issues the certificate of conformity for those projects which entail or could entail computer risks. Those certificates, which are based upon the recommendations of the CREB, attest that the projects meet the current relevant regulation. He/she also provides the administrative and financial support that is necessary to operate the CREB and its members' continuous training. In order to adequately supervise the conduct of projects which might entail computer risks, the Dean of Research and Innovation also commits to:

1. Only make available the funding associated to any project which might entail computer risks to researchers following to the issuance of a certificate of conformity by the CREB;
2. Immediately freeze the access of researchers to the funds associated to any project that involves or could involve computer risks if the institution finds out that a project:

i. violates the institution's procedure pertaining to research projects that involve computer risks;
ii. infringes a relevant provincial or federal law or regulation;
iii. does not observe the conditions of approval imposed by the CREB;

3. Revoke the suspension as described in 2, once the offence has been rectified to the satisfaction of the CREB.

6. Certification procedure

Polytechnique requires that all research projects that entail or could potentially entail computer risks be evaluated by the CREB before they can start. Researchers therefore need to obtain a certificate of conformity, issued by the CREB, which attests that the project meets the institution's applicable requirements.

6.1 Application for a Certificate of conformity

Those researchers whose project involves or could potentially involve computer risks must submit an application for a certificate of conformity to the Dean of Research and Innovation (or the person he/she designates) which includes the following information:

1. An open document which :
   i. Describes the research project, the risks (e.g. malicious codes, equipment overload, nuisance to system operation, network data collection etc.) it may involve and the precautions that the researcher intends to take to minimize them;
   ii. Specifies the research project's source of funding;
   iii. Specifies the duration of the project (or the experiment sequence) and the name of the involved individuals;
   iv. Clearly describes to which data the researcher will need to have access;
   v. Specifies how and where the researcher will collect this data (e.g. will the researcher collect the data at Polytechnique's network input, throughout the network or only part of it?);
   vi. Specifies who will have access to the data, where it will be kept and for what duration;
   vii. Specifies how the data will be destroyed;
   viii. Describes the means to be taken to ensure the anonymity of the collected data;
2. When applicable, a copy of the grant application or of the research contract associated to the project, as well as the award reference number or contract number.
3. If the project involves students, research associates, invited researchers, Polytechnique employees or other individuals who do not have a student status at Polytechnique, the applicable declaration form duly signed.

6.2 Application processing

Upon receipt of an application for a certificate of conformity, the Dean of Research and Innovation, or his/her representative, issues a notice of receipt to the researcher and passes on the application to the members of the CREB. The members of the CREB first assess the relevance of the proposed project. Then, they assess the level of risk associated with the project, as well as the foreseeable advantages and disadvantages of the research project. The CREB particularly makes sure that the foreseeable disadvantages of the research do not outweigh the anticipated advantages and that the researcher has taken all the necessary precautions to prevent any damage to Polytechnique or third parties. Moreover, the CREB makes sure that the researcher observes all applicable norms pertaining to the protection of personal or confidential information, particularly those related to the access and diffusion of such information. Finally, the CREB makes sure that the project complies with all the relevant provincial and federal laws and regulations. A meeting with the researcher who is in charge of the project may be requested and organized by the CREB.
When the CREB is content with the project and is convinced that it can be carried out safely, it notifies the Dean of Research and Innovation about it, who then issues a certificate of conformity to the researcher which attests that the project complies with all the relevant rules. It also transmits a copy to the Research and Technology Transfer Office.

If a project spans several years, or if it involves several phases, and the work that involves or could potentially involve computer risks is not conducted from the start, the project can be evaluated within the framework of a two-stage process. In this instance, part of the funding can be released for the portion of time which does not involve any

computer risks, after the approval in principle of the research protocol (through a memorandum of agreement). In any case, a certificate of conformity must be obtained by the researcher before the start of the research work involving or potentially involving computer risks.

6.3 Follow up supervision of the approved projects

For the entire duration of the project, researchers must notify the CREB without delay about any modification to their research project that entails or could potentially entail computer risks. Researchers also have the duty to submit an annual report which describes the unwinding of the project, the encountered difficulties and delays, including any change with respect to the original project. Furthermore, the institution reserves the right to conduct verifications at any time to ensure that the measures recommended by the CREB, in concert with the researcher in charge of the project, to supervise the computer risks that a project may entail, are adequately implemented.

6.4 End of project

Researchers must submit a final report at the termination of their project to the Dean of Research and Innovation.

7. Sanctions for non compliance

Polytechnique shall not tolerate any activity that contravenes to the present procedure or its mission, particularly if it affects its computer infrastructure, leads to the loss, theft or leak of data or intellectual property, to the infiltration of the institution's computer infrastructure by malicious codes introduced intentionally or inadvertently, overloads its equipment etc. Consequently, in case of non-compliance with its institutional procedure or any relevant federal or provincial law, regulation, procedure or guideline pertaining to research that involves or could potentially involve computer risks, including Quebec's law pertaining to the access to documents and personal information held by public bodies [2], Polytechnique could take any measure deemed necessary depending on the gravity of the committed offence. Polytechnique can notably suspend without notice the payment of the research funding associated with the project in question.

Conclusion

Polytechnique's procedure pertaining to the supervision and follow up of research projects that involve or could potentially involve computer risks is, to the authors' knowledge, the first of its kind in an academic context in Canada. It is hoped that this institutional initiative can serve as a template framework for the conduct and supervision of such projects in other academic institutions around the world. The authors believe that this initiative could induce other institutions that have researchers who are active in these fields of expertise, impose similar procedures to their researchers and thereby maintain and promote their respectability and credibility with the academic community, their collaborators and the public at large. At a time where the security of information systems is regularly questioned due to unpredicted attacks of all kinds, the pursuit of research efforts, notably in the field of information systems security, appears more relevant than ever before. However, since the conduct of such projects entails major risks, we believe that research institutions have a duty to prevent these risks, as any other kind of risk, due to their potential financial and other impacts. As such, our hope is to provide a regulatory framework, so that computer risks can be adequately evaluated and managed by the academic institutions conducting this kind of research, while allowing society to benefit from its results.

References

01. Memorandum of Understanding (MOU) on the Roles and Responsibilities in the Management of Federal Grants and Awards http://www.nserc-crsng.gc.ca/NSERC-CRSNG/Policies-Politiques/MOURoles-ProtocolRoles/index_eng.asp
02. Loi sur l'accès aux documents des organismes publics et sur la protection des renseignements personnels (http://www2.publicationsduquebec.gouv.qc.ca/dynamicSearch/telecharge.php?type=2&file=%2F%2FA_2_1%2FA2_1.htm)