Date: Tue, 18 Mar 1997 22:42:12 -0700 (CST)
From: Keith Miller <miller@uis.edu>
To: weil@charlie.cns.iit.edu
Subject: My last revision

TESTING, RELIABILITY, AND TRUSTWORTHINESS:
Informed Consent and the Computing Professional

INTRODUCTION

All professionals have responsibilities and privileges due to their role. Computer professionals are trusted to make technical decisions about software and hardware. These decisions require sensitivity to human values as well as technical expertise.

The interaction of human values and technical decisions is particularly important in the area of software quality. The question of "how good is good enough" requires values clarification, allocation of resources, prediction of costs, and analyses and predictions that cannot be based on certainty, but should be based on measurement.

Most software is so complex that guaranteeing perfection in PRODUCT quality, while highly desirable, is infeasible. However, guaranteeing adherence to mutually agreed-upon development PROCESSES from which product quality can be expected to flow is feasible. In the suggestions below we insist that both product and process be addressed when dealing with professional responsibilities for software quality.

We propose that computer professionals adopt an ethical standard of "informed consent," as outlined below.

GUIDING PRINCIPLE

A software developer should obtain informed consent from the client. A software user should have available information about the safety and reliability of software. The public should be able to obtain detailed information about the testing and reliability measures of any commercial software.

DEFINITIONS

"software" : computer programs, internal documentation, design documents, test plans, user manuals, online help, and the like

"software developer" : any professional involved in the production of computer software; this includes but is not limited to designers, coders, testers, managers, and salespeople

"client" : the person or entity that pays for the software

"user" : any human who interacts with the software

"public" : any citizen or organization

"informed consent": see below

INFORMED CONSENT

"Informed consent" is a term used in medical ethics. We borrow this term and define it for computer professionals as follows:

The client of a computer professional who is buying software should be given

sufficient information to make a reasonable choice about investing in the software. The developer should disclose information at an appropriate level of detail. The acceptance of the client should be voluntary, and should include a formal authorization whenever possible.

Words such as "sufficient," "reasonable," and "appropriate" can only be defined specific to a particular situation. Part of a professional's responsibility in informed consent is to make these definitions in a good faith for each particular exchange with a client.

Sometimes the people who buy software are remote from the developer; for example, shrink wrapped software clients. In this case "informed consent" will not be formalized in the same way that it can be when custom software is developed for an individual client. However, informed consent can be approximated in this cases by a good faith effort to make disclosure information available to a customer before purchase.

Except for those cases where the client cannot be negotiated with directly (such as shrink-wrapped software), we assume below that the client or a representative of the client is available. When the client is not available for direct consultation, the quantifiable information required for informed consent should be available to customers shopping for software.

IMPLEMENTATION OF INFORMED CONSENT

The developer should create as part of a contract or as a separate document an informed consent form. This document discloses the information presented by the developer about software quality, and the client's willingness to accept the software knowing the measurements and limitations included in that document. Informed consent is complete when both the developer and the client sign the document.

CONTENTS OF AN INFORMED CONSENT DOCUMENT

I. Product Measurements:

This section includes any and all software quality measures agreed to by the developer and the client. These could include mean-time-to-failure under a certain distribution of inputs; software metrics, either as an average or within an acceptable range over all modules; safety conditions that are never violated after a certain number of random tests; or any other repeatable, verifiable measures. When presenting the informed consent document for signing, the developer demonstrates that the software meets or exceeds the agreed upon measures. Measures must be defined in such detail (such as margins for error, significant digits, rounding protocols) as to be unambiguous. Each measurement should be defined in a single reference document that includes this type of detail.

II. Process Description:

This section describes the processes used to develop the software and to verify its software quality. The developer describes how adherence to the process guidelines is verified. Each process must be described in a single defining reference document.

III. Assessment Implementation:

This section details who assesses compliance with the product measurements and the process requirements. This section may include details about who is responsible for what in the assessment phase; for example, either the client or the developer may be responsible for the generation of test cases.

CONTRACT RAMIFICATIONS

Informed consent should be a binary transaction: either the two parties mutually accept it, or they do not. Mutual acceptance of an informed consent document is part of the final phase of a software project. The development of the document should begin in the earliest phases of development, but it cannot be signed until all the described measurements and assessments have been completed. A contract can make reference to the time when this document is signed to determine bonuses or penalties, but the document itself should focus on software quality, not schedule or payment. The issues of time and money are a vital part of the negotiations between client and developer on what level of quality are acceptable; however, informed consent, once agreed to, becomes a required step in acceptance. Renegotiating informed consent is possible, but not encouraged.

INFORMED CONSENT DOCUMENTS AS PUBLIC ARCHIVES

The informed consent document is made available by the developer in paper form (at minimal cost) and electronically (without cost) to the public. User documentation gives information about how to access the document. The IEEE Computer Society maintains a directory to all such electronic documents for publicly available software.

==========

WHY I THINK THIS MIGHT WORK

The description above does not require any particular style of testing or verification. I do research in testing and reliability techniques, and I cannot imagine that the research community or the business community will ever reach consensus about which techniques should be required. The informed consent form does require mutually agreed to measurements of some kind. This seems like a minimum level of professionalism.

By not including contractual details in the document, parties to the consent should be willing to make the document public. A collection of documents could be a rich source of information for researchers in software quality, and public display of these documents would encourage more responsibility from developers and clients.

We have to do SOMETHING to encourage professionalism in software development. Perhaps an informed consent emphasis will help.

--

Keith Miller
miller.keith@uis.edu
office: (217) 786-7327
fax: (217) 786-7188

University of Illinois at Springfield
Computer Science Department, HSB 137
Springfield, Illinois 62794