MTAT.07.006 Research Seminar in Cryptography
Comments on “Program Obfuscation. A Small Overview”

Mart Sõmermaa

January 10, 2006

1 Overview

The survey gives an overview of obfuscation. Obfuscation is a transformation that maps program code to behaviourally equivalent code that can not be reverse-engineered.

First half of the article discusses the theoretical results regarding obfuscation. The most important result is negative – it has been proven, that generic obfuscators don’t exist. If they did, they would have many interesting applications, e.g. construction of homomorphic and public key cryptosystems.

Regardless of the negative theoretical result, there is industry interest in obfuscation technologies and some research has been conducted in adhoc obfuscation techniques that should make program reverse-engineering infeasible. Second half of the aricle gives an overview of these techniques.

2 Remarks

The article is well structured and seems to cover most important aspects of obfuscation. The general impression is good.

2.1 Style

The language of the article is at times informal, especially in the beginning. This is inappropriate for an academic text. Phrases like ”sort of” and ”thing called” should be avoided. However, this applies only to specific passages, most of the text is well-written.

There are some spelling and grammar mistakes, but these do not affect readability nor the overall impression.

A minor note – index [1] is repeating in the references, these should be re-checked.

2.2 Content

The discussion of the theoretical background might have been a little more profound. What I felt missing was the treatment of the recent positive research results on obfuscation and how do these relate to the negative result. There’s a recent paper (also referred to in the article) that claims that point function obfuscation is possible. Quite evidently point functions can be used as building blocks in more complex obfuscation transforms. It remains open how limited or generic such composition can be.

3 Conclusion

The article gives a good overview of the subject, is readable and well structured.