Abstract

Software developers rely on obfuscation techniques for protecting their source code against reverse engineering attacks. Most of the obfuscation techniques are not based on well-defined measurements to clarify their effectiveness in protecting the source code from both dynamic and static analysis by human subjects. This study presents an experimental technique towards the aim to provide an assessment tool that investigates the impact of control flow obfuscation on software protection against human attacks. The main objective is to estimate how the obfuscation prevents or limits the ability of the attacker to understand and to perform any modification on the source code. An experiment was designed to assess the capabilities of the control flow obfuscation technique with the opaque predicates in preventing or limiting the attacks on source code.

As a result of the statistical analysis used in this study, it is shown that the presence of obfuscation on source code increases seven times the difficulties for the attacker to successfully complete the understanding task. Also, the control flow obfuscation significantly reduces the capability of subjects to correctly perform the understanding tasks while there is no significant difference for modification tasks. Also, it is shown that the presence of obfuscation on source code increases the amount of time needed for subjects to perform modification and understand the source code.

الملخص

يعتمد مطوروا البرمجيات على تقنيات تشويش الشفرات المصدرية للبرمجيات في حماية برامجهم ضد هجمات الهندسة العكسية من قبل المهاجمين. معظم تقنيات التشويش لاتعتمد على قياسات وأدلة واضحة من اجل معرفة مدى فعاليتها وكفائتها في حماية الشفرات المصدرية للبرامج. تقدم هذه الدراسة تحقيقاً عملياً يهدف إلى دراسة تأثير تشويش الشفرات المصدرية للبرامج على حماية البرامج ضد الهجمات البشرية. تم تصميم تجربة عملية تهدف لدراسة وتقييم قدرات تقنيات التشويش في منع أو الحد من قدرة المهاجم على فهم وتنفيذ أي تعديل على الشفرة المصدرية.

تبين نتيجة التحليل الإحصائي المستخدم في هذه الدراسة ، أن وجود التشويش على الشفرة المصدريه للبرنامج يزيد سبعة أضعاف الصعوبات التي يواجهها المهاجم من أجل فهم الشفرة المصدرية للبرنامج بشكل صحيح، بينما لا يؤثر التشويش بشكل كبير في حالة أراد المهاجم التعديل على الشفرة المصدرية للبرنامج. أيضاً ، يتضح أن تشويش الشفرة المصدرية يزيد من مقدار الوقت اللازم للمهاجم لفهم وتعديل الشفرة المصدرية.