Erhöhung der quantitativen Messbarkeit von Softwareschutz-Techniken

(Technologietransfer)

Projektverantwortliche	**Dr. Sebastian Schrittwieser (sebastian.schrittwieser@univie.ac.at)**, DI Patrick Kochberger
Projektbeschreibung	Das Projekt EMRESS (Evaluation Models for the Resilience and Stealth of Software Protections and Malware) beschäftigt sich mit dem Problem der Quantifizierbarkeit von Softwareschutztechniken, welche sowohl in kommerziellen Programmen als auch in Schadsoftware (Malware) eingesetzt werden. Obwohl diese Techniken seit mehr als zwei Jahrzeiten erforscht und in der Praxis sehr häufig verwendet werden, gibt es bis jetzt keine belastbaren Modelle, welche für eine vorliegende Software die Stärke von möglichen Schutzmechanismen ermitteln können. Das Fehlen solcher Modelle ist höchst problematisch zum einen für Softwareanbieter, welchen automatisierte Entscheidungssysteme für die Wahl der optimalen Schutzstrategie für ihre Software fehlt, und zum anderen für Schadsoftware-Analysten, welche in Abhängigkeit der eingesetzten Schutztechniken der Schadsoftware die passende Analysestrategie festlegen müssen. Ziel des Forschungsvorhabens ist die Erstellung von quantitativen Prädiktionsmodellen für die Stärke von Softwareschutztechniken in Bezug auf die beiden Eigenschaften Resilience (Stärke des Schutzes gegenüber verschiedenen Analysestrategien) und Stealth (Verdecktheit des Schutzes). Die Quantifizierbarkeit der Resilience soll durch die Entwicklung neuartiger Modelle und Metriken geschehen, die prognostizieren können, inwieweit ein Softwareanalyst bestehende Schutzmechanismen durch die Verwendung von State-of-the-art Tools und Software-Analysetechniken rückgängig machen kann. Die Stealth von Softwareschutzmechanismen soll durch die Entwicklung von neuartigen Techniken zur Identifikation von Codebereichen in Software mit einer vorgegebenen Semantik quantifizierbar gemacht werden. Die Ergebnisse des Projekts EMRESS sollen den wissenschaftlichen State-of-the-art im Bereich der Quantifizierung von Softwareschutzmechanismen sowohl in der Theorie als auch in der Praxis signifikant verbessern. Weiters werden positive Effekte für die Forschungsfelder des Software-Testens und der Software-Assurance erwartet.
Schlagworte/Keywords	Softwareschutz, obfuscation, malware

Zentrale Ziele der Third-Mission-Aktivität	Softwareschutz-Techniken (beispielsweise Code Obfuscation) werden eingesetzt, um die exakte Funktionsweise eines Programms bzw. darin enthaltende Daten vor Analyse (Reverse Engineering) zu schützen. Eine Quantifizierung der Stärke einer Schutztechnik ist mit bisherigen Methoden jedoch nicht möglich. In unserer Aktivität erforschen wir neuartige Konzepte mit dem Ziel die Stärke von Softwareschutz-Techniken messbar zu machen.
Universitätsexterne Kooperations-partner*innen	Keine
Kooperations-partner*innen aus dem Wissenschafts- bzw. Forschungsbereich	Ghent University, Belgien
Fakultät	Fakultät für Informatik/Forschungsgruppe Security & Privacy
Projektlaufzeit	1.10.2020 - 30.6.2022
Finanzierung	FWF
Forschungsbasierung	Sebastian Schrittwieser forscht seit 10 Jahren im Gebiet der Code Obfuscation. In seiner Dissertation hat er sich mit Hardware-unterstützten Schutztechniken für Software beschäftigt.
Gesellschaftliche/Wirtschaftliche Relevanz	Softwareschutz-Techniken werden in nahezu jeder kommerziell vertriebenen Software eingesetzt (zum Beispiel in Form eines Kopierschutzes für ein Computerspiel). Da jedoch die Stärke einer Technik nur unzureichend bewertet werden kann, bleiben auch wichtige Parameter für die Abschätzung des wirtschaftlichen Erfolgs des Software-Produkts unklar.
Einbindung der Third-Mission-Aktivität in die Lehre	Nein
Ergebnisse/Wirkung (Impact)	In der Theorie kann jede Schutztechnik für Software durch Reverse Engineers mit genügend Ausdauer und Motivation gebrochen werden. Jedoch zeigt sich in der Praxis, dass die Verbreitung von Schutztechniken in kommerzieller Software und Schadsoftware hoch ist. Eine bessere Messbarkeit der Stärke von Schutztechniken hilft Unternehmen bei der Umsetzung einer geeigneten Schutzstrategie ihrer Software.

Transferaspekt der Aktivität	Unsere Aktivität ermöglicht Software-Entwickler*innen eine bessere Planbarkeit und eine zielgerichtetere Umsetzung von Schutztechniken für Software.
Nachhaltigkeit & Zukunftsorientierung	Unsere Aktivität fördert nachhaltig die Implementierung von geeigneten Schutztechniken in der Software-Branche. Die Messbarkeit der Stärke von Schutztechniken ermöglicht in Zukunft eine schnellere Entwicklung neuer Methoden und einen zielgerichteteren Einsatz bestehender Techniken.
Überprüfung der Zielerreichung der Third-Mission-Aktivität	In der Aktivität sind Studien mit professionellen Reverse Engineers geplant, welche die Zielerreichung evaluieren sollen.
Maßnahmen, um die Transferaktivität längerfristig durchzuführen bzw. auszuweiten	Nach Beendigung des aktuellen Projekts (FWF) sind weitere Projektanträge im Themenkomplex der Aktivität geplant.
Sichtbarmachung	Eine Projektwebseite ist in Arbeit.
Homepage/Publikationen	/