Verwendung von Klonerkennung zum Auffinden von Signaturen von Malware-Familien: Eine Fallstudie über FinSpy

Nils Scheidweiler
Nils.Scheidweiler@uni-jena.de
Friedrich-Schiller-Universität Jena

André Schäfer
Andre.Schaefer@uni-jena.de
Friedrich-Schiller-Universität Jena

Wolfram Amme
Wolfram.Amme@uni-jena.de
Friedrich-Schiller-Universität Jena

Thomas S. Heinze
Thomas.Heinze@dlr.de
Deutsches Zentrum für Luft- und Raumfahrt

Abstract
Bei der Entwicklung von Malware wird oftmals existierender Code wiederverwendet. Die Suche nach Code, der bekannter Malware ähnelt, kann daher für die Malwaredetektion eine vielversprechende Strategie sein. Nach einer Vorstellung verschiedener Techniken zur Malwaredetektion analysieren wir die Verwendung des Klon-Detektors StoneDetector zum Auffinden von Android-Malware. StoneDetector erzeugt aus Quellcode die Kontrollflussgraphen und wandelt diese in Dominatorbäume um. Durch die Extraktion der Pfade von den Blättern zur Wurzel eines Dominatorbaums werden Beschreibungsmengen gebildet. Mithilfe von bösartigen Samples einer Malwarefamilie und gutartigen Samples werden Beschreibungsmengen gesucht, die in den meisten bösartigen Samples, aber nicht in den Gutartigen vorkommen und diese Beschreibungsmengen als Signatur der Malwarefamilie extrahiert. Die Machbarkeit des Ansatzes wird anhand einer Fallstudie mit Android-Samples der FinSpy-Malwarefamilie gezeigt. Es werden 31 FinSpy und 20 gutartige Samples in eine Trainings- und eine Testmenge unterteilt und die Signatur mithilfe der Samples der Trainingsmenge gebildet. Für die Beurteilung wird die FinSpy Signatur in bösartigen und gutartigen Samples der Testmenge gesucht. Es kann gezeigt werden, dass mit dem Ansatz alle getesteten bösartigen und gutartigen Samples richtig klassifiziert werden.