InnoSecBW

CYBERSECURITY-BOOSTER-BERICHT
WIBU-SYSTEMS AG

Ein Projekt des

FZI

FZI Forschungszentrum Informatik
Haid-und-Neu-Str. 10–1476131
Karlsruhe

Gefördert durch das

Baden-Württemberg
MINISTERIUM FÜR WIRTSCHAFT, ARBEIT UND TOURISMUS

Die WIBU-SYSTEMS AG ist Hersteller von innovativen Lösungen zum Schutz und zur Lizenzierung von Software. Mit Hilfe dieser Lösungen können Firmen ihre Software vor Raubkopien schützen und Lizenzierungsmodelle technisch durchsetzen.

PROBLEMSTELLUNG

Um mit den Fähigkeiten von Angreifern mithalten zu können, müssen die Lösungen stets überprüft und weiterentwickelt werden. Außerdem ist es wichtig, dass Firmen den Softwareschutz möglichst einfach auf ihre bestehende Software anwenden können. Im Rahmen des Cybersecurity-Boosters haben die WIBU-SYSTENS AG und das FZI Forschungszentrum Informatik aktuelle Analysemethoden und deren Weiterentwicklung als Forschungsfragen erfasst.

Zum einen wurde das BlurryBox-Verfahren betrachtet, das Softwarelizenzierung mittels Hardware-Dongle umsetzt. Während es zwar in einem theoretischen Modell beweisbar sicher ist, so sind Fragen in Bezug auf die Praxistauglichkeit noch ungeklärt. Aktuell ist die Technik noch nicht automatisiert integrierbar. Hierfür ist ein aufwendiges manuelles Anpassen der Software notwendig.

Zum anderen wurde die Anwendbarkeit sowie Sicherheit von rein softwarebasierten Verfahren betrachtet. Das Produkt AxProtector CTP der WIBU implementiert ein solches Verfahren, setzt jedoch bislang die Nutzung bestimmter Kompilierwerkzeuge voraus. Außerdem müssen rein softwarebasierte Ansätze besonders resilient gegenüber einer Vielzahl von Angriffstechniken sein.

STAND DER KUNST UND VORGEHEN

Die Sicherheit von BlurryBox basiert auf der Verwendung sicherer Hardware, bspw. in Form eines Hardware-Dongles, sowie hinreichender Komplexität der zu schützenden Software. Kritische Programmbestandteile sind nur noch verschlüsselt verfügbar und können

nur mit Hilfe des Dongles ausgeführt werden. Außerdem werden Fallen im Programmcode versteckt, die in einer realen Ausführung niemals aufgerufen werden, deren Entschlüsselung als Angriff interpretiert wird und den Dongle deaktiviert.

Konkret wird von der Software gefordert, dass sie einerseits eine hinreichend verzweigte Struktur aufweist, und andererseits Programmteile in nichttriviale Codevarianten aufgeteilt werden können, die nur für einen bestimmten Wertebereich gültig sind. Dies muss bisher manuell sichergestellt werden. Im Rahmen des Cybersecurity-Boosters wurde untersucht, welche Arten von Hürden bei einer automatisierten Variantenbildung auftreten können. Dabei wurden einige offene Forschungsfragen identifiziert, deren Beantwortung intensivere Forschung erfordert, wofür ein gemeinsames Förderprojekt für FZI und WIBU beantragt wurde.

Der rein softwarebasierte AxProtector CTP basiert auf verschleiernden Codetransformationen, die beim Kompilieren angewendet werden. Damit Anwender ihre Software nicht mehr auf vorgegebene Kompilierwerkzeuge portieren müssen, hat WIBU im Rahmen des Cybersecurity-Boosters ein Konzept vorgestellt, mit dem der Schutz auf bereits kompilierte Programme angewendet werden kann. Dafür sollen ausführbare Binärdateien zurück in die LLVM-Zwischensprache übersetzt werden, wo der Schutz angewandt und schließlich wieder zurück in das native Format kompiliert werden. Das FZI hat Angriffsvektoren auf softwarebasierten Lizenzierungsschutz identifiziert und weitere Schritte zur Erforschung vorgeschlagen. Diese Forschung soll im Rahmen eines weiteren Förderprojekts aufgenommen werden, welches WIBU und FZI beantragt haben.

Erkenntnisse und Nutzen

Das FZI hat in Zusammenarbeit mit WIBU offene Problemstellungen im Themenbereich Softwareschutz identifiziert und erste Lösungsansätze entworfen. Die gewonnenen Erkenntnisse werden Unternehmen mittelfristig dabei helfen, ihr geistiges Eigentum und ihre Lizenzierungsmodelle besser zu schützen und so Einnahmen zu sichern. Gemeinsam haben die Partner zudem Projektanträge bei öffentlichen Förderprogrammen eingereicht, um die identifizierten Lösungsansätze weiter zu erforschen und konkretisieren.