Zürcher Hochschule
für Angewandte Wissenschaften

School of
Engineering

InIT Institut für angewandte
Informationstechnologie

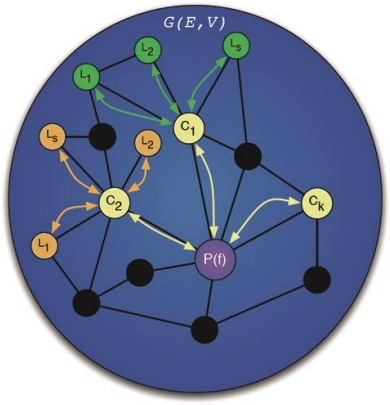
Konzeption und Implementierung von Schutzmassnahmen für ein Softwareprodukt

Diplomierende
Enrico Bozzolini
Roland Krummenacher

Dozent
Marc Rennhard

Die Software des Industriepartners dieser Arbeit ist eine Client-Server-Applikation basierend auf Microsoft .NET zur Überwachung und Analyse von Produktionsprozessen. Sie wird eigenständig oder zusammen mit kompatiblen Produktionsmaschinen verkauft. Die Software wird auf unterschiedliche Weise lizenziert, bislang ist sie jedoch gegen Lizenzmissbrauch technisch nicht geschützt. Sie kann somit auch mit Konfigurationen betrieben werden, die nicht der Lizenzabmachung entsprechen oder als Mietsystem vor Ablauf der Mietfrist kopiert werden. Im Rahmen dieser Arbeit wurden die vollständigen Anforderungen erhoben und Massnahmen evaluiert, um die Software gegen Lizenzmissbrauch zu schützen. Diese Massnahmen lassen sich in drei Kategorien aufteilen:
- Lizenzschutzmassnahmen überwachen die Einhaltung der Lizenzvereinbarungen (Mietfrist, Anzahl lizenzierter Anlagen, Anzahl lizenzierter Datenbanken).
- Kopierschutzmassnahmen stellen sicher, dass die Software nur auf dem ursprünglichen System betrieben wird.
- Schutz gegen Software-Manipulation verhindert, dass Lizenz- oder Kopierschutzmassnahmen überlistet oder entfernt werden.

Aufgrund der Evaluation einer Vielzahl von Hard- und Softwarelösungen wurde entschieden, die Softwareprodukte DeployLX Licensing und DeployLX CodeVeil des kalifornischen Herstellers XHEO zu erwerben. Diese Produkte haben im Test bezüglich der vorgegebenen Anforderungen sehr gut abgeschnitten. Es ist auch ein Entscheid gegen eine Hardware-Lösung, da von Seiten des Industriepartners schlechte Erfahrungen beim Einsatz von Kopierschutzsteckern gemacht wurden. Im Anschluss an die Evaluation wurde eine gegebene Testapplikation mit den geplanten Schutzmassnahmen ausgerüstet. Neben der Sicherstellung von kundenspezifischen Lizenzvereinbarungen (z.B. Miete, Demoversionen oder featurebasiertes Lizenzieren) konnte auch ein effektiver Kopierschutz implementiert und die Applikation durch Verschleierung vor Quellcode-Manipulationen geschützt werden. Dank dem sehr grossen Funktionsumfang von DeployLX wurden sämtliche Anforderungen und Anwendungsfälle umgesetzt oder zumindest so konzipiert, dass die spätere Umsetzung keine Probleme mehr bereiten sollte.



Das Bild zeigt ein Modell eines zufällig aussehenden Programmgraphen mit Knoten L, Checksummen C und Prüfroutinen P. Die Checksummen testen den Quellcode auf Manipulation und melden die Resultate der Prüfroutine. Diese Prüfroutine besitzt einen Schwellenwert f, d.h. die Kontrolle meldet erst dann einen Manipulationsversuch, wenn von den k Teiltests f fehlschlagen. Somit weiss der Angreifer bei sinnvoller Implementierung der einzelnen Teilschritte nicht, welche der Prüfroutinen, die nun an dem Fehlschlag beteiligt sind, dafür verantwortlich sind.