5. Juli 2021 Studie · Mobile Sicherheit · Web & Cloud

Android Application Patching durch Runtime-Manipulation

Der Volltext liegt derzeit nur in der Fassung „English“ vor. Die Übersetzung folgt.

Archiviert. Dieser Inhalt wird nicht mehr aktualisiert. Er bleibt zur Information verfügbar.

Stand 2021-06-23
Quelle https://technology2.a-sit.at/veroeffentlichungen/android-application-patching-durch-runtime-manipulation/

Application Patching ist ein vielversprechender Ansatz, mit dessen Hilfe der Ausführungs-Fluss einer kompilierten Android-Applikation modifiziert werden kann, um ihre Implementierung zu analysieren, Fehler zu beheben oder neue Funktionalität einzufügen. Während traditionelles statisches Application Patching rechenintensiv ist und daher auf leistungsstarker Desktop-Hardware ausgeführt werden muss, kann ein dynamischer Ansatz, der die Datenstrukturen der ART-Runtime modifiziert, am Gerät selbst operieren und die Technik damit für viele weitere Anwendungsfelder öffnen.

In diesem Forschungsprojekt haben wir die Machbarkeit und Praktikalität dieses Ansatzes untersucht. Mehrere bestehende Open-Source-Implementierungen wurden identifiziert und auf ihre Stärken und Schwächen hin analysiert. Auf Basis der verlässlichsten Kernkomponenten und einem Verständnis für die Implementierungsdetails der ART-Runtime wurde dann eine neue Lösung für das dynamische Intercepten von Methodenaufrufen in beliebigen Android-Applikationen realisiert. Die resultierende Software-Bibliothek wurde in eine komplette On-Device Application-Patching-Pipeline integriert und erfolgreich an mehreren der beliebtesten Android-Applikationen aus dem Google Play Store getestet.