Titel

Sicherheitslücken in Android-Apps durch die Demonstration von Angriffen aufspüren

Referent(en)

Stefan Gärtner, Leibniz Universität Hannover

Mitautor(en): Thorsten Kerber, mediaTest digital / Kurt Schneider, Leibniz Universität Hannover

An wen richtet sich der Beitrag?

Sicherheitsexperten, Qualitätsbeauftragte und Entwickler mit einem Schwerpunkt auf Sicherheit und Apps

Stichwörter

Sicherheitslücke, Angriffsdemonstration, Android

Zusammenfassung

Die Sicherheit bei Android-Anwendungen (Apps) rückt zunehmend in den Fokus der öffentlichen Aufmerksamkeit. Das liegt einerseits am umfassenden Einsatz von Apps im Alltag (z.B. Online-Banking, soziale Netzwerke). Andererseits nimmt auch der professionelle Einsatz von Apps in vielen Unternehmen zu. Die Ausnutzung etwaiger Sicherheitslücken in Apps durch einen Angreifer bedroht somit viele Lebens- und Geschäftsbereiche. Wenn daher ein Angriff bekannt wird, müssen App-Entwickler umgehend reagieren: Sie müssen so schnell wie möglich identifizieren, welche Sicherheitslücke der Angreifer in der App ausgenutzt hat und diese schließen. Entwicklern fehlt jedoch oft die Expertise, den Angriff nachvollziehen zu können und den Teil im Quelltext zu finden, der ihn ermöglicht hat.

Häufig werden von einfallsreichen Angriffen Mechanismen missbraucht, bei denen im Vorfeld nicht unbedingt absehbar war, dass diese sicherheitskritisch sind. Ein Beispiel ist hierfür der Angriff über manipulierte QR-Codes. Sie können somit kaum durch herkömmliche qualitätssichernde Maßnahmen gefunden werden. Überdies interagieren Apps typischerweise über Sensoren, Internet und vielerlei andere Weise mit ihrer ohnehin dynamischen Umgebung. Dadurch eröffnen sich hier besonders viele Querbezüge, die Angreifer auf ungeahnte Weise ausnützen können. Das geschilderte Problem ist bei Apps damit besonders gravierend.

Wir stellen ein Eclipse-basiertes Werkzeug vor, mit dem wir die Analyse von Angriffen zielführend unterstützen, um das Auffinden der ausgenutzten Sicherheitslücken im Code der App zu erleichtern. Die Sicherheitslücken können dann von den App-Entwicklern rasch behoben werden. Aufwendiges Suchen nach der Sicherheitslücke im Code durch den Entwickler wird somit vereinfacht. Dabei setzen wir voraus, dass ein bestimmter Angriff auf eine App von einem Sicherheitsexperten nachgestellt werden kann.

Die Grundidee unseres Ansatzes ist, dass bei der Demonstration eines Angriffs durch den Sicherheitsexperten alle notwendigen Informationen mit geringem Aufwand für die Analyse der Sicherheitslücken im Code aufgezeichnet werden. Dies erfolgt unter anderem mit Hilfe eines Videos, das durch den Sicherheitsexperten mit Hilfe einer Kopfkamera aufgenommen wird. Das Video zeichnet alle Aktivitäten auf, die auf der Oberfläche der App durchgeführt werden sowie die

Interaktion des mobilen Geräts mit der Umgebung. Außerdem werden ein Codetrace (Sequenz der ausgeführten Methoden im Programm) sowie notwendige Sensordaten bei der Demonstration im Hintergrund auf dem mobilen Gerät aufgezeichnet und mit dem Video synchronisiert. Nach der Demonstration erlaubt unser Werkzeug, die ausgeführten Programmteile (Codetraces) im Editor schrittweise mit dem Video nachzuvollziehen und so zu erkennen, wo sich eine Sicherheitslücke im Code befindet.

Im Vortrag werden die Probleme bei der Aufzeichnung von relevanten Informationen bei mobilen Geräten näher erläutert, die aufgrund von beschränkter Leistungs- und Speicherkapazität sowie kleinen Bildschirmen und unterschiedlicher Sensorik bestehen. Dazu werden passende Lösungen präsentiert.

Eine naheliegende Fortsetzung dieser Arbeiten besteht darin, die gewonnenen Erkenntnisse aus der Analyse von Sicherheitslücken einem breiteren Kreis von Entwicklern zu Gute kommen zu lassen. Über Demonstrationen und Schulungen basierend auf dem aufgezeichneten Informationen kann so ein organisationsweiter Lernprozess angestoßen werden.

Zielgruppe des Vortrags sind Sicherheitsexperten sowie Qualitätsbeauftragte und Entwickler mit einem Schwerpunkt auf Sicherheit, die in ihrer täglichen Arbeit mit Sicherheitslücken von Apps zu tun haben. Ihre Arbeit kann durch die vorgestellte Technik unterstützt werden. Des Weiteren möchten die Referenten durch die vorgestellte Lösung eine Diskussion über den Umgang mit Sicherheitslücken bei Apps anstoßen.

Biografie

Stefan Gärtner hat Informatik am Karlsruher Institut für Technologie (KIT) mit den Schwerpunkten Softwaretechnik und Robotik studiert. Von Mai 2009 bis Januar 2011 hat er dort im Humanoids and Intelligence Systems Lab gearbeitet. Seit Februar 2011 ist Stefan Gärtner wissenschaftlicher Mitarbeiter bei Prof. Dr. Kurt Schneider im Fachbereich Software Engineering an der Leibniz Universität Hannover. Seine Forschungsschwerpunkte liegen im Bereich der IT-Sicherheit, der statischen Codeanalyse und der Entwicklung von mobilen Anwendungen.
