

Michael Spreitzenbarth

Mobile Hacking

**Ein kompakter Einstieg ins
Penetration Testing mobiler Applikationen –
iOS, Android und Windows Mobile**



dpunkt.verlag

Michael Spreitzenbarth

Lektorat: René Schönfeldt

Lektoratsassistentz: Stefanie Weidner

Projektkoordination: Miriam Metsch

Copy-Editing: Ursula Zimpfer

Satz: Da-TeX, www.da-tex.com

Herstellung: Susanne Bröckelmann

Umschlaggestaltung: Helmut Kraus, www.exclam.de

Druck und Bindung: M.P. Media-Print Informationstechnologie GmbH, 33100 Paderborn

Bibliografische Information der Deutschen Nationalbibliothek

Die Deutsche Nationalbibliothek verzeichnet diese Publikation in der Deutschen Nationalbibliografie; detaillierte bibliografische Daten sind im Internet über <http://dnb.d-nb.de> abrufbar.

ISBN:

Print 978-3-86490-348-9

PDF 978-3-96088-124-7

ePub 978-3-96088-125-4

mobi 978-3-96088-126-1

1. Auflage 2017

Copyright © 2017 dpunkt.verlag GmbH

Wieblinger Weg 17

69123 Heidelberg

Die vorliegende Publikation ist urheberrechtlich geschützt. Alle Rechte vorbehalten. Die Verwendung der Texte und Abbildungen, auch auszugsweise, ist ohne die schriftliche Zustimmung des Verlags urheberrechtswidrig und daher strafbar. Dies gilt insbesondere für die Vervielfältigung, Übersetzung oder die Verwendung in elektronischen Systemen.

Es wird darauf hingewiesen, dass die im Buch verwendeten Soft- und Hardware-Bezeichnungen sowie Markennamen und Produktbezeichnungen der jeweiligen Firmen im Allgemeinen warenzeichen-, marken- oder patentrechtlichem Schutz unterliegen.

Alle Angaben und Programme in diesem Buch wurden mit größter Sorgfalt kontrolliert. Weder Autor noch -Verlag können jedoch für Schäden haftbar gemacht werden, die in Zusammenhang mit der Verwendung dieses Buches stehen.

5 4 3 2 1 0

Vorwort

Der Marktanteil von Smartphones und Tablets wächst signifikant im Gegensatz zu herkömmlichen PCs und hält auch in immer mehr Unternehmen Einzug. Diese Geräte haben einen enormen Funktionsumfang und werden schon lange nicht mehr nur zum Telefonieren verwendet. Dies bietet jedoch nicht nur neue Möglichkeiten für den Einzelnen sowie viele Firmen, sondern birgt auch ein hohes Maß an Gefahren und Risiken in sich.

Wenn Sie sich schon immer gefragt haben, was die Applikationen auf Ihrem Smartphone so alles im Hintergrund machen und ob die verarbeiteten Daten auch wirklich sicher abgelegt und übertragen werden, dann ist dieses Buch genau das Richtige für Sie!

Im Rahmen des Buches wird Ihnen anhand von ausführlichen Beispielen gezeigt, warum es sinnvoll für Unternehmen – aber auch für Privatpersonen mit einem Bewusstsein für das Schützenswerte – ist, nicht auf die Versprechen der Hersteller mobiler Apps zu hören, sondern selbst zu prüfen, ob Applikationen den eigenen Ansprüchen und Vorgaben entsprechen. Sie erfahren, welche Open-Source-Tools es auf dem Markt gibt und wofür man sie einsetzen kann. Dabei ist immer zu bedenken, dass dies nur eine Auswahl an Tools ist und keinesfalls den Anspruch auf Vollständigkeit erheben soll. Nach der Analyse einiger Apps hat jeder Analyst seine eigene Sammlung an Werkzeugen und Vorgehensweisen, auf die er bei der täglichen Arbeit zurückgreift.

Dabei stehen unter anderem folgende Fragestellungen im Vordergrund:

- Was sind die wichtigsten Komponenten der einzelnen mobilen Betriebssysteme?
- Wie können Sie prüfen, ob Daten einer App auch bei Verlust bzw. Diebstahl eines mobilen Endgerätes weiterhin geschützt sind?
- Wie können Sie feststellen, ob Daten bei der Übertragung ausreichend geschützt sind?
- Welche Schwachstellen sind für Angreifer besonders interessant?

Dieses Buch kann man als Leser auf verschiedene Weisen angehen, die in Abbildung 1 aufgezeigt sind. Hierbei werden in den ersten beiden Kapiteln die Grundlagen geschaffen, um einem Leser, der bisher keine Erfahrungen mit mobilen Be-

triebssystemen oder dem Reversing gesammelt hat, den Einstieg zu ermöglichen. Danach gibt es immer einen »Doppelpack« an Kapiteln, der sich mit der statischen Analyse von Apps einer bestimmten Plattform befasst und sich der anschließenden Suche nach Sicherheitsproblemen widmet. Dies alles wird wieder in Kapitel 9 zusammengeführt, das die Analyse der Datenübertragung als Schwerpunkt hat, die auf allen Systemen nahezu identisch abläuft und deshalb an dieser Stelle auch übergreifend zusammengefasst ist. Den Schluss des Buches bildet ein kurzes Kapitel, das dem Leser Hinweise zu Übungen gibt, die er nun selbst in Angriff nehmen kann, und weitere Werkzeuge und vertiefenden Lesestoff vorschlägt.

Dr. Michael Spreitzenbarth

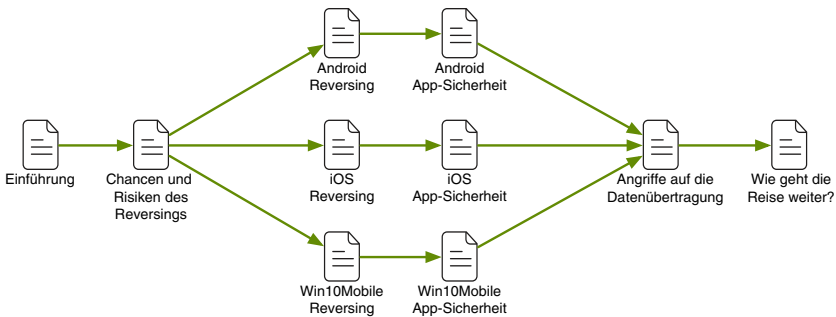


Abb. 1: Mögliche Wege für den Leser durch dieses Buch

Danksagung

Dieses Buchprojekt wäre ohne die Unterstützung anderer nur schwer umsetzbar gewesen. Aus diesem Grund möchte ich einigen dieser Personen auf diesem Wege meinen Dank aussprechen.

Zuerst möchte ich Andreas Kurtz und Siegfried Rasthofer danken, die mir sehr guten Input für dieses Buch gegeben und auf einige hilfreiche Tools und Beispiele aufmerksam gemacht haben.

Ebenso möchte ich aber auch den vielen Autoren und Entwicklern aus der Open-Source-Community danken, die zahllose Stunden in die Verbesserung und Entwicklung neuer Werkzeuge gesteckt haben. Ohne diese Arbeit wären wir heute nicht in der Lage, solche Assessments durchführen zu können.

Mein Dank geht ebenso an den dpunkt.verlag und die anonymen Reviewer sowie an Marko Rogge, die mich gerade in der Schlussphase auf wichtige Verbesserungen am Buch aufmerksam gemacht haben.

Besonderer Dank geht an meine Lebensgefährtin, die mich immer wieder motiviert und unterstützt hat, auch wenn es Zeiten gab, in denen durch dieses Buch und die tägliche Arbeit nahezu keine Freizeit mehr blieb.

Inhaltsverzeichnis

1	Einführung in mobile Betriebssysteme und deren Applikationen ...	1
1.1	Android	2
1.2	Apple iOS	8
1.3	Windows 10 Mobile	18
1.4	Chancen und Risiken von mobilen Applikationen	24
1.5	OWASP Mobile Top 10	27
1.6	Eine Laborumgebung erstellen	31
1.7	Zusammenfassung und Ausblick	37
2	Chancen und Risiken des Reversings	39
2.1	Statische Analyse (Reversing)	39
2.2	Dynamische Analyse	40
2.3	Vergleich der beiden Techniken	40
2.4	Schlussfolgerung	41
3	Reversing von Android-Applikationen	43
3.1	Vorgehensweisen beim Reversing von Android-Applikationen	43
3.2	Beschaffen der zu untersuchenden Applikation	44
3.3	Analysieren des Android-Manifests und Entpacken der Applikation	45
3.4	Werkzeuge zum Analysieren der Applikationen	47
3.5	Zusammenfassung	64
4	Sicherheitsprobleme bei Android-Applikationen	67
4.1	Wichtige Tools und Helfer	67
4.2	Analyse der Zugriffe auf sensible Nutzerdaten	76
4.3	Exportierte Activities erkennen und ausnutzen	83
4.4	Exportierte Content Provider und SQL-Injections erkennen und ausnutzen	86
4.5	Schwachstellen des JavascriptInterface erkennen und ausnutzen	91
4.6	Ungewollten Datenabfluss durch Verwendung der Backup-Funktion erkennen	94
4.7	Spurensuche im Dateisystem	95
4.8	Android-Applikationen zur Laufzeit manipulieren	110
4.9	Zusammenfassung	113

5	Reversing von iOS-Applikationen	115
5.1	Vorgehensweisen beim Reversing von iOS-Applikationen	115
5.2	Wichtige Tools und Helfer	115
5.3	Beschaffen der zu untersuchenden Applikation	124
5.4	Werkzeuge zum Analysieren der Applikationen	127
5.5	Zusammenfassung	135
6	Sicherheitsprobleme bei iOS-Applikationen	137
6.1	Wichtige Tools und Helfer	137
6.2	Analyse der Zugriffe auf sensible Nutzerdaten	146
6.3	iOS-Applikationen zur Laufzeit manipulieren	149
6.4	Spurensuche im Dateisystem	159
6.5	Fehlende systemeigene Sicherheitsfunktionen in iOS-Applikationen erkennen	171
6.6	Zusammenfassung	178
7	Reversing von Windows-10-Mobile-Applikationen	179
7.1	Aufbau der Windows-10-Mobile-Applikationen	179
7.2	Vorgehensweisen beim Reversing von Windows-10-Mobile-Applikationen	182
7.3	Werkzeuge zum Analysieren der Applikationen	183
7.4	Zusammenfassung	186
8	Sicherheitsprobleme bei Windows-10-Mobile-Applikationen	187
8.1	Analyse der Zugriffe auf sensible Nutzerdaten	187
8.2	Spurensuche im Dateisystem	189
8.3	Fehlende Sicherheitsfunktionen in Windows-10-Mobile-Applikationen erkennen	193
8.4	Weitere Angriffsvektoren erkennen	196
8.5	Zusammenfassung	197
9	Angriffe auf die Datenübertragung	199
9.1	Schutz der übermittelten Daten auf dem Transportweg	199
9.2	Man-in-the-Middle-Angriffe	200
9.3	SSL-Strip-Angriffe	209
9.4	Anwendungsbeispiele und Auswertung	210
9.5	Zusammenfassung	213
10	Wie geht die Reise weiter?	215
10.1	Weitere Tools	215
10.2	Wo kann ich üben?	217
10.3	Wo finde ich weiterführende Informationen?	218

Literaturverzeichnis 219

Index 221