

APP-SECURITY IN IOS UND ANDROID

Seminararbeit

0.1

Hochschule für angewandte Wissenschaften
Würzburg-Schweinfurt

David Artmann
Kristoffer Schneider

20. Mai 2015

Inhaltsverzeichnis

1	Vorwort	4
2	Das Android Betriebssystem	5
3	Apple's Law Enforcement Process Guidelines	6
4	Sicherheitsarchitektur iOS	7
4.1	Historisches	7
5	Geheime Dienste	8
5.1	lockdownd - remote access	8

Abbildungsverzeichnis

1	Die Architektur von Android ASI-P-2	5
---	---	---

1 Vorwort

Die aus Cupertino in Kalifornien stammende US-Amerikanische Apple Corporation ist eine der größten Firmen der Welt und hatte einen Umsatz von 182 Mrd. USD im Geschäftsjahr 2014. Sie ist ebenfalls der Erfinder des mobilen Betriebssystems iOS, welches auf den firmeneigenen Geräten iPad, iPad mini, iPhone, iPod touch und dem Apple TV ab der zweiten Generation zum Einsatz kommt. Der Kern des Betriebssystems basiert auf dem freien UNIX Betriebssystem Darwin, das auch als Vorlage für das Betriebssystem OS X genutzt wurde.

Im Februar 2015 hatte iOS in den USA einen Marktanteil von 38,8% und 17,4% in Deutschland.¹ Es existieren mehr als einhundert Millionen iPhones auf der ganzen Welt. Das Smartphone ob iOS, Android oder Windows Phone als Betriebssystem, ist in unserer heutigen Welt nicht mehr wegzudenken und mehrere Studien haben offen gelegt, dass das Smartphone den Computer bzw. Laptop - zumindest bei der Generation unter 18 Jahren - schlägt.^{2 3}

Welche Auswirkung hätte es, wenn Sicherheitslücken auf diesen zu finden wären, oder schlimmer noch, diese völlig ohne das Wissen des Nutzers ausgenutzt werden könnten? Mit dieser Arbeit möchte ich besonders auf Sicherheitstechnische Problematiken dieses Betriebssystems eingehen und zeigen, dass ein Proprietäres Betriebssystem viele Vorteile hat, aber ebenso auch Nachteile besitzt die es nicht zu verachten gilt. Ebenso werde ich versuchen mit praktischen Beispielen zu zeigen, dass iOS - obwohl proprietär - dennoch angreifbar ist und Lücken aufweist.

¹<http://www.kantarworldpanel.com/global/smartphone-os-market-share/>

²http://www.bitkom.org/files/documents/BITKOM_PK_Kinder_und_Jugend_3_0.pdf

³<http://www.mpfs.de/fileadmin/JIM-pdf13/JIMStudie2013.pdf>

2 Das Android Betriebssystem

Das Unternehmen Android wurde 2003 von Andy Rubin gegründet und wurde 2005 von Google aufgekauft. Seitdem kümmert sich Google und das Android Open Source Project (AOSP) um die Weiterentwicklung des Systems. Aktuell ist Android, mit 55.6% Marktanteil⁴, das vorherrschende Betriebssystem für mobile Endgeräte in den USA.

Basis für das Betriebssystem ist ein modifizierter Linux-Kernel und eine Java Virtual Machine (JVM). Bis einschließlich Version 4.4 wurde hierfür die Dalvik Runtime und für alle neueren Versionen die Android Runtime (ART) verwendet. Jede App läuft in einer eigenen Instanz der entsprechenden Runtime und damit in einer Sandbox.

Oberhalb der JVM sind die meisten Komponenten in Java implementiert.

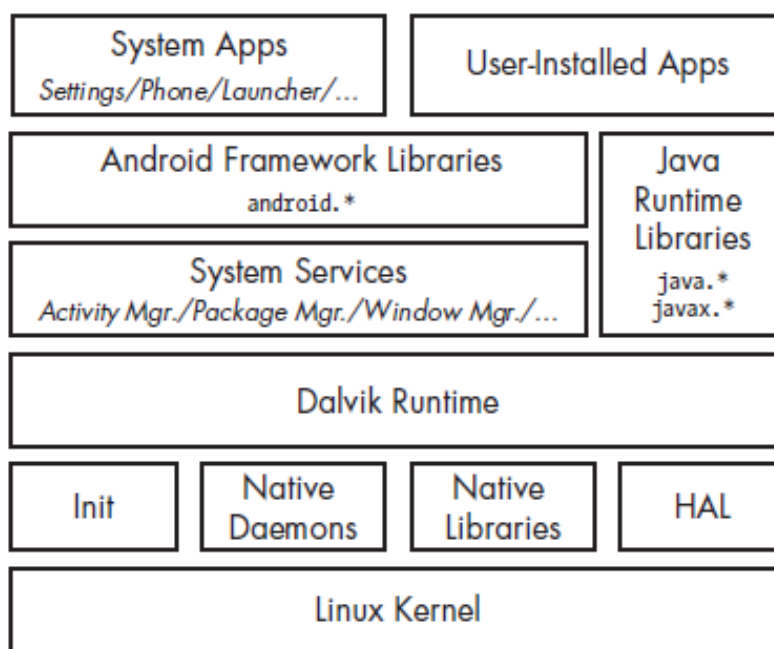


Abbildung 1: Die Architektur von Android ASI-P-2

⁴Kantar Worldpanel: Smartphone OS sales market share, <http://www.kantarworldpanel.com/global/smartphone-os-market-share/>, 17.5.2015

3 Apple's Law Enforcement Process Guidelines

Die Firma Apple schreibt auf ihrer Webseite:

Our commitment to customer privacy doesn't stop because of a government information request.

Weiterhin wird beteuert:

In addition, Apple has never worked with any government agency from any country to create a back door in any of our products or services.

Apple beteuert hier, seine Verpflichtung zur Einhaltung der Privatsphäre des Kunden auch nicht einzustellen, wenn die Regierung um Auskunft genau dieser Daten bittet. Zusätzlich wird versichert, dass Apple niemals mit Regierungsbehörden jedweder Länder gearbeitet hat, um Trojaner in eines ihrer Produkte oder Dienstleistungen einzubauen.

Eine Einhaltung dieser Richtlinien ist von Kundenseite natürlich gewünscht. Ob Apple hier wirklich Wort hält, werde ich auf den kommenden Seiten genauer beleuchten.

4 Sicherheitsarchitektur iOS

Sicherheitsarchitektur...

4.1 Historisches

Historisches...

5 Geheime Dienste

Apple kann SMS, Fotos, Videos, Kontakte, Musik, Aufnahmen und Anruferhistorie aus passcode geschützten Geräten auslesen. Möglich machen dies nicht dokumentierte Dienste, welche auf jedem Gerät mit iOS installiert sind. In diesem Kapitel will ich auf diese Dienste eingehen und deren genauen Einsatzzweck erläutern.

5.1 *lockdownd* - remote access

Der Dienst *lockdownd* ermöglicht den Zugriff auf ein iOS Gerät per TCP oder USB-Anschluss auf Port 62078.