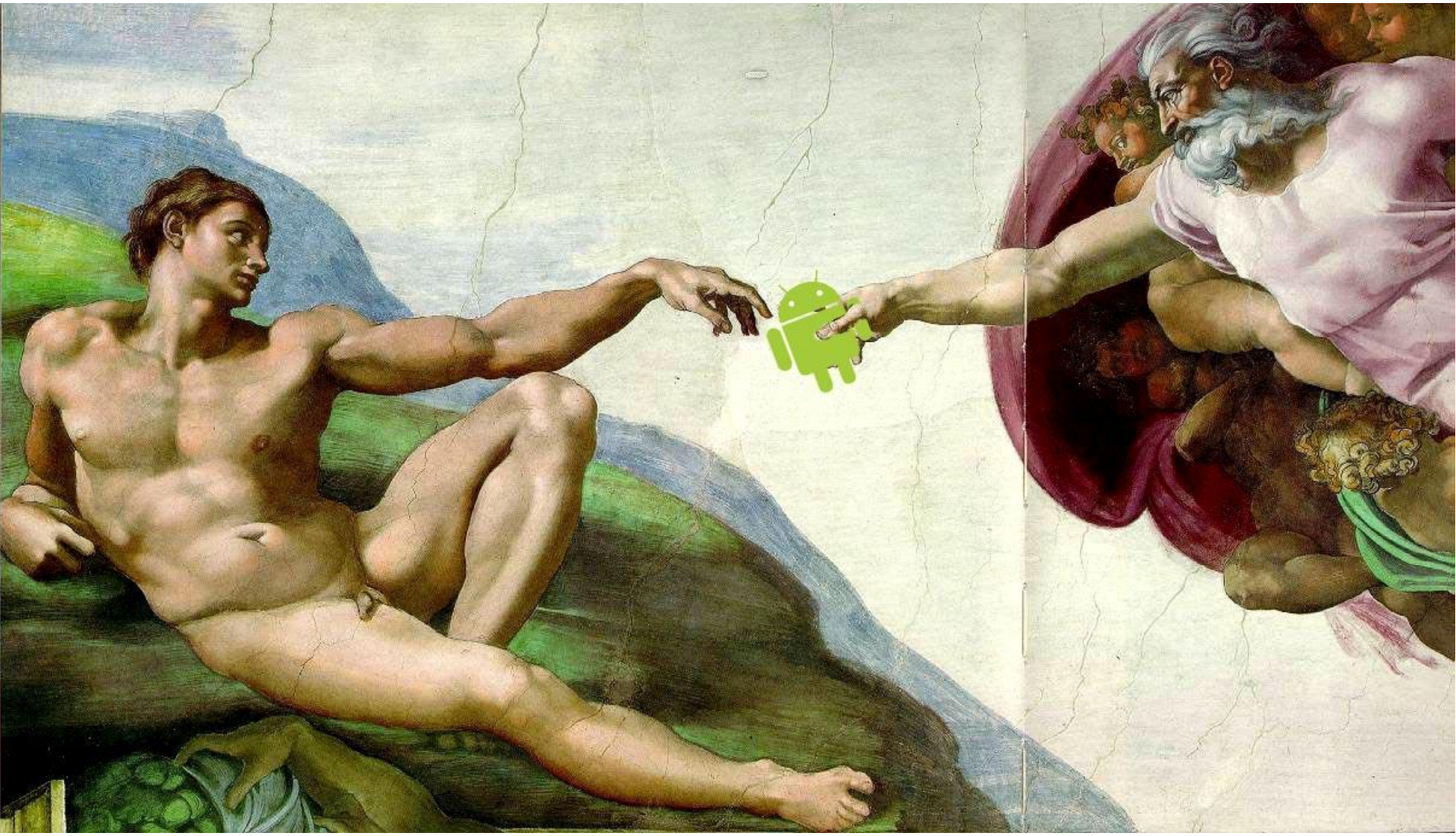


Android from a SIB/SIM Perspective

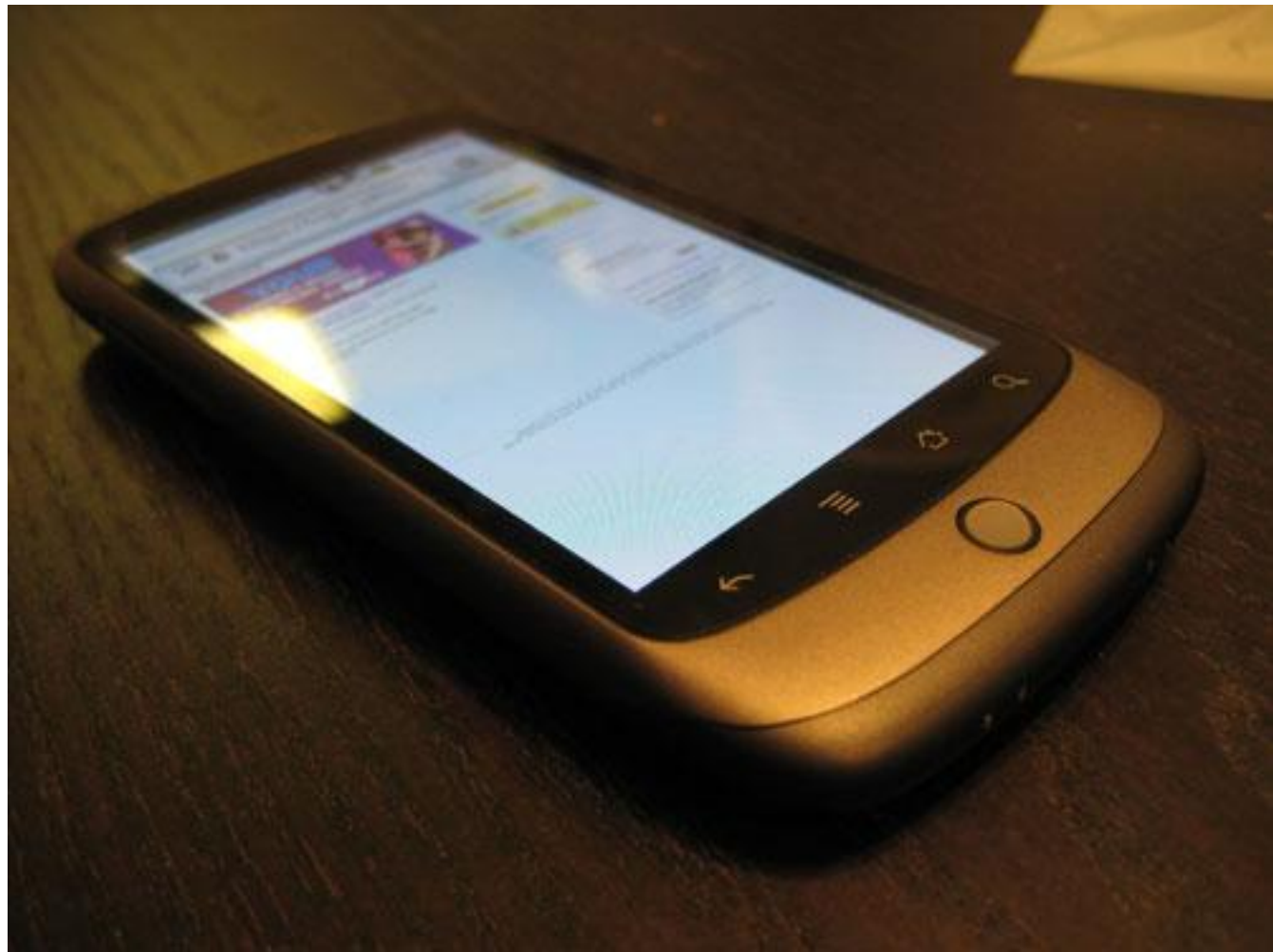
HackingNight 2010.5

Android from a *SIB/SIM* Perspective





Screen Lock/Pattern **Unlock**



Screen Lock/Pattern **Unlock**



Screen Lock/Pattern **Unlock**

“...we determined that **68 percent** of password **smudge patterns** are **fully detectable**, and **92 percent** are **partially detectable**.”

Studie „Smudge Attacks on Smartphone Touch Screens“,
Pennsylvania August 2010

Was kann passieren,
wenn ich mein Smartphone
unbeaufsichtigt lasse?

Probleme beim Zugriff auf dein Konto?

Du hast dein Passwort vergessen? Gib deine E-Mail-Adresse oder deine Handynummer unten ein und vervollständige die Sicherheitskontrolle. Wenn du deine E-Mail-Adresse eingibst, senden wir dir eine E-Mail mit dem Link zum Zurücksetzen deines Passworts. Wenn du deine Handynummer eingibst, senden wir dir eine SMS mit dem Link zum Zurücksetzen deines Passworts. Wenn du deine Handynummer nicht bestätigt hast, kannst du sie zum Zurücksetzen deines Passworts nicht verwenden.

Du hast bereits einen Bestätigungscode?

E-Mail oder Handy:

Weiter

Falls du ein anderes Problem bei der Anmeldung für dein Konto hast, besuche bitte unsere [Hilfeseite für Anmeldeprobleme](#).



ANDROID

market



Android Market Security?

Android Market Security??

Community ist
selbst verantwortlich!

Geschätzte Anzahl an Android Apps die **NICHT** in
den Market kommen?

ca. **1 %**

Android Market App Requirements:

1. Application must be signed
(validity period ends after 22 October 2033)
2. Application must define `android:versionCode`,
`android:versionName` in its manifest
3. Application must define both an `android:icon` and an
`android:label` attribute in the manifest.

Quelle: <http://developer.android.com/guide/publishing/publishing.html>

Android Market Responsibility:

Terms of Service:

"You agree that Google is not responsible for any Product on the Market that originates from a source other than Google"

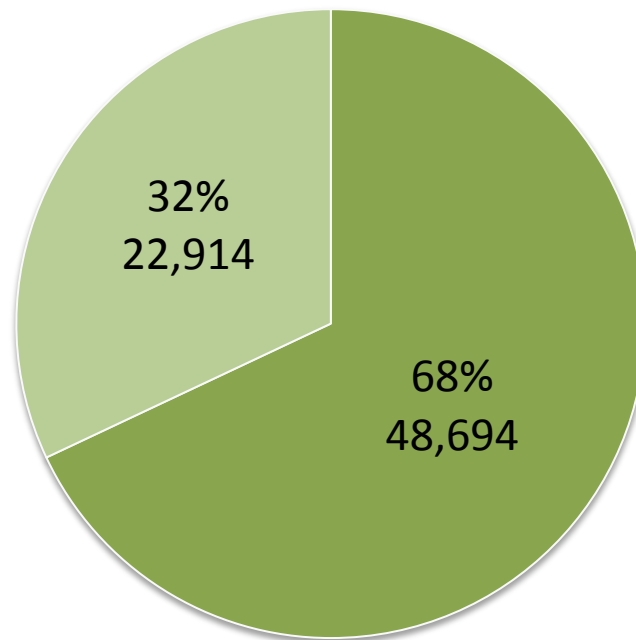
Android Market Studie:

Android Market Threat Analysis

(von SMobile Systems)

Android Market Studie:

Apps Metadaten Aquirierung



Android Market Studie:

Permission Übersicht

Permission Name	# of Apps Requesting the Permission
ACCESS_COARSE_LOCATION	12,062
ACCESS_FINE_LOCATION	7,533
BRICK	9
CALL_PHONE	2,670
CALL_PRIVILEGED	103
GET_ACCOUNTS	312
INTERNET	34,636
PROCESS_OUTGOING_CALLS	274
READ_CALENDAR	500
READ_CONTACTS	4,203
READ_OWNER_DATA	200
READ_SMS	849
RECEIVE_MMS	107
RECEIVE_SMS	1,172
RECORD_AUDIO	876

Android Market Studie:

Permission Übersicht II

# Applications	# Permissions
20,786	2
5,783	3
2,708	4
826	5
435	6
147	7
97	8
27	9
39	10
10	11

Android Market Studie:

Permission Übersicht II

# Applications	# Permissions
20,786	2
5,783	3
2,708	4
826	5
435	6
147	7
97	8
27	9
39	10
10	11

Android Market **Security Evidence:**

FILED UNDER [Cellphones](#), [Mobile Software](#)

Phishing Android apps explain our maxed-out credit cards

By Chris Ziegler  posted Jan 11th 2010 2:07PM



There's no such thing as a perfect mobile app store strategy -- you're either too [draconian](#), too arbitrary, or too loose in your policies, and as far as we can tell, there's no way to find a balance that isn't going to trigger an alarm here and there or get a few people worked into a lather. If you're too loose, for instance, you're liable end up with the occasional bout of malware, which is exactly what appears to have gone down recently in the [Android Market](#) with a few fake banking apps published by a bandit going as "Droido9." As you might imagine, the apps end up doing little more than stealing your information

Android Market **Security Evidence:**

FILED UNDER *Cellphones, Mobile Software*

Phishing Android apps explain our maxed-out credit cards

By C "We recently learned that a fraudster developed a **rogue Android Smartphone app**," the bank warned, "It creates a **shell of mobile banking apps** that tries to **gain access** to a **consumer's financial information**. Droid09 launched this **phishing attack** from the **Android Marketplace** and it's since been removed."



SAM SPRETT - GETTY IMAGES

Zustand des Android Markets?

Android OS Security

Linux 2.6 + Java = Secure

... right?

APPLICATIONS

Home

Contacts

Phone

Browser

...

APPLICATION FRAMEWORK

Activity Manager

Window Manager

Content Providers

View System

Package Manager

Telephony Manager

Resource Manager

Location Manager

Notification Manager

LIBRARIES

Surface Manager

Media Framework

SQLite

OpenGL | ES

FreeType

WebKit

SGL

SSL

libc

ANDROID RUNTIME

Core Libraries

Dalvik Virtual Machine

LINUX KERNEL

Display Driver

Camera Driver

Flash Memory Driver

Binder (IPC) Driver

Keypad Driver

WiFi Driver

Audio Drivers

Power Management

National Cyber-Alert System

Vulnerability Summary for CVE-2010-1807

Original release date: 09/10/2010

Last revised: 11/11/2010

Source: US-CERT/NIST

Overview

WebKit in Apple Safari 4.x before 4.1.2 and 5.x before 5.0.2, and Android before 2.2, does not properly validate floating-point data, which allows remote attackers to execute arbitrary code or cause a denial of service (application crash) via a crafted HTML document.

Impact

CVSS Severity (version 2.0):

CVSS v2 Base Score: 9.3 (HIGH) (AV:N/AC:M/Au:N/C:C/I:C/A:C) (legend)

Impact Subscore: 10.0

Exploitability Subscore: 8.6


CVSS Version 2 Metrics:

Access Vector: Network exploitable; Victim must voluntarily interact with attack mechanism

Access Complexity: Medium

Authentication: Not required to exploit

Impact Type: Allows unauthorized disclosure of information; Allows unauthorized modification; Allows disruption of service

[E-mail](#) | [Print](#) | [Permalink](#) | [LinkedIn](#) | 

[facebook](#) [twitter](#) 

Fake Angry Birds App Exposes Android Vulnerability

Flaw bypasses a security control, allowing an application to silently download and grant complete access rights to additional apps.

By [Mathew J. Schwartz](#), [InformationWeek](#)
November 15, 2010 12:18 PM

Angry Birds may be a top-selling game for all smartphone platforms, but don't mistake it for the unauthorized Angry Birds Bonus Levels app released by security researcher Jon Oberheide, CTO at Scio Security.



Fake Angry Birds App Exposes Android

Vul

Flaw b
access

By Math
Novem

Angry B
don't m
release

This vulnerability would make it possible for one application to **download and launch additional applications** from the [Android] Marketplace.

To demonstrate this, Jon had also **uploaded several other applications** to Marketplace: **Fake Contact Stealer, Fake Location Tracker, and Fake Toll Fraud**. These would be launched by the Angry Birds **trojan**.

88 'high-risk' security defects found in Android kernel

By Ryan Naraine | November 2, 2010, 12:12pm PDT

Summary

The high-risk defects in the Android kernel included memory corruption flaws, memory illegal accesses and resource leaks.



Topics

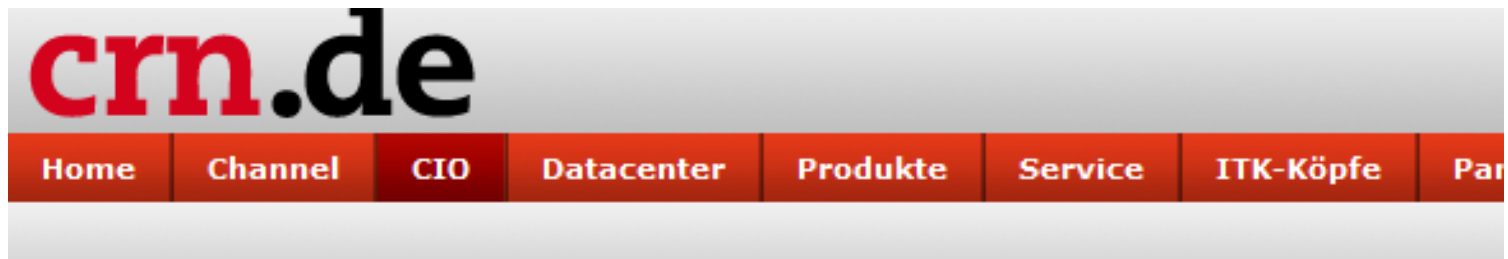
[Software](#), [Defect](#), [Kernel](#), [HTC Droid Incredible](#), [Android](#), [Ryan Naraine](#)

A security audit of the Android kernel has turned up 88 “high-risk defects” with significant potential to cause security vulnerabilities, data loss, or quality problems such as system crashes.

According to Coverity, a source code analysis firm, the high-risk defects included memory corruption flaws, memory illegal accesses and resource leaks.

Blogger Info

Android Rootkit



Home » CIO

Noch nicht in freier Wildbahn gesehen

Rootkit für Android entwickelt

von *Werner Veith, Mathew J. Schwartz*

07.06.2010



In einer Art Machbarkeitsstudie haben zwei Sicherheitsforscher bei Trustwave ein Rootkit für Android entwickelt. Im Gegensatz zu Windows ist eine Rootkit-Suche schwieriger. Nun geht es darum, Abwehrstrategien zu entwickeln.

Android hat eine wachsende Popularität bei Smartphones. Auch bei den Tablet-Rechnern ist es im Rennen. Nun zeigt sich, dass Android durch Rootkits verwundbar ist. Erklärt haben das die zwei Forscher Nicholas Percoco und Christian Papathanasiou von

Android Rootkit

crn.de

Home

Channel

CIO

Datacenter

Produkte

Service

ITK-Köpfe

Par

Hor

Nov

Ro

vor

07.

In

Ro

sch

And

ist es im Kennen. Nun zeigt sich, dass Android durch Rootkits verwundbar ist. Erklärt

haben das die zwei Forscher Nicholas Percoco und Christian Papathanasiou von

Wir haben ein **Android-Rootkit** auf **Kernel-Ebene** entwickelt. Es kommt in Form eines **nachladbaren Kernel-Moduls**«. **Läuft** das **Rootkit einmal** auf einem Smartphone mit dem auf Linux basierenden Android, bekommt der **Hacker** sehr **einfach** die **Kontrolle**: **Jemand ruft** eine »**Trigger Nummer**« auf und bekommt über TCP den **vollen Zugriff als Root** auf dem Gerät

Android OS Security

*Actually better than
„industry standard“*

“The Android kernel used in the HTC Droid Incredible has about half the defects that would be expected for similar software of the same size.”

“Accountability for Android software integrity is fragmented. The problem is no different with Android than what we see across open source.”

Danke Für eure Aufmerksamkeit