

Hey, What's Your App is Doing on my Phone?



Shay Zalalichin | CTO, Comsec Global

Agenda

Quick Intro

The Challenge

Android Security

Mitigations

Fun Stuff (if time allows 😊)

Quick Intro

The Most Useful App

Armin Heinrich



I Am Rich

Category: Lifestyle

Released Aug 05, 2008

Seller: Armin Heinrich

© 2008 Armin Heinrich


Version: 1.0

0.1 MB

\$999.99

BUY APP

Now on Android Market

 **Android Market**


Android Market › Social › I'm Rich!! (Blue Diamond)

I'm Rich!! (Blue Diamond)

★★★★★ (8)

INSTALL

钻石是爱情和忠贞的象征 蓝钻 价值¥8.



OVERVIEW

USER REVIEWS

WHAT'S NEW

PERMISSIONS

ABOUT THIS APP

RATING:
★★★★★
(8)


UPDATED:
August 15, 2011

CURRENT VERSION:
1.3.7

REQUIRES ANDROID:
1.6 and up


CATEGORY:
Social

INSTALLS:
1,000 - 5,000




last 30 days

Permissions? Anyone?


★★★★★ (8)
INSTALL

OVERVIEW | **USER REVIEWS** | **WHAT'S NEW** | **PERMISSIONS**


More from developer




I'm Rich!! (Pink Diamond)
★★★★★
No ratings
₹47.72



I'm Rich!! (White Diamond)
★★★★★
No ratings
₹477.22




I'm Rich!! (Black Diamond)
★★★★★
No ratings
₹715.84



★★★★★
★★★★★ (10)
Free

Users who viewed this also viewed



Panava Diamond

Permissions

THIS APPLICATION HAS ACCESS TO THE FOLLOWING:

NETWORK COMMUNICATION
FULL INTERNET ACCESS
Allows an application to create network sockets.

YOUR PERSONAL INFORMATION
READ SENSITIVE LOG DATA
Allows an application to read from the system's various log files. This allows it to discover general information about what you are doing with the device, potentially including personal or private information.

PHONE CALLS
READ PHONE STATE AND IDENTITY
Allows the application to access the phone features of the device. An application with this permission can determine the phone number and serial number of this phone, whether a call is active, the number that call is connected to and the like.

STORAGE
MODIFY/DELETE USB STORAGE CONTENTS **MODIFY/DELETE SD CARD CONTENTS**
Allows an application to write to the USB storage. Allows an application to write to the SD card.

technologyטכנולוגיה

[סלולר וניידים](#) • [טכנופובי](#) • [הלוח](#) • [כזה אני רוצה](#) • [אפליקציות לסלולרי](#)

חדש: אפליקציה שלא עושה כלום

אם תשלמו למתכנת ישראלי 99 סנט, תקבלו אפליקציה לאנדרואיד שמבטיחה לא לעשות דבר - ולראשונה בשוק התוכנה המקומי, עומדת בכל הציפיות

עידו קיין

פורסם: 08:42, 26.06.11



[>> עתיד הצילום עומד להשתנות. שוב](#)

999.99 דולר עלתה אפליקציית האיפון "I Am Rich" שפיתח ארמין היינריך, הסכום המירבי שאפשר לגבות עבור אפליקציה בחנות של אפל. אי אפשר להגיד שהיא לא עשתה כלום: משהופעלה היא הציגה אבן חן בוהקת. אפשר להסתכל עליה כסמל סטטוס וירטואלי, עדות לכך שבעליה הוא אדם אמיד, שיכול להרשות לעצמו לזרוק אלף דולר רק כדי להפגין את עושרו וטעמו הרע. אפשר גם לשפוט אותה כיצירת אמנות - שהרי גם יצירות אמנות, לצד הערך התרבותי שלהן, משמשות להפגנת עושר ומעמדו של הרוכש. שמונה אייפונים ברי מזל קנו את אפליקציית העושר מאז השקתה באמצע 2007 ועד [שאפל הסיירה אותה](#) מחנות האפליקציות שלה בסוף 2008, אולי בגלל תלונה שהופצה באינטרנט, של משתמש שטוען שרכש אותה בטעות כי חשב שמדובר בבדיחה.

גם [Nothing](#), אפליקציית האנדרואיד החדשה, לא עושה דבר. אבל היא לא עושה זאת תמורת סכום קטן בהרבה: 99 סנט. "כמה פעמים שילמתם שום דבר וקיבלתם משהו בתמורה? עכשיו אנחנו מציעים לכם הזדמנות יחודית: שלמו משהו וקבלו שום דבר בתמורה!", נכתב בעמוד האפליקציה. "האפליקציה הזאת עושה פשוט שום דבר. ברכישתה תסייעו לנו להוכיח ששום דבר אכן שווה משהו!"

ם לפייסבוק שלכם



Arielle



Osama

מחלקת הכלום

Nothing

Lets Start

Evolution in the Mobile Area



The New Mobile



Capabilities and Assets

נכסי המידע	קישוריות	פונקציונאליות
<ul style="list-style-type: none"> • מספרי טלפון • שמות אנשי קשר • תכתובות של הודעות קצרות • פרטים של אנשי קשר • קבצי מדיה (תמונות, סרטונים וכו') • מיילים • נתוני מיקום • מסמכים / קבצים אישיים • זהות בגישה למערכות נוספות • מידע עסקי 	<ul style="list-style-type: none"> • מקשי חיוג • תפריטים חכמים • מסך מגע • ... • IrDA • Bluetooth • ... • HS Internet • ... • GPS • USB • Wifi 	<ul style="list-style-type: none"> • שיחות קוליות • הודעות קצרות • ... • שיחות וידאו • מיילים • משחקים • גלישה • ניווט • צילום • ... • יישומים • יישומים עסקיים • ...

Find the Differences



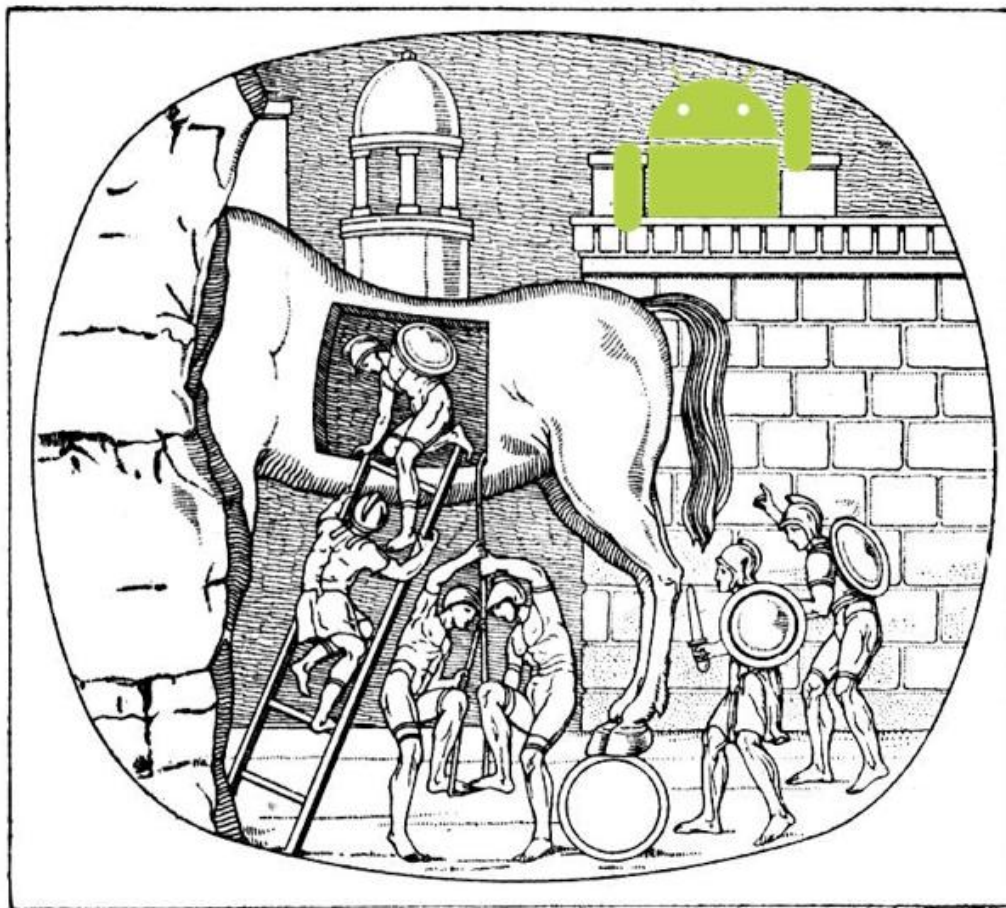
Users are Changing



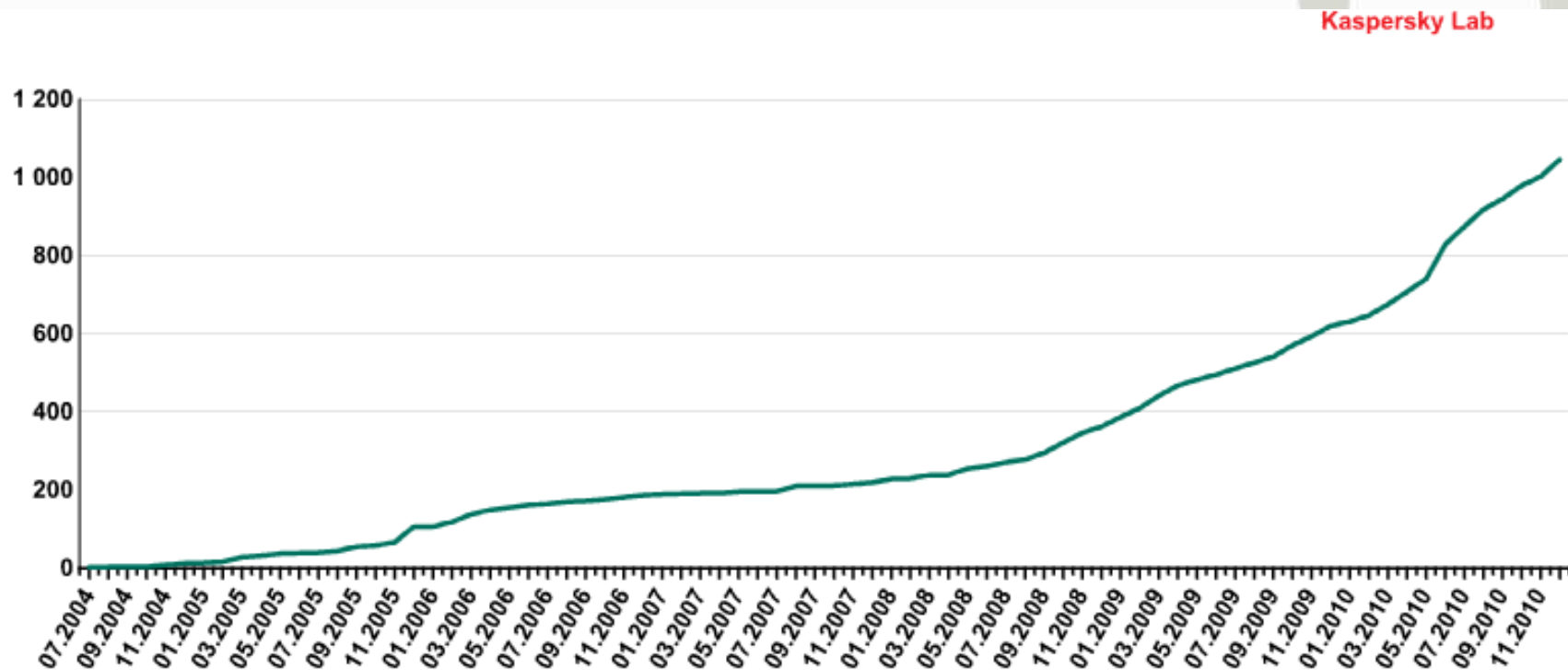
Everything is on the Cloud



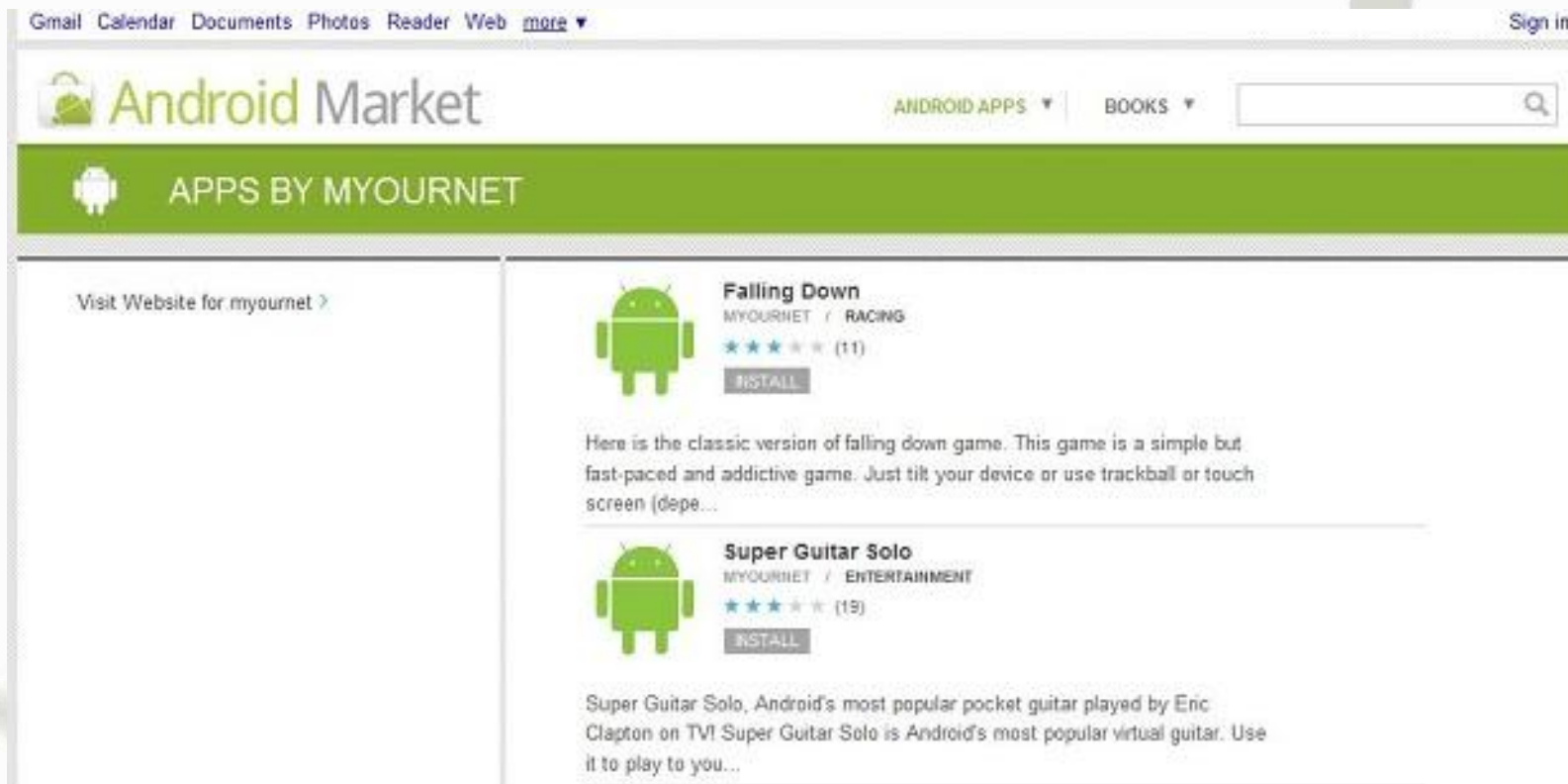
Mobile Malware Evolution



Mobile Malware Evolution



Malware from the Market



Android Security

Android Architecture



Android Security Model

Based on Linux + Android Extensions

Applications Isolation

Each App gets its own UID

Does not use the Java Security Model

Android Permissions

Permissions are Granted at Installation (or Updates)

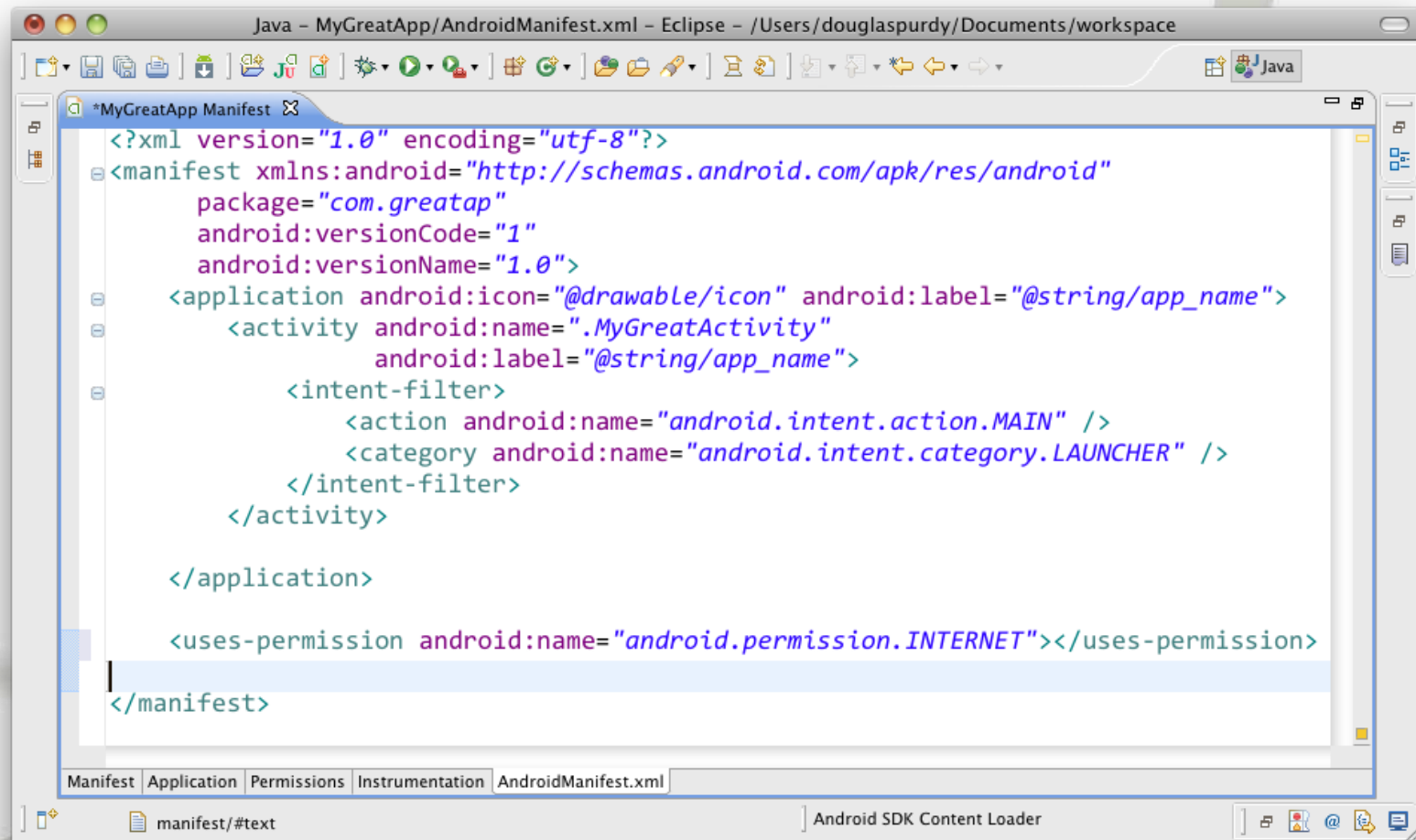
Basic Permissions are based on Linux (Files, Network, BT etc)

Dalvik Java Permissions are not Used

Permissions are Descriptive Strings with Business/Logic Meaning

Enforced by Activity Manager

Android Manifest.xml



The screenshot shows the Eclipse IDE interface with the 'MyGreatApp Manifest' file open. The code is as follows:

```
<?xml version="1.0" encoding="utf-8"?>
<manifest xmlns:android="http://schemas.android.com/apk/res/android"
    package="com.greatap"
    android:versionCode="1"
    android:versionName="1.0">
    <application android:icon="@drawable/icon" android:label="@string/app_name">
        <activity android:name=".MyGreatActivity"
            android:label="@string/app_name">
            <intent-filter>
                <action android:name="android.intent.action.MAIN" />
                <category android:name="android.intent.category.LAUNCHER" />
            </intent-filter>
        </activity>
    </application>
    <uses-permission android:name="android.permission.INTERNET"></uses-permission>
</manifest>
```

The IDE window title is 'Java - MyGreatApp/AndroidManifest.xml - Eclipse - /Users/douglaspurdy/Documents/workspace'. The bottom status bar shows 'manifest/#text' and 'Android SDK Content Loader'.

Android Permissions (Cont.)

Internet (Network Access)

Contacts

SMS/MMS

Location

Get Phone Details

Phone Calls

Browser History Access

Hardware Access

Various Administrative Functions

Android Key Components

Activities (Screens / GUI)

Services (for background work)

Broadcast Receivers (notifications)

Content Providers (for sharing relational data)

Android Intents

Android's way of doing IPC

Component Communication

Component / App Decoupling

Inter/Intra App Communication

Explicit vs. Implicit Intents

Android Specific Challenges

Intent Sniffing

Intent Spoofing / Injection

Intent MITM

Insecure Storage

SQL Injection

Little Documentation

Overprivileges

Rooting

Open Platform (!?!)

Mitigations

Process Failures



How the customer explained it



How the Project Leader understood it



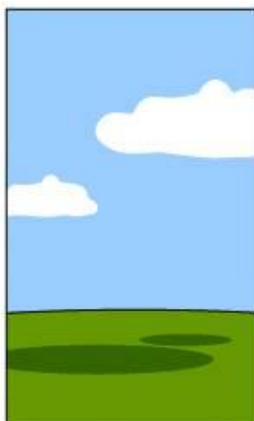
How the Analyst designed it



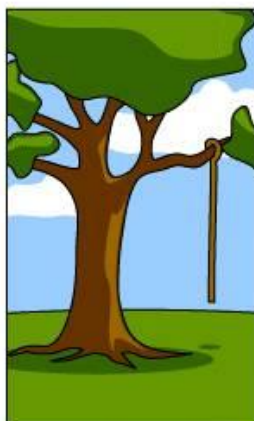
How the Programmer wrote it



How the Business Consultant described it



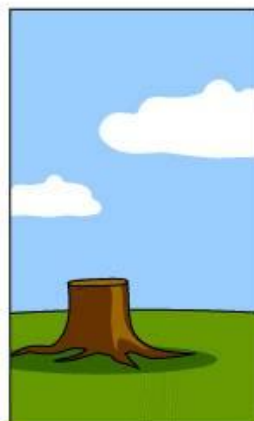
How the project was documented



What operations installed



How the customer was billed



How it was supported

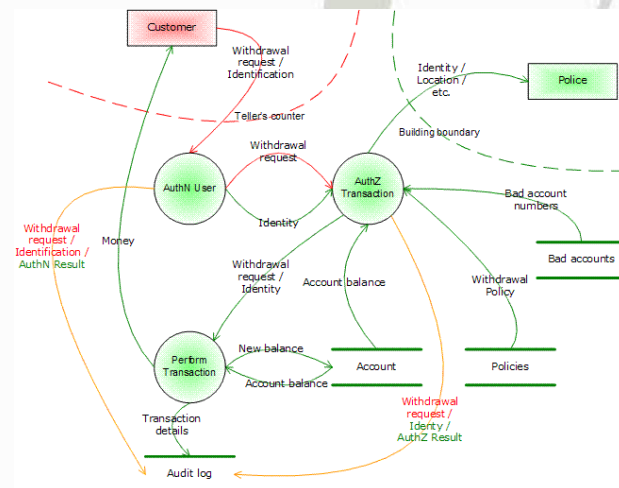


What the customer really needed

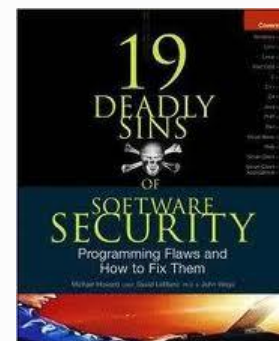
Reinventing the Wheel



Microsoft® Security Development Lifecycle



OWASP



OWASP Mobile Project



OWASP

The Open Web Application Security Project

Navigation

- ▶ Home
- ▶ News
- ▶ OWASP Projects
- ▶ Downloads
- ▶ Local Chapters
- ▶ Global Committees
- ▶ AppSec Job Board
- ▶ AppSec Conferences
- ▶ Presentations
- ▶ Video
- ▶ Press
- ▶ Get OWASP Books
- ▶ Get OWASP Gear
- ▶ Mailing Lists
- ▶ About OWASP
- ▶ Membership

Reference

- ▶ How To...
- ▶ Principles
- ▶ Threat Agents
- ▶ Attacks

OWASP Mobile Security Project

[Main/Project About](#)[For Security Testers](#)[Secure Development Guidelines](#)[Top Ten Mobile Risks](#)[Top Ten Mobile C](#)[Mobile Threat Model/Project About](#)[GoatDroid Project/Project About](#)

PROJECT INFO

What does this OWASP project offer you?

what

is this project?

Name: OWASP Mobile Security Project ([home page](#))

Purpose: The rapid growth of mobile computing has made the need for secure mobile development absolutely essential. The OWASP Mobile Security Project will help the community better understand the risks present in mobile applications, and learn to defend against them. This project will be forked into each of the following platforms:

- iOS Project
- Android Project
- webOS Project
- Windows Mobile Project
- Blackberry Project

RELEASE

What releases are ava

current release

Not Yet Published

last reviewed release

Not Yet Reviewed

all releases

Top 10 Mobile Risks

1. Insecure or unnecessary client-side data storage
2. Lack of data protection in transit
3. Personal data leakage
4. Failure to protect resources with strong authentication
5. Failure to implement least privilege authorization policy
6. Client-side injection
7. Client-side DOS
8. Malicious third-party code
9. Client-side buffer overflow
10. Failure to apply server-side controls

Top 10 Mobile Controls

1. Identify and protect sensitive data on the mobile device
2. Handle password credentials securely on the device
3. Ensure sensitive data is protected in transit
4. Implement user authentication/authorization and session management correctly
5. Keep the backend APIs (services) and the platform (server) secure
6. Perform data integration with third party services/applications securely
7. Pay specific attention to the collection and storage of consent for the collection and use of the user's data
8. Implement controls to prevent unauthorised access to paid-for resources (wallet, SMS, phone calls etc...)
9. Ensure secure distribution/provisioning of mobile applications
10. Carefully check any runtime interpretation of code for errors

Discussing Maturity

Evolution of Process Maturity

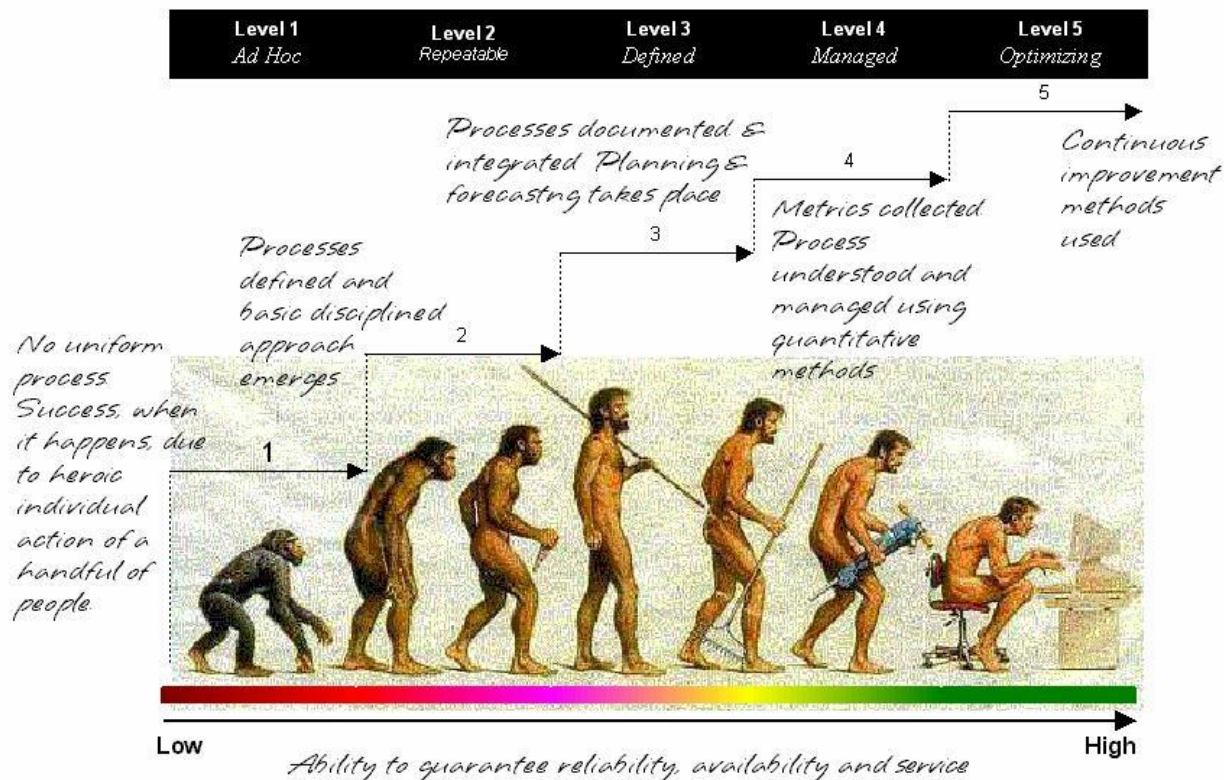


Illustration Copyright © 2001, Mike Tarrani and Linda Zaratre. All Rights Reserved

The DigiNotar Incident

Discussing Maturity

SECURITY

Sep 7, 2011 11:30 am

DigiNotar Certificates Are Pulled, but Not on Smartphones

By Robert McMillan, IDG News

Browser makers have generally been quick to react to the computer compromise at digital certificate issuer DigiNotar, but that hasn't been the case for all mobile phone makers.

SIMILAR ARTICLES:

[Apple Silent on DigiNotar Certificates Hack](#)

[How to Protect Yourself From Certificate Bandits](#)

[Comodo CEO Says DigiNotar Hack Was State-Sponsored](#)

[Google One of Many Victims in SSL Certificate Hack](#)

[Google, Skype, Yahoo Targeted by Rogue Comodo SSL Certificates](#)

[After Digital Certificate Hack, Mozilla Seeks Reassurances](#)

On Tuesday neither Google nor Apple would comment on whether they plan to revoke certificates issued by DigiNotar for Android or the iPhone, even as desktop software makers pulled the plug on the Dutch company's certificates.

Apple hasn't said anything about the DigiNotar situation since it was disclosed last week, but Google was quick to revoke the company's certificates for its Chrome browser last week. Its silence Tuesday spoke to the complexity of its situation as both a victim of the attacks and a provider of the software that can thwart them. The problem is that Google's Android phones are updated via mobile phone carriers, companies that are typically much slower to issue patches than PC software vendors such as Microsoft.



תודה!

www.comsecglobal.com

שי צלייכין, CTO

info@comsecglobal.com

שאלות?

