RSA®Conference2015

San Francisco | April 20-24 | Moscone Center

CHANGE
Challenge today's security thinking

SESSION ID: **MBS-W02**

Live Mobile Hacking Demo and Dissection!

Lior Ben-Porat

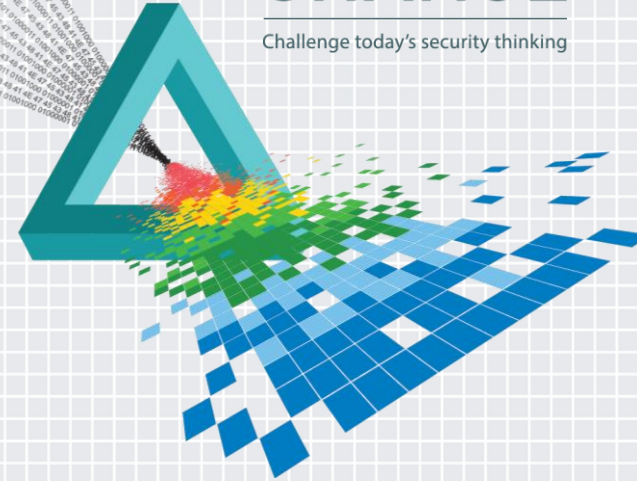Security Researcher

RSA Security

@liorbp

Rotem Salinas

Security Researcher

RSA Security

@groovesmyth

Jason Rader
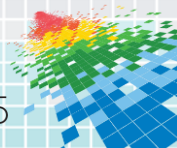
Director of Cyber Threat Intelligence

RSA Security

@jraderRSA

#RSAC

Agenda

◆ Introduction

◆ Brief History

◆ Demo: From the Victim's Perspective

◆ Demo: From the Attacker's Perspective

◆ Malware Analyst's Perspective: Tools of the Trade

◆ Demo: From the Malware Analyst's Perspective

◆ Final Demo: Mobile Ransomware…The Reality!

◆ Wrap-up and Summary

◆ Questions

RSA®Conference2015

San Francisco | April 20-24 | Moscone Center

**Demo:
Fraudster tries to log in to bank's website with stolen credentials.**

#RSAC

RSA®
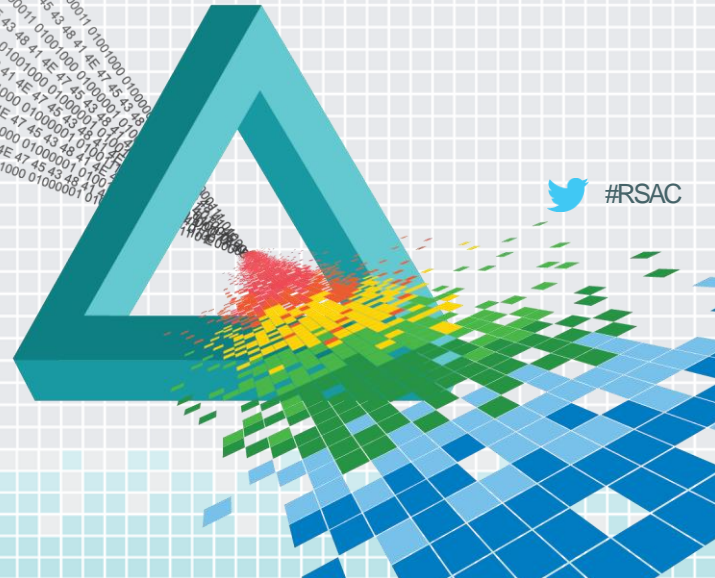
iBanking

- Actively sold for over a year. During this time, price raised from $4,000 to $5,000

- Most notably used by Neverquest (aka Vawtrak) cyber gang

- Communicates over SMS and/or HTTP

- Commands supported:
  - Capture all in/out SMS & call-list
  - Send SMS / perform a call
  - Redirect incoming calls
  - Record ambient noise of the surroundings
  - Wipe all data from the device
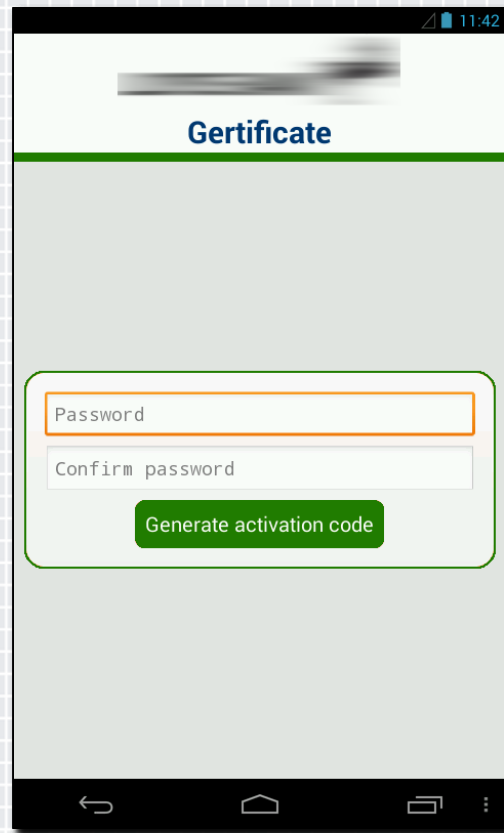
The iBanking Leak

- In February 2014 the iBanking source code was leaked on several underground forums

- Following that, few modifications were observed:
  - AES algorithm was added to encrypt all of the app's resources
  - Security fixes to the web-panel
  - Code obfuscation (Spaghetti code)
  - Anti-SDK mechanism

```
<resources>
    <string-array name="adm_domens">
        <item>4338aa1dc5facbdd4ec0b8be27e4ccb4</item>
        <item>6388995b4c309de03aa68ac12c9b4ff5</item>
        <item>942a7d4f210ad5e1db0c015a4726771e</item>
        <item>11412065eb093a3ade1c4825b64e6d16</item>
        <item>22a5ed85e999ace9c23a870822fda2a3</item>
        <item>9e2d6f1bd13eec8af0c19ef85e16ae55</item>
        <item>0d4a2ebf7fd4b5659a83e951d1aea77b</item>
        <item>4af46d70be43642f4a2bb74c44913ae2</item>
        <item>30679f21a7676ec32650a119b8bb5180</item>
    </string-array>
</resources>
```
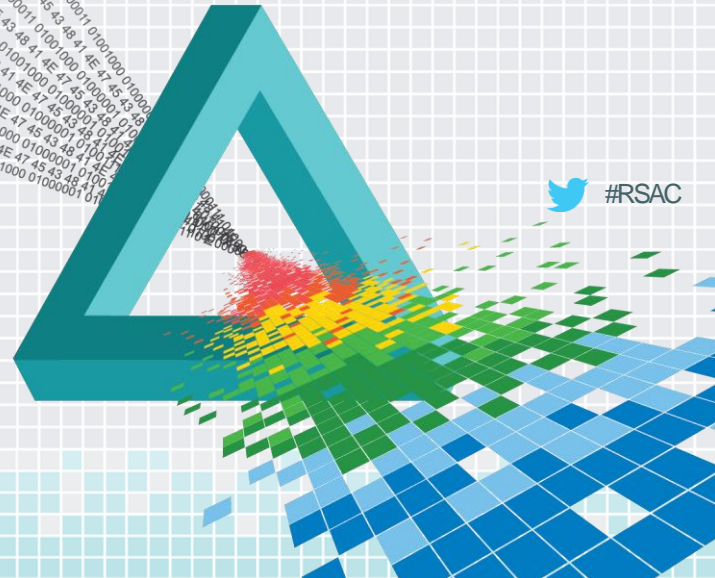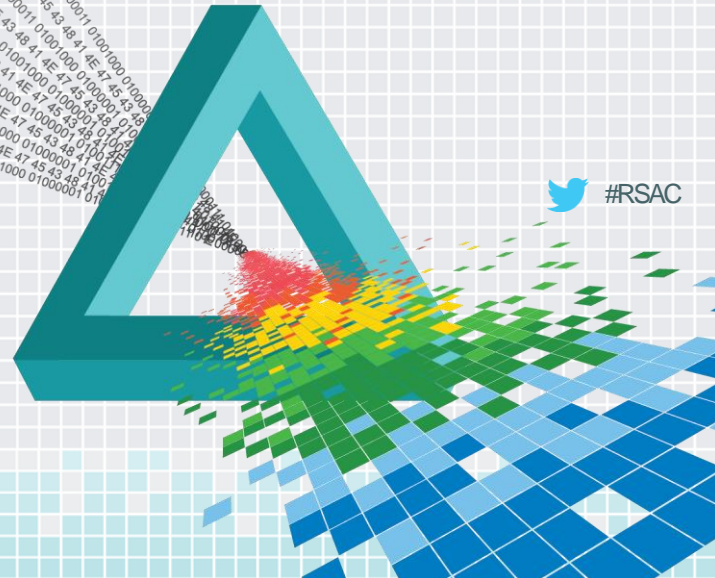
Infection Methods – Social Engineering

RSA®Conference2015

San Francisco | April 20-24 | Moscone Center

Demo:
Victim installs malicious app on his phone through bank's website

#RSAC

Analysis Tools
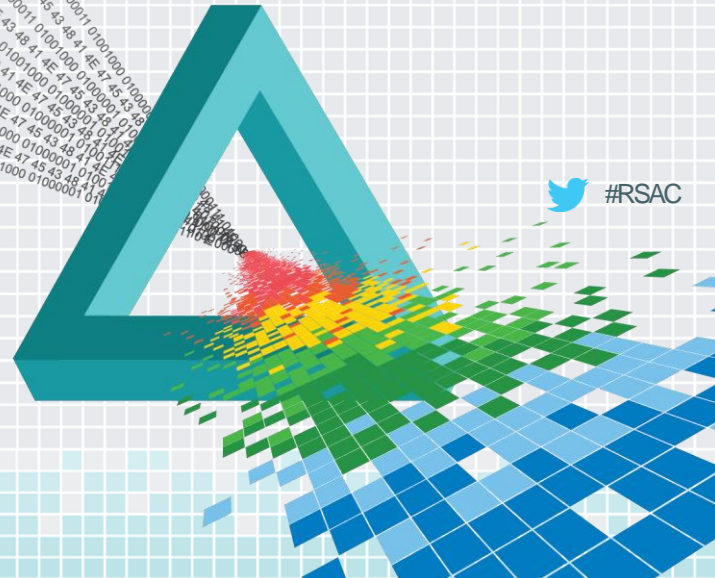
- Virtualization – Android SDK

- Android Debug Bridge (ADB)

- Emulator Console (Telnet)

- Network Monitoring and Interception
  - Wireshark - https://www.wireshark.org/download.html
  - Burp Suite - http://portswigger.net/burp/

- JD-Gui

- APKTool

- Dex2Jar

- Smali/Baksmali.jar

- JarSigner

RSA®Conference2015

San Francisco | April 20-24 | Moscone Center

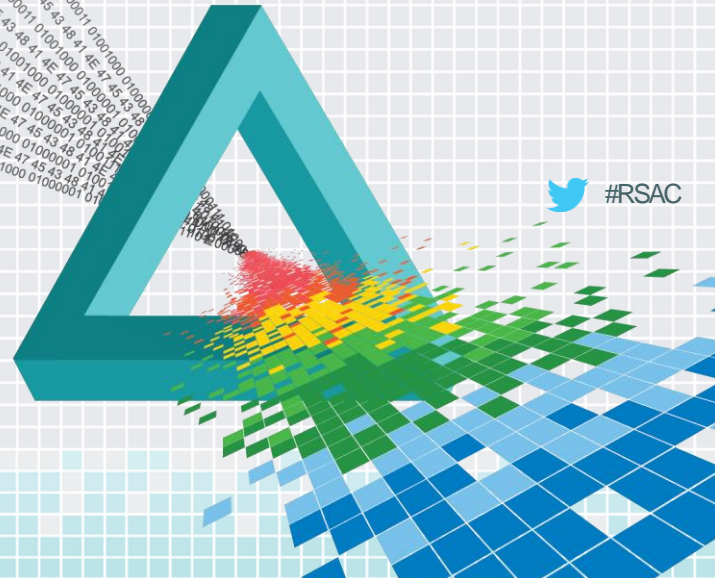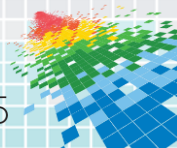# Final Demo: Mobile Ransomware…The Reality!

#RSAC

# Wrap-up & Summary

- iBanking is one of many active mobile malware projects

- They are maturing (using encryption, etc)

- They are avoiding detection and analysis

- Android and Jailbroken IOS platforms are susceptible

- The consumer needs to be aware and vigilant
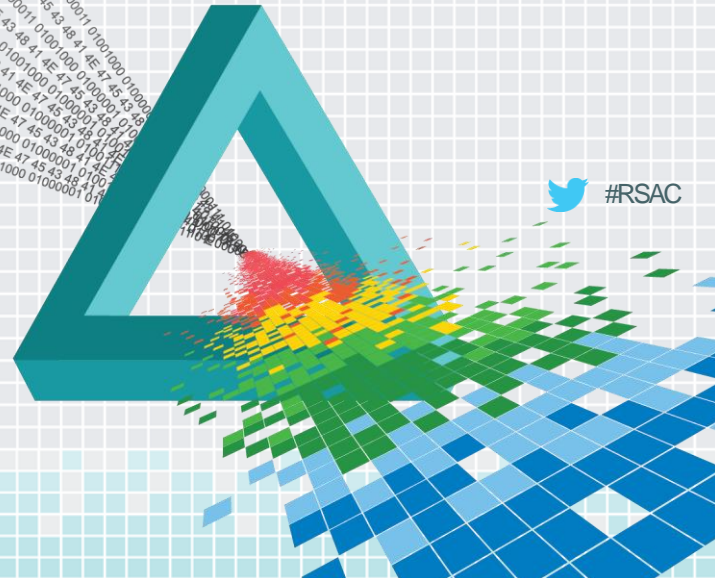
- The reality of BYOD and MDM solutions

Apply

◆ Always inspect the permissions apps request before installing.

◆ Make sure the "**Verify Apps**" option is turned-on.

◆ Do not allow users to install from sources other than the Google Play Store by disabling the "**Unknown Sources**" option in the Security Settings.

◆ Do not allow "**USB Debugging**" unless needed.

◆ Do not Root or Jailbreak your device.

◆ Make sure that no admin rights are given to applications you really trust them.
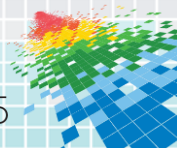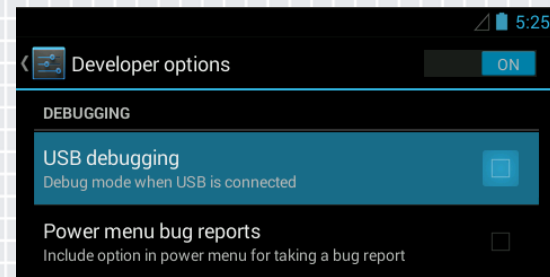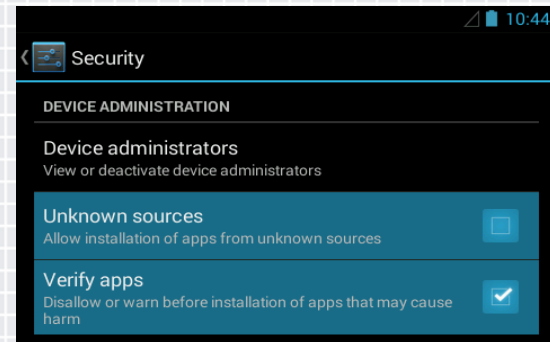
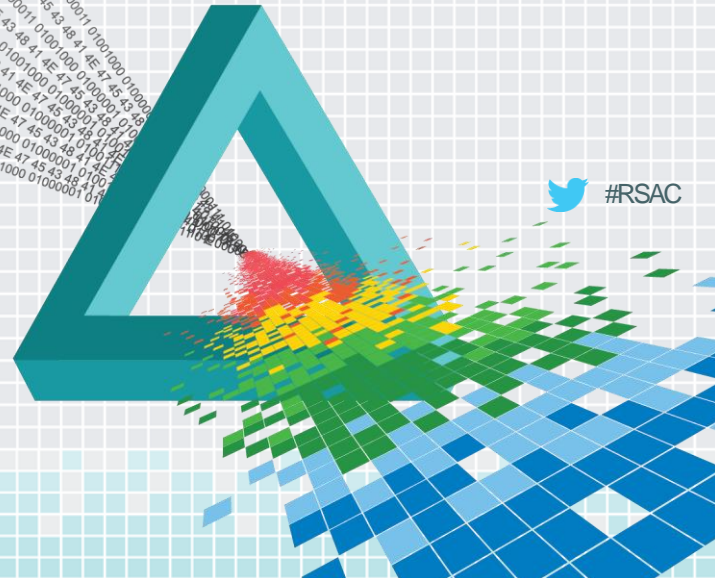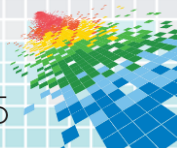# RSA®Conference2015

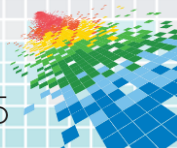San Francisco | April 20-24 | Moscone Center

#RSAC

Thank You!

RSA

Appendix – Table of Contents

- Mobile Malware Analysis Basics

- Dynamic Analysis Tools

- Live Environments/VM's

- Dalvik – Android Java VM

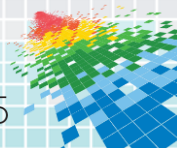- Android Architecture

- ByteCode – JIT

- Smali/Baksmali

- APK

Mobile Malware Analysis Basics

◆ Dynamic Analysis

  ◆ Running the Malware in a confined environment, such as an emulator or a VM. In our case the most popular tool is the Android SDK.

◆ Static Analysis

  ◆ Reviewing the Malware's package, and more specifically the code and the malware's resources.

Dynamic Analysis Tools

- Virtualization

  - Virtual Box - http://www.oracle.com/technetwork/server-storage/virtualbox/overview/index.html

  - VMWare - http://www.vmware.com/

  - Android SDK - http://developer.android.com/sdk/index.html

  - Google x86 Android (No Emulation=Works Faster) –

  https://code.google.com/p/android-x86/downloads/list

Dynamic Analysis Tools
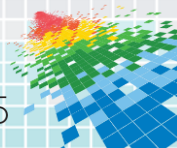
◆ Android Debug Bridge (ADB)

◆ Emulator Console (Telnet)

◆ Network Monitoring and Interception

  ◆ Wireshark - https://www.wireshark.org/download.html

  ◆ Burp Suite - http://portswigger.net/burp/

Dynamic Analysis Tools

- Virtualization
    - Virtual Box - http://www.oracle.com/technetwork/server-storage/virtualbox/overview/index.html
    - VMWare - http://www.vmware.com/
    - Android SDK - http://developer.android.com/sdk/index.html
    - Google x86 Android (No Emulation=Works Faster) –

    https://code.google.com/p/android-x86/downloads/list

Live Environments/VM's

- AppUse by AppSec Labs - https://appsec-labs.com/AppUse
    - Reframworker
    - Has all the needed tools already set up and good to go.

- Santoku Linux - https://santoku-linux.com/
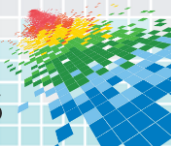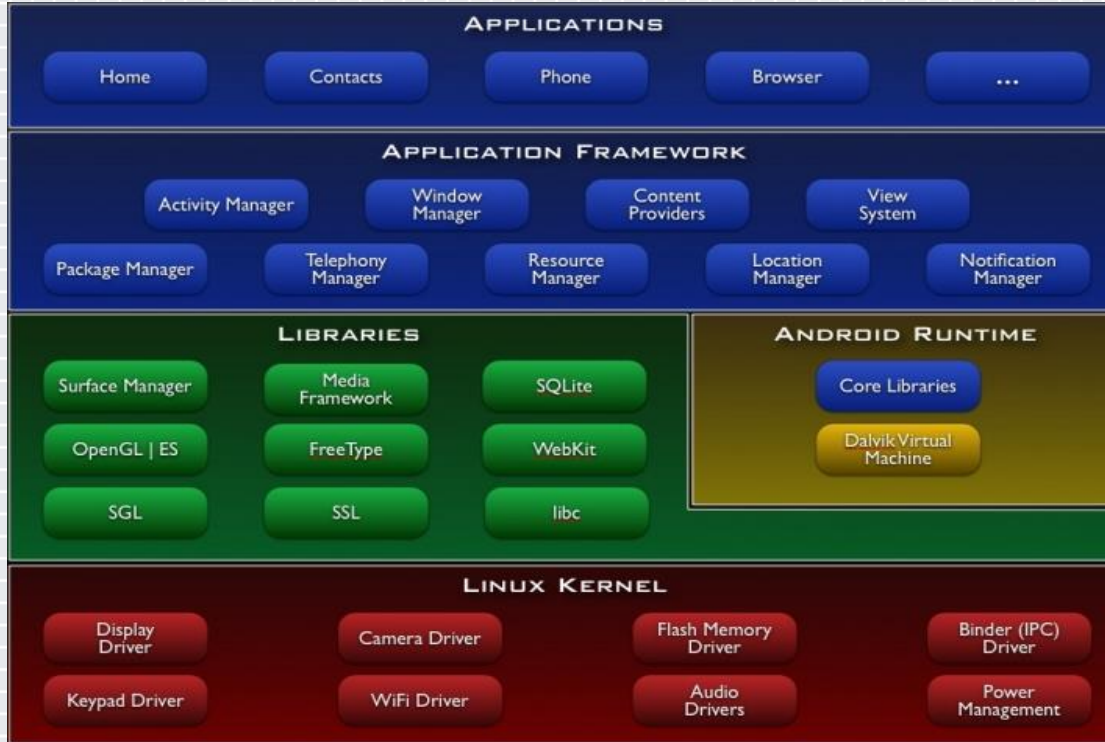
- Kali Linux - http://www.kali.org/downloads/
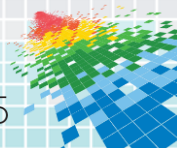
Dalvik – Android Java VM

◆ Dalvik is the virtual machine (VM) in Google's Android operating system.

◆ It is the software that runs the apps on Android devices.

◆ Dalvik is thus an integral part of Android, which is typically used on mobile devices such as mobile phones and tablets.
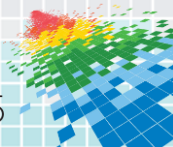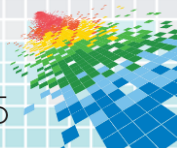
Android Architecture

Dalvik – Android Java VM

◆ Programs are commonly written in Java and compiled to Bytecode.

◆ They are then converted from Java Virtual Machine-compatible .class files to Dalvik-compatible .dex (Dalvik Executable) files before installation on a device.

◆ The compact Dalvik Executable format is designed to be suitable for systems that are constrained in terms of memory and processor speed.

Bytecode?

◆ **Bytecode,** is a form of instruction set designed for efficient execution by a software interpreter.

◆ The name bytecode stems from instruction sets which have one-byte opcodes followed by optional parameters.

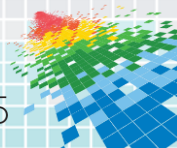- Opcode is the binary representation of a specific bytecode instruction.
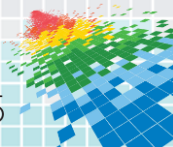
ByteCode - JIT

◆ Some systems, called dynamic translators, or "just-in-time" (JIT) compilers, translate bytecode into machine language as necessary at runtime: this makes the virtual machine hardware-specific, but doesn't lose the portability of the bytecode itself.
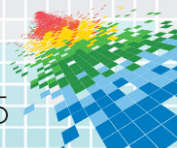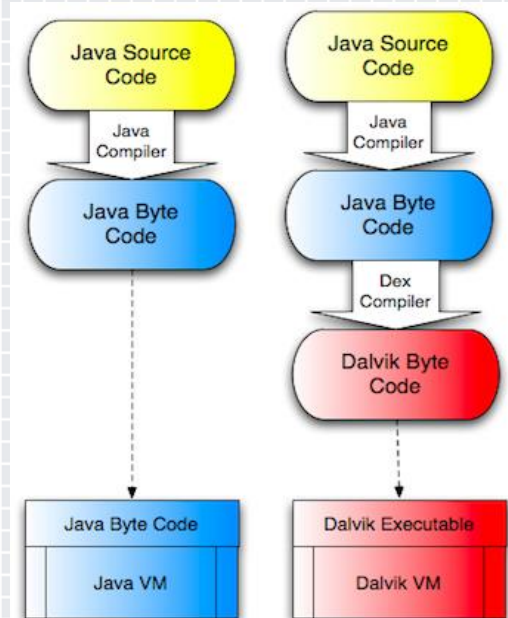
Smali/Baksmali

◆ Smali/Baksmali is an assembler/disassembler for the dex format used by dalvik (Android's Java VM implementation).

◆ The syntax is loosely based on Jasmin's/dedexer's syntax.

Smali/Baksmali

◆ The names "smali" and "baksmali" are the Icelandic equivalents of "assembler" and "disassembler" respectively.

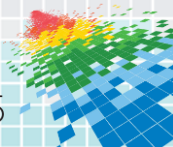◆ Why Icelandic you ask? Because dalvik was named for an Icelandic fishing village.
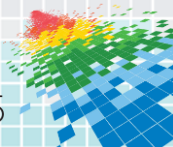
Java-Smali Comparison

◆ Hello World Program in Java

import java.io.PrintStream;

public class HelloWorld {

    public static void main(String[] paramArrayOfString) {

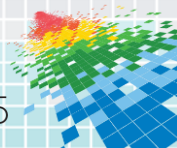   System.out.println("Hello World!");

    }

}

Java-Smali Comparison
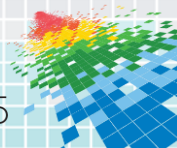
- ◆ Hello World in Smali

```
.class public LHelloWorld;
.super Ljava/lang/Object;


.method public static main([Ljava/lang/String;)V
   .registers 2
   sget-object v0, Ljava/lang/System;->out:Ljava/io/PrintStream;
   const-string  v1, "Hello World!"
   invoke-virtual {v0, v1}, Ljava/io/PrintStream;->println(Ljava/lang/String;)V
   return-void
.end method
```

APK

- Android **application package file** (**APK**) is the file format used to distribute and install application software and middleware onto Google's Android operating system.

- An APK file contains all of that program's code (such as .dex files), resources, assets, certificates, and manifest file.

- APK files are ZIP file formatted packages based on the JAR file format, with .apk file extensions.

APK