Automated Security Analysis of Android & iOS Applications with Mobile Security Framework

Ajin Abraham

About Me

- Application Security Engineer, Yodlee
- Author of OWASP Xenotix XSS Exploit Framework, Mobile Security Framework.
- Co-Organizer of X0RC0NF.
- Blog about Security: **http://opensecurity.in**


n|uCON


black hat
EUROPE 2013


HITBSecConf
AMSTERDAM // MALAYSIA


OWASP
APPSEC
APAC 2013


ClubHACK


ASIA'S FOREMOST INFORMATION SECURITY CONFERENCE
GROUND ZERO


black hat
ASIA 2015

The Takeaways

- A Free and Open Source Tool
- Mobile App Pentesters/Malware Analysts - How to make your life easier.
- Developers – Build secure mobile Apps by detecting vulnerabilities at earlier stages of development.
- For the Rest – Some new Information.

WTF is it?

Mobile Security Framework is an open source mobile application (Android/iOS) automated pentesting framework capable of performing static and dynamic security analysis*.

Hosted in your environment. Your application and data is never send to the cloud.

Basic Requirements

Android

- Python 2.7
- Django 1.8
- Oracle Java - JDK 1.7+
- Oracle VirtualBox

iOS

- Python 2.7
- Django 1.8
- Oracle Java - JDK 1.7+
- Oracle VirtualBox
- Mac

Static Analyzer

Mobile Security Framework

Static Analysis

Android Binary

- INFORMATION GATHERING
- DECOMPILE TO JAVA & SMALI
- PERMISSION ANALYSIS
- MANIFEST ANALYSIS
- JAVA CODE ANALYSIS
- ANDROID API INFO
- FILE ANALYSIS
- URLS, EMAIL, FILES, STRINGS, ANDROID COMPONENTS
- **REPORT GENERATION**

Static Analysis

Android Source

- INFORMATION GATHERING
- ~~DECOMPILE TO JAVA & SMALI~~
- PERMISSION ANALYSIS
- MANIFEST ANALYSIS
- JAVA CODE ANALYSIS
- ANDROID API INFO
- FILE ANALYSIS
- URLS, EMAIL, FILES, STRINGS, ANDROID COMPONENTS
- **REPORT GENERATION**

DEMO

- Static Analysis of APK
- Static Analysis of Zipped Source Code

Static Analysis

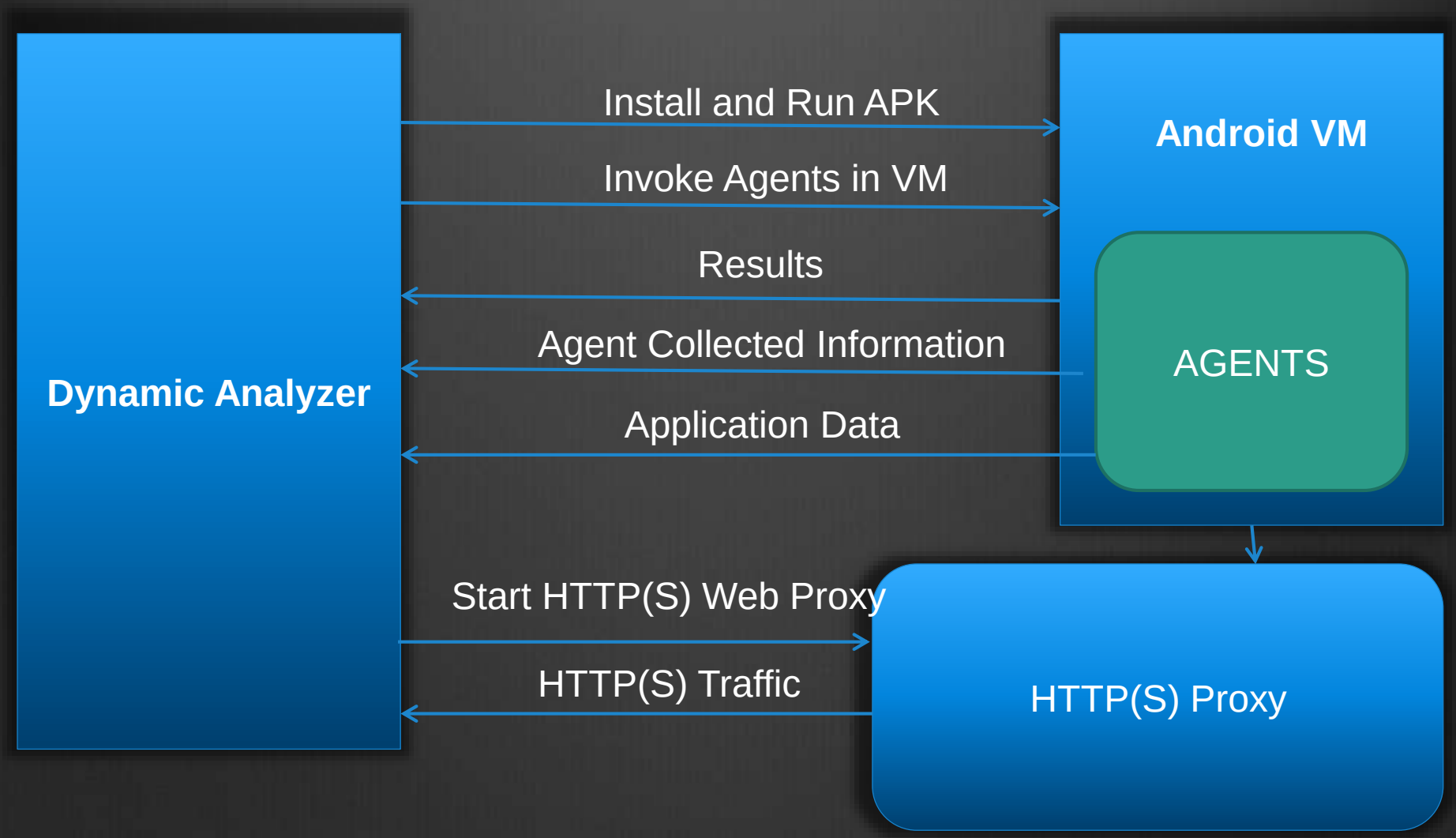
- iOS - Binary
  - BASIC INFORMATION
  - BINARY ANALYSIS
  - FILE ANALYSIS
  - LIBRARIES
  - **REPORT GENERATION**
- iOS - Source
  - BASIC INFORMATION
  - CODE ANALYSIS
  - iOS API INFORMATION
  - FILE ANALYSIS
  - URL, EMAIL, FILES, LIBRARIES
  - **REPORT GENERATION**

DEMO

- Static Analysis of IPA Binary
- Static Analysis of Zipped Source Code

Dynamic Analyzer

Dynamic Analyzer - Architecture



Dynamic Analysis

- SCREENSHOT
- CAPTURE HTTP(S) TRAFFIC
- LOGCAT and DUMPSYS
- DYNAMIC API MONITOR
- DYNAMIC URLS and EMAILS MONITOR
- APPLICATION DATA DUMPER
- FILE ANALYSIS ON APPLICATION DATA
- REPORT GENERATION
- UNDER DEVELOPMENT

DEMO

- Dynamic Analysis of Android Application

Some Real World Results

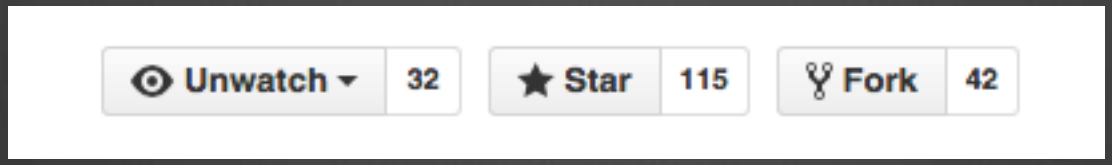
- Mobile Security Framework – Bypassing PIN in Whisper Android Application - http://opensecurity.in/mobile-security-framework-bypassing-pin-in-whisper-android-application/
- AppLock MITM Password Reset Vulnerability - http://opensecurity.in/applock-mitm-password-reset-vulnerability/

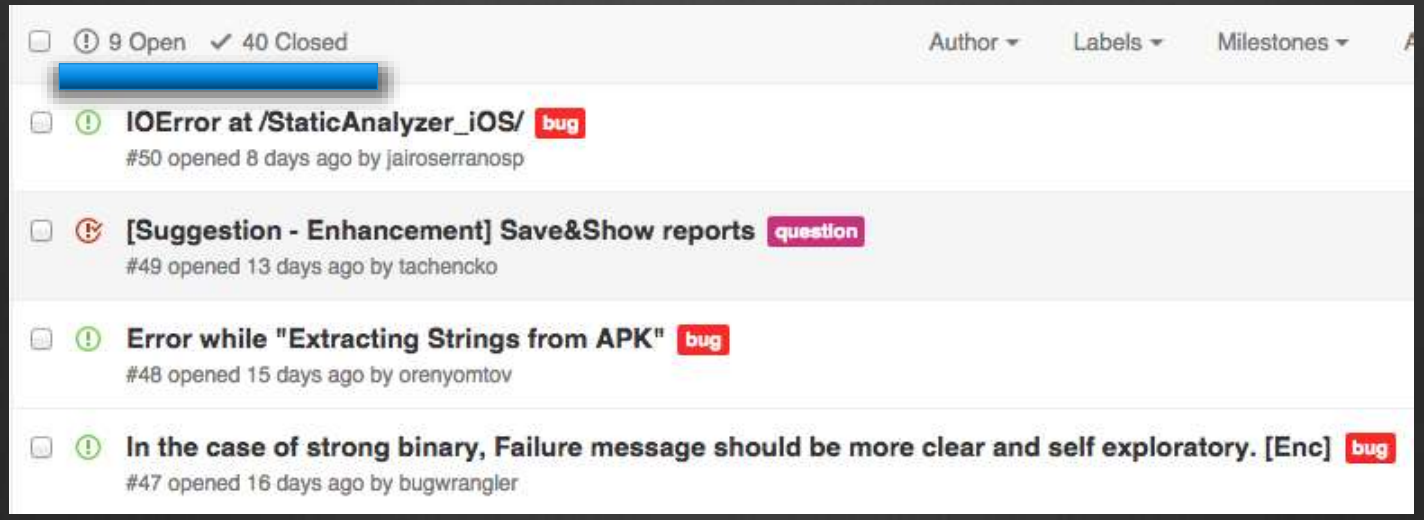
AppLock MITM Password Reset Vulnerability DEMO

ANDROID MALWARE ANALYSIS DEMO

Future Plans

- Looks like people are interested!





In Aplha Dev

- Web Service Testing/REST API testing for Hybrid Applications.
- Dynamic Analysis Support for Real Android and iOS Devices.
- Anti VM/Sandbox Detection Bypass.
- IDOR and Cross Talk Detection support in Proxy.
- Better Front End.
- DB Support.
- Scheduled Scans.

What you can do?

- Download, Test, Contribute
- Source: https://github.com/ajinabraham/YSO-Mobile-Security-Framework
- Issues: https://github.com/ajinabraham/YSO-Mobile-Security-Framework/issues

QA

Thanks

- Bharadwaj Machiraju
- Anto Joseph
- Tim Brown
- Thomas Abraham
- Graphics/Image Owners

@ajinabraham

ajin25@gmail.com

http://opensecurity.in