COVERT Tool User Manual

version 2.0

COVERT is a tool for compositional analysis of Android inter-application vulnerabilities. It automatically identifies vulnerabilities that occur due to the interaction of apps comprising a system. Subsequently, it determines whether it is safe for a bundle of apps, requiring certain permissions and potentially interacting with each other, to be installed together. COVERT takes as input Android executable files, so-called APK files. APKs are essentially Java bytecode packages used to distribute and install Android applications. As an output, COVERT produces a list of inter-application vulnerabilities identified in the input applications.

SMlab
Computer Science Department
George Mason University

WWW: http://www.sdalab.com/
Point of Contact: Sam Malek, PhD
Email: smalek@gmu.edu
November 2014

Covert Command Line Tool

Installation

1- Install **JDK 8**
2- Unzip COVERT.zip (the unzipped directory: **$COVERT**)

Usage (Mac, Linux)

1- Go to **$COVERT**/app_repo directory and create a new subdirectory that represents a bundle of apps (**$bundle**)
2- Copy the app files (.apk files) into the created bundle directory (**$bundle**)
3- Open command line and go to the COVERT root directory **($COVERT**)
4- Run COVERT with the name of **$bundle** as the only parameter: `covert.sh $bundle` (e.g., covert.sh test)
5- The generated report of detected vulnerabilities is a XML file named **$bundle.xml** (e.g. test.xml) in the **$bundle** directory

Usage (Windows)

Same as Mac/Linux usages, except that (in step5) run `covert.bat $bundle`

Covert Client Tool

Installation (mac)

Use **Covert-2.0.dmg**

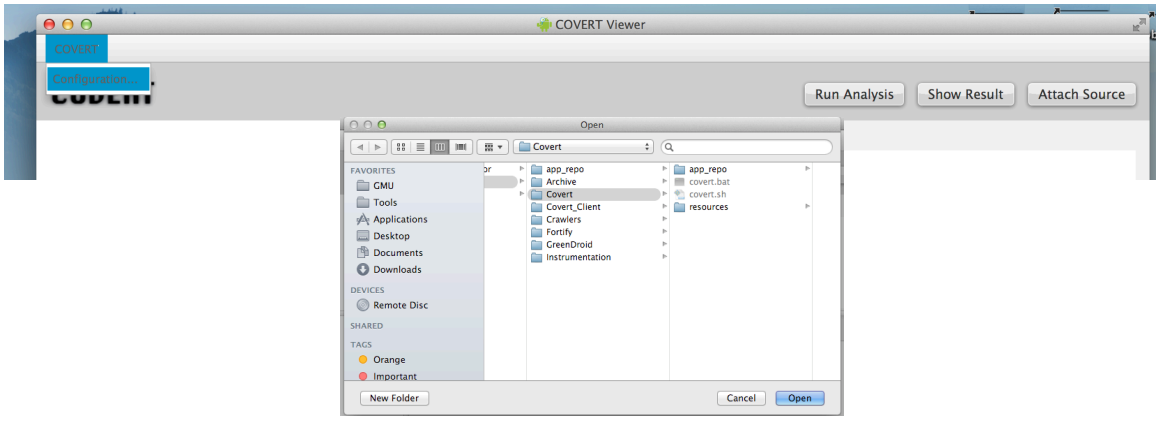
Installation (windows)

Use **Covert-2.0.exe**

(The tool bundle will be copied to C:/Users/[yourname]/AppData/Local/Covert)

Usage

1. In menu-> Covert -> Configuration… Set the **$COVERT** directory (unzipped in step2 of command line installation) as the root directory.



2.

a. (Faster, *Recommended*) For viewing the results of covert command line tool (see Covert Command Line Tool Usage in the previous section), click **"Show Result"** and select the **$bundle.xml** file generated before.
b. (Slower) For running the covert analyzer directly from the Client Tool, click **"Run Analysis"** and select the apps (.apk files) to be analyzed.

3. The decompiled source code of the vulnerable components is shown by default. If the app's source code is available, it can be attached to the result by **"Attach Source"** button.