apkのリバースエンジニアリング

第9回Android勉強会in札幌

2011.05.28

高橋@codeHead.jp

自己紹介

高橋@codeHead

（株）コードヘッド 代表

Androidアプリ開発

- 自社アプリ企画、開発
  - scrapRoid
    A3 2010-2011 Winter
    企画賞 受賞！！

- 受託開発
  - 企業向け
  - マーケット販売用

Webシステム開発

- Webシステム受託開発
  - インフラ層 〜 アプリ層　迄を全て
  - 一般的なWebシステム
    〜 ワンオフの特殊システム迄
- OSS利用、仮想化

今回の話題は？

apkファイルから
ソースコード、リソースを
解析する話題です

何故

やろうと思ったか？

Seagate
CAUTION:

2011年5月30日月曜日

2011年5月30日月曜日

はじめに

apkファイル

- apk = application package file
- 配布用のパッケージファイル
- コード（dexファイル）、リソース、アセット、マニフェストファイルを内包

dexファイル

- dex = Dalvik Executable
- DalvikVM用にコンパイルされた実行ファイル
- プログラムコード部分に相当
  .javaからコンパイル

早速リバースしてみよう！

使用ツール、環境

- apktool
  .apkファイルをデコンパイル
- baksmail
  .odexファイルをディスアセンブル

※今回、Centos5上にリバース環境を作成しました

デモ1

- 自分で作成した.apkファイルをリバースしてみる
- 元のソースを見る
- 結果を見てみる
  → 結構読める！！

結構読めます

ローカル変数

.local v0, btn:Landroid/widget/Button;

.local ?, [変数名]:[変数の型]

メソッド呼出し

Ljp/codehead/revtest01/Revtest01;->
findViewById(I)Landroid/view/View;

L[パッケージ]/[クラス];->
[メソッド]([引数の型])[戻り値の型];

デモ２

- 端末から持ってきた.apkファイルをリバースしてみる
- 結果を見てみる
- odexファイルをデコンパイル
- 結果を見てみる

デモ３

- 難読化した.apkファイルをリバースしてみる
- 結果を見てみる
- 今回の様な単純な例の場合、結構読める...

それで、どうなの？

- インテントの調査には、かなり使える
- レイアウト、アニメーションの調査にもGOOD！
- コードを読むのは、結構ツライ...
- うっかりソース公開されているものをリバースしない
- 難読化は万能ではない

【補足資料】

情報ソース

- Web
  - http://code.google.com/p/android-apktool/
  - http://code.google.com/p/smali/

END