If you can see this, you aren't viewing this presentation the right way.

To help illustrate some of the concepts in this presentation, I've used PowerPoint animations. View this presentation in Slide Show mode (press F5 to start). Watch for embedded video and audio content, too!

Thanks!

-Josh
INTRODUCTION

- Motivation
- The Plan
- Android Package Analysis — Ghost Hunter, Joe's Ghost Box
- Android Static Analysis — Ghost Hunter
- Obfuscated Static Analysis — Ghost Radar
- Cross-Platform Dev Analysis — Ouija: Real Spirit Board
- Applying Android Reverse Engineering Skills
THE PLAN

Spend $200 on Android ghost detection apps from four categories
  - Electromagnetic Frequency Measurement (EMF) tools
  - Electronic Voice Phenomenon (EVP) measurement (ghost audio)
  - Ghost radar and visual identification apps
  - Ghost communication tools

Use apps in a variety of locations as intended (cemeteries, woods at night)

Reverse engineer apps to evaluate how they function
  - Using open-source/free tools, and a cheap, rooted Android device

Use this project to build my Android reverse-engineering skills
CHOOSING APPS

Limited to pay-for applications ($0.99 to $29.99)
Focus on "pro" apps that claim to meet or exceed commercial tools
Focused on apps that perform "genuine" ghost detection
Exclude apps marked as intended for entertainment

- Ghost Hunter
- Joe's Ghost Box
- Ghost Speaker
- P-SB7 Ghost Box
- My Own Ouija Board
GHOST HUNTER App

- Published by IntelliTech Entertainment, $0.99
- 3.6 stars, 498 ratings, 10K-50K downloads
- EMF scanner, EVP recording, visual decoding, and a spirit board

"I use a lot of the "ghost hunting" apps. [...] I have tested my phone against equipment used by pros & it has worked. I can tell a fake app when I see one."

Julie Hafford, 4-star Rating
NO PARANORMAL ACTIVITY DETECTED
$ adb shell pm list packages | grep -Ev "com\.android|com\.google"
package:com.gregorypothier.AIOGhostHunter
package:android
package:com.example.android.softkeyboard
package:com.svox.pico
package:jp.co.omronsoft.openwnn
$ adb shell ls /data/app/com.greg*
/data/app/com.gregorypothier.AIOGhostHunter-1.apk
$ adb pull /data/app/com.gregorypothier.AIOGhostHunter-1.apk
[100%] /data/app/com.gregorypothier.AIOGhostHunter-1.apk
$ mkdir aioghosthunter
$ unzip -d aioghosthunter/ com.gregorypothier.AIOGhostHunter-1.apk
Archive: com.gregorypothier.AIOGhostHunter-1.apk
inflating: aioghosthunter/res/layout/audiomain.xml
inflating: aioghosthunter/res/layout/audiorecorderlayout.xml
inflating: aioghosthunter/res/layout/audiotrack.xml
inflating: aioghosthunter/res/layout/draw.xml
inflating: aioghosthunter/res/layout/emf.xml
...  
extracting: aioghosthunter/res/drawable-hdpi/redscan1.jpg
extracting: aioghosthunter/res/drawable-hdpi/redscan10.jpg
extracting: aioghosthunter/res/drawable-hdpi/redscan2.jpg
extracting: aioghosthunter/res/drawable-hdpi/redscan21.jpg
... 
extracting: aioghosthunter/res/drawable-mdpi/icon.png
inflating: aioghosthunter/classes.dex
inflating: aioghosthunter/META-INF/MANIFEST.MF
inflating: aioghosthunter/META-INF/CERT.SF
inflating: aioghosthunter/META-INF/CERT.RSA
GHOSTLY IMAGES

8 static images with "ghosts" on radar view
// 70% of the time, display the animated green scanning images
if (PreviewActivity.this.randInt0to100 < 70) {
    randInt0to10 = new Random().nextInt(10);
    if (randInt0to10 < 4) {
        ((ImageView) ... setSource(R.drawable.greenscan1);
    }
}
// 30% of the time, display the Paranormal Activity Detected red images
if (PreviewActivity.this.randInt0to100 >= 70) {
    if (randInt0to10 < 4) {
        ((ImageView) ... setSource(R.drawable.redscan1);
    }
    else if (PreviewActivity.this.mySecondsPassed == 1) {
        if (randInt0to10 < 8) {
            ((ImageView) ... setSource(R.drawable.redscan3);
        }
        else if (randInt0to10 < 8) {
            ((ImageView) ... setSource(R.drawable.redscan23);
        }
        else if (randInt0to10 > 8) {
            ((ImageView) ... setSource(R.drawable.ghost3); // scary
I. Flores, 5-star Rating

"I was just looking at my dad's picture in my head telling him I missed him. Then on my third try using the app I hear I love you to in Spanish which is the language he spoke..."
JOE’S GHOST BOX
Functionality

Simple controls, turn the virtual replica of the actual Joe’s Ghost Box on.

Extracts and plays EVP audio content.

You ask questions and listen for answers.
JOE'S GHOST BOX FILE SYSTEM DATA

$ mkdir joesghostbox
$ unzip -d joesghostbox/ com.stevehultay.joesbox1-1.apk
 Archive: com.stevehultay.joesbox1-1.apk
 inflating: joesghostbox/AndroidManifest.xml
 inflating: joesghostbox/assets/Fonts/font_one.ttf
 inflating: joesghostbox/res/anim/abc_fade_in.xml
 inflating: joesghostbox/res/anim/abc_fade_out.xml
 extracting: joesghostbox/res/raw/a000001.mp3
 extracting: joesghostbox/res/raw/a0000010.mp3
 extracting: joesghostbox/res/raw/a00000100.mp3
 extracting: joesghostbox/res/raw/a00000101.mp3
 extracting: joesghostbox/res/raw/a00000102.mp3
 extracting: joesghostbox/res/raw/a00000103.mp3
 extracting: joesghostbox/res/raw/a00000104.mp3
 extracting: joesghostbox/res/raw/a00000105.mp3
 extracting: joesghostbox/res/raw/a00000106.mp3
 extracting: joesghostbox/res/raw/a00000107.mp3
 extracting: joesghostbox/res/raw/a00000108.mp3
 extracting: joesghostbox/res/raw/a00000109.mp3

Ghostly MP3 File Count: 13,986
public void initializeViews() {
    try {
        // Choose a random "song" from the songNames list as a mediaPlayer object
        this.value = new Random().nextInt(this.songNames.size());
        this.nameIntRandom = Integer.parseInt(this.songNames.get(this.value));
        this.mediaPlayer = MediaPlayer.create(getActivity(), this.nameIntRandom);
    }
    if (this.countInitialaze > 0 && toggleCount > 0) {
        if (this.finalTime < 2000.0d) {
            // finalTime is a constant - future feature?
            play(); // Play the selected song
        }
    }
    this.countInitialaze++;
}

Question: Can ghosts influence the RNG on Android devices?
P-SB7 GHOST BOX App

- Published by Luna Spirit Detection
- $14.99, 2.9 stars, 11 ratings
- EVP app, decoding AM/FM radio frequency waves, noise cancellation

"I own a P-SB7 device and I decided to compare this app to it. To my surprise, they picked up nearly exactly the same readings. I highly recommend this app"

Billy Allen, 5-star Rating
P-SB7
GHOST BOX
Functionality

Click "ON" to hear EVP

Recommends waiting 3 minutes for calibration

Ask questions, listen for answers

"Proven to work on many accounts ... featured on the Travel Channel!"

"Tap the power button and wait 2-3 minutes for calibration"

"The P-SB7 will cancel out noise and detect AM/FM frequency waves"
ANDROID APP DECOMPILATION

Android apps are distributed as bytecode interpreted files

- Like a Java JAR file — unlike Windows PE, Linux ELF, macOS Mach-O files (NDK exception)

APK files can be viewed as decompiled Java source

- Not the original Java source, but pretty close

 Historically, DEX2JAR, then JD-GUI, Procyon, CFR, Fernflower, etc.

Better: JadX by Skylot

JadX is a superior Android RE tool, eliminating the need for DEX2JAR
public class MainActivity extends Activity {

    MediaPlayer mplayer;

    /* renamed from: com.gbox.p_sb7.MainActivity_1 */
    class AnonymousClass1 implements OnCheckedChangeListener {
        private final /* synthetic */ MediaPlayer mediaPlayer;

        AnonymousClass1(MediaPlayer mediaPlayer) {
            this.val$mplayer = mediaPlayer;
        }

        public void onCheckedChanged(CompoundButton buttonView, boolean isChecked) {
            if (isChecked) {
                this.val$mplayer.start();
                this.val$mplayer.setLooping(true);
                return;
            }
            this.val$mplayer.setLooping(false);
            this.val$mplayer.stop();
        }
    }

    protected void onCreate(Bundle savedInstanceState) {
        super.onCreate(savedInstanceState);
        setContentView(R.layout.activity_main);
        ((ToggleButton) findViewById(R.id.toggleButton1)).setOnCheckedChangeListener(new AnonymousClass1(MediaPlayer.create(this, R.raw.ghost)));
    }
}
$ ls
com.gbox.p_sb7-1.apk
$ unzip -q com.gbox.p_sb7-1.apk
$ cd res/raw
$ ls -l ghost*
-rw-r--r-- 1 jwright staff 1212537 Mar 22 2015 ghost.ogg

R.RAW.GONE

$15!!!
GHOST SPEAKER App

- Published by Luna Spirit Detection
- $2.99, 3.5 stars, 403 ratings
- EVP app, decoding AM/FM radio frequency waves, noise cancellation

"Got names at a Cemetery. George for one, turned around was standing in front of Georges head stone. This app is real and can be manipulated by spirit."

Jojo B., 5-star Rating
GHOST SPEAKER App

Surveys the environmental electromagnetic field readings

Accepts input in the form of questions from user

Decodes EMF data, producing speech synthesis output

"... values are processed through the speech translation software"

"... calculates energy values that paranormal entities might be projecting"
Krugism used application obfuscation to obscure object and variable names.
DECODING OBFUSCATED CODE

Import JadX code into Android Studio for analysis

- Start Android Studio, click Import project (Eclipse ADT, Gradle, etc.)
- Select JadX output directory then click Next | Next | Next | Next | Next | Next | Finish

Start your analysis at the micro-level

- Focus on small-picture items, ignore the big-picture for now
- Try to understand small pieces of code, a little at a time
- Use the Android Developer and Stack Overflow sites to help understand code

$ mkdir ghostspeaker
$ jadx -d ghostspeaker com.krugism.GhostSpeaker-1.apk
...
$ ls ghostspeaker/
AndroidManifest.xml  android/  com/  org/  res/

$ mkdir ghostspeaker
$ jadx -d ghostspeaker com.krugism.GhostSpeaker-1.apk
...
REFACCTOR AND RENAME VARIABLES
USE LOGGING MESSAGES, EXCEPTIONS

Use string clues in code to rename variables, methods.
It's OK to rename variables to complex object type names.
USE TEMPORARY NAMES FOR READABILITY

When you have more context, rename again later, adding comments as needed.
GHOST SPEAKER: readSensorDataMaths
GHOST SPEAKER: `speakDictWordHandler`
GHOST SPEAKER: readDictWordListIntoArray

BUSTED
FUN WITH SCARY WORDLIST

```python
$ python
>>> import os, random
>>> words = [line.rstrip() for line in open("DICT")]
>>> len(words)
2854
>>> for i in range(0,4): os.system("say -v Bahh -i %s"%random.choice(words))
claim
lighthouse
abscess
poisoned
>>> for i in range(0,4): os.system("say -v Bad -i %s"%random.choice(words))
born
relax
evil
Camille
>>> for i in range(0,4): os.system("say -v Whisper -i %s"%random.choice(words))
angel
musette bag
metal
burn
```
OUIJA App

• Published by Redwerk Board
• $3.84, 3.4 stars, 18 ratings
• "Converse with ghosts and spirits right from your phone"

"Connected with spirit named P. This app should be strictly prohibited to cold hearted users. I couldn't sleep last night. And I feel like I am possessed now."

Mukta Poudel, 4-star Rating
OUIJA App Functionality

Type to ask a question

Spirit responds by moving planchette

"No spirits were hurt during the development of this project"
CROSS-PLATFORM DEV

Unity logo discloses that Ouija is a cross-platform development app

- PhoneGap, Xamarin, 5App, etc.

_Behavioral_ analysis remains the same

_Static_ analysis techniques require platform-specific tools and techniques

Unity offers C#, BOO or JavaScript support with the Unity Engine
# EXTRACTED OUIJA APK

<table>
<thead>
<tr>
<th>File(s)</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>AndroidManifest.xml</td>
<td>Minimal Android app declarations</td>
</tr>
<tr>
<td>classes.dex</td>
<td>Minimal Android app to launch the Unity Engine (for ARM, or x86)</td>
</tr>
<tr>
<td>lib/*</td>
<td>Natively compiled libraries for the Unity Engine</td>
</tr>
<tr>
<td>assets/bin/Data/*</td>
<td>Shaders, textures, and other Unity objects</td>
</tr>
<tr>
<td>assets/bin/Data/Managed/Assembly *.dll</td>
<td>Unity app binaries</td>
</tr>
</tbody>
</table>

Unity code is not compiled; it is stored in CIL format (like a JAR file)
OUIJA APP DECOMPILATION

Ouija has Assembly-CSharp.dll

We can use a C# decompiler to analyze Ouija's code

JetBrains dotPeek decompiles CIL files, revealing approximated C# code

- Free, closed source
- "JadX for C#"
public SpiritAI()
{
    this.bots = new List<ChatterBotSession>();
    base..ctor();

    ChatterBotFactory chatterBotFactory = new ChatterBotFactory();
    this.cleverBot = chatterBotFactory.Create(ChatterBotType.CLEVERBOT);      
    this.cleverBotSession = this.cleverBot.CreateSession();
    this.pandoraBot = chatterBotFactory.Create(ChatterBotType.PANDORABOTS, (object) "b0dafd24ee35a477"));
    this.pandoraBotSession = this.pandoraBot.CreateSession();

    HttpWebResponse response = (HttpWebResponse) httpWebRequest.GetResponse();
    if (response != null && response.StatusCode == HttpStatusCode.OK)
    {
        this.jabberwackyBot = chatterBotFactory.Create(ChatterBotType.JABBERWACKY);
        this.jabberwackyBotSession = this.jabberwackyBot.CreateSession();
    }
    this.bots.Add(this.cleverBotSession);
    this.bots.Add(this.pandoraBotSession);
    this.bots.Add(this.jabberwackyBotSession);
    this.105Fuck = object.Equals(new object(), new object());
    if (this.105Fuck)
CHATTERBOXFACTORY CLASS

```csharp
switch (type)
{
    case ChatterBotType.CLEVERBOT:
        return (ChatterBot) new Cleverbot("http://www.cleverbot.com/", "http://www.cleverbot.com/webservicemin", 18);
    case ChatterBotType.JABBERWACKY:
        return (ChatterBot) new Cleverbot("http://jabberwacky.com", "http://jabberwacky.com/webservicemin", 20);
    default:
        throw new ApplicationException("PANDORABOTS needs a botid arg");
        return (ChatterBot) new PandoraBots(arg.ToString());

        return (ChatterBot) null;
}
```
Why does the sun shine?
Is there a spirit present?

There is always some spirit in the machine.
Are you a bot?

I am always your bot.
SPIRIT RESPONSE

Are you a bot?
I am not a ghost. I am as real as you.
```csharp
static ReplaceWords()
{
    ReplaceWords.ReplaceWordsDictionary = new Dictionary<string, string[]>();
    {
        "spirit",
        "ghost",
        "psyche",
        "soul"
    });
    {
        "spirit",
        "ghost",
        "psyche"
    });
}
```
SPIRITAI CLASS, REPLACEWORDS

```
if (answerCanStoreItems == str3) {
    string[] strArray;
    if (ReplaceWords.ReplaceWordsDictionary.GetValue(str3.ToLowerInvariant(), out strArray))
        stringBuilder.Append(strArray[0].ToString() + strArray[1].ToString());
}
```
GHOST BOX APPS

I evaluated 20 Android "Ghost Box" apps for signs of otherworldly existence

Many apps took less than an hour to evaluate

Obfuscated, complex applications took 4+ hours in many cases

Was this a smart use of time?

Busted: 18 apps
Plausible: 2 apps
Confirmed: 0 apps
WHAT I LEARNED

Many apps reveal their secrets with file system data

JadX is a valuable decompiler for Android app RE

- Use jadx-gui to browse decompiled sources
- Use jadx to extract APK sources to a directory, search with grep/findstr/Select-String

Android Studio is essential for obfuscated app analysis

- "Rename All Instances", "Find Usages", "Go To Declaration"
- Start small, understand little bits of code, work your way to broader understanding

Cross-platform Development requires different analysis tools

- Unity, Xamarin susceptible to .NET decompilers, PhoneGap discloses JavaScript code
HOW YOU SHOULD APPLY THIS

Start evaluating your own apps

Write your own Android app
- Something simple, like a decimal to hex converter, or hexadecimal scientific calculator
- Forces you to learn Android APIs, programming idioms; makes you a better RE

Pick a project you will have fun with
- Cheating at video games, exposing advertiser misconduct, hacking JARVIS/home automation, analyze fortune teller apps, etc.

Become a better pen tester by building skills, and put them into action.
CONCLUSION

I spent $200 on Ghost Box apps...and it was well spent

None of the apps conclusively communicate with the dead

- File system objects reveal static audio files, images
- APK reverse engineering reveals Java source and feeble trickery
- Obfuscated apps require more time, but fail with persistent analysis
- Cross-platform apps fail as well, but require different analysis tools

I didn't find any ghosts, but I'm a better analyst now than when I started.
A Haunting
RESOURCES

Destination America's A Haunting -
http://www.destinationamerica.com/tv-shows/a-haunting

Ghost Hunter App - http://tinyurl.com/lgvv3tb

Joe's Ghost Box App - http://tinyurl.com/httteu7

P-SB7 Ghost Box App - http://tinyurl.com/jqbupgs

Ghost Speaker App - http://tinyurl.com/9k7ug43

Ouija Game: Real Spirit Board App - http://tinyurl.com/jr3mp4n

JadX - https://github.com/skylot/jadx

ProGuard - https://www.guardsquare.com/proguard


JetBrains dotPeek - https://www.jetbrains.com/decompiler

Jabberwacky - http://www.jabberwacky.com

Joshua Wright

"I never met an Android app I didn't like (to break)"

@joswr1ght
jwright@hasborg.com