Whack-A-Mobile

Getting a Handle on Mobile Testing with MobiSec

Tony DeLaGrange,
& Kevin Johnson
Senior Security Consultants
info@secureideas.net
Office - 904-639-6709
Twitter - @secureideasllc

Tony DeLaGrange

- Security Consultant at Secure Ideas
- Over 25 years IT experience
  - Healthcare & Banking industries
- Focus on Mobile Security for past 7 years
- Co-Author of SEC571 Mobile Device Security
- Project Lead for the MobiSec Live Environment
- Co-Chair of the SANS Mobile Device Summit

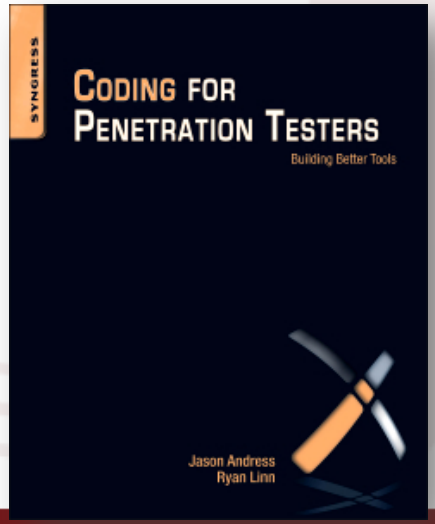
Kevin Johnson

- Security Consultant at Secure Ideas
- Author of SEC542/642/571
  - Web App PenTesting/Adv Web PenTesting/Mobile Security
- SANS Senior Instructor
- Open Source Project Lead
  - SamuraiWTF, Laudanum, Yokoso, WeaponizedFlash etc.
- Co-Chair of the SANS Mobile Device Summit

Let's Talk About...

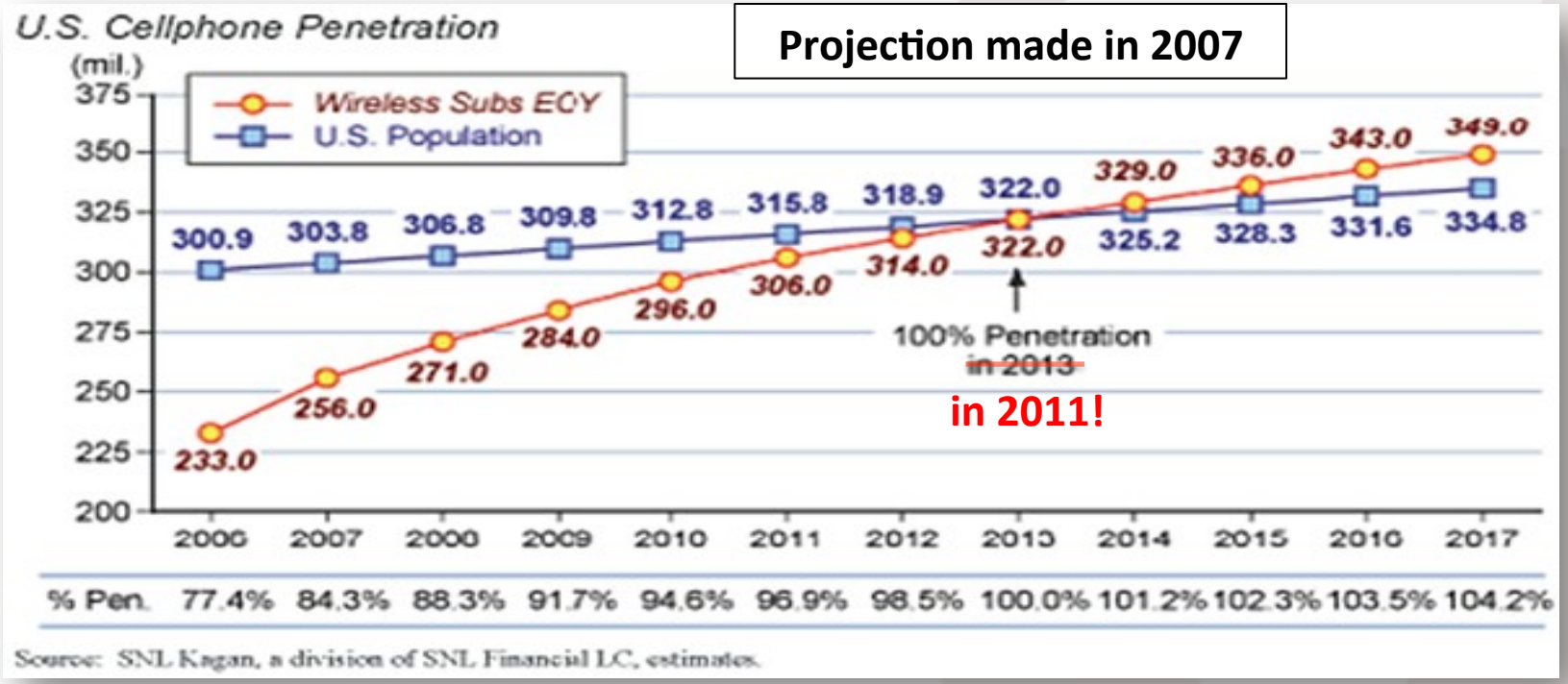
- Overview of Mobile Security Testing
- Introduce the MobiSec Live Environment
- MobiSec Structure & Testing Tools
- Leveraging the DARPA CFT Program
- OWASP Mobile Security Project
- Some really awesome people!

- But NOT PowerShell
  - Hi Chris ☺



Mobile Security Shamearity*

- Why is it important?

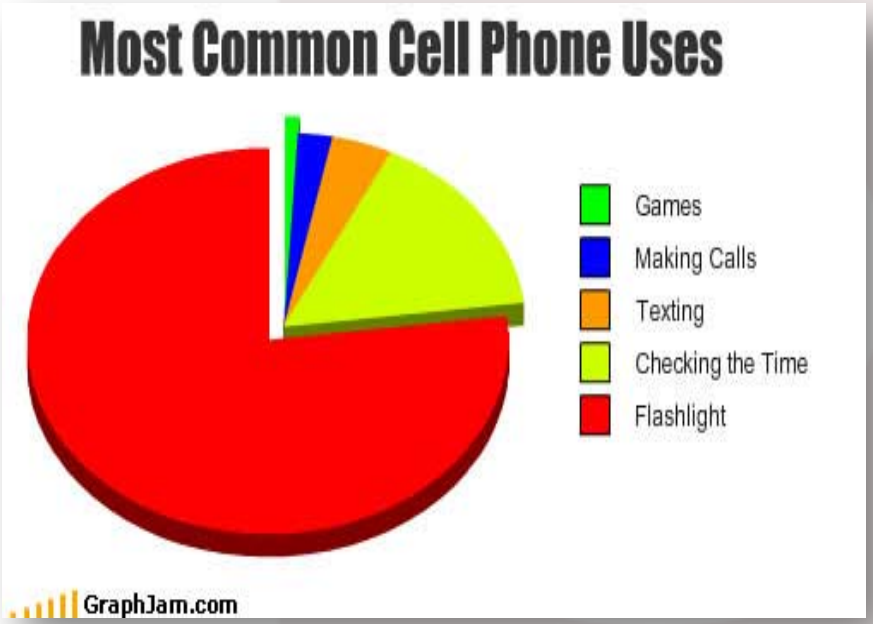


- Mobile Devices... They're EVERYWHERE!

**** Kevin and Tony both make up words!***

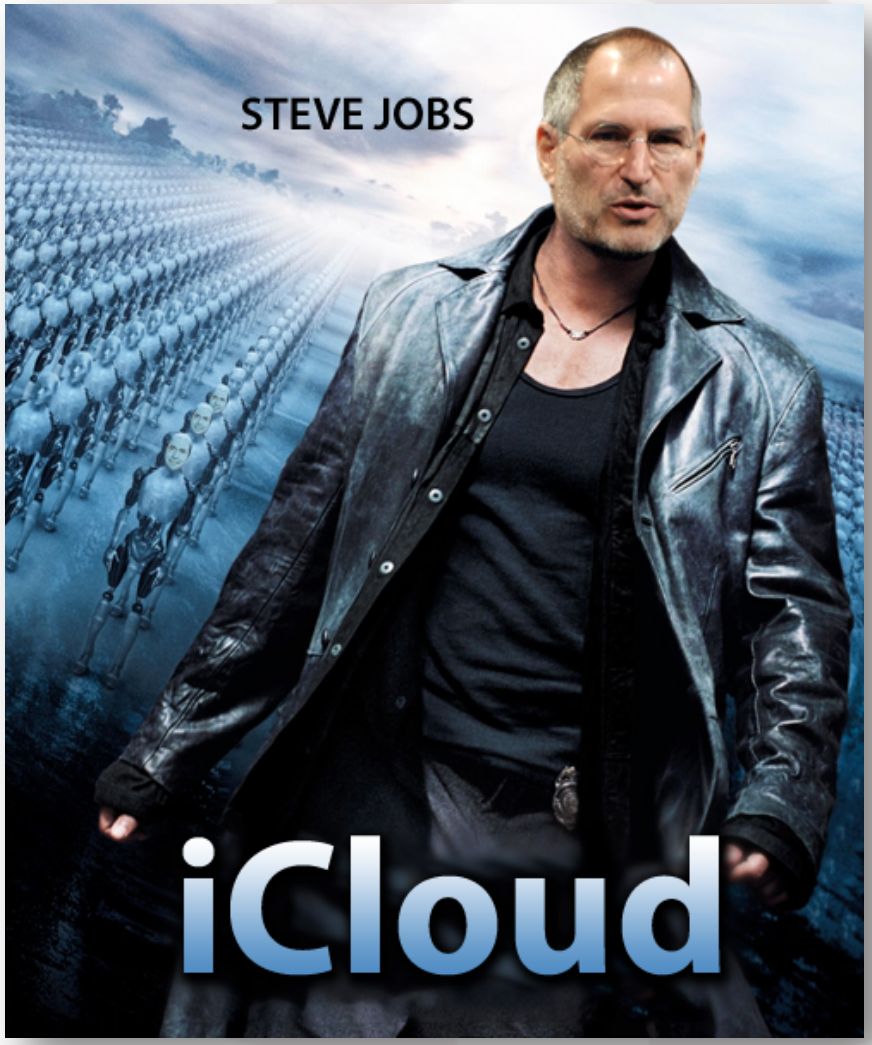
Lot's of Uses

- Increased capability, affordability, accessibility, easibility... any more abilities?
- Why do most people buy a smartphone?



Target Rich Environment

- Always On,
  Always Connected
- People have their entire lives on their mobile device
- To the Cloud!



Challenges with Mobile Testing

- Finding the "right tools" for the job

You can "roll your own" but...

- Time consuming
- Expensive from labor cost perspective
- Not always fully tested to work

Run What Ya Brung

- Anyone got a tool? Anyone?
- Use features in existing tools
- Some specific tools, but not many

- Need for affordable and robust testing tools
  - affordable = "free" / robust = "it actually works"

MobiSec Live Environment

- What is it? Why did we do this?
- Similar to
  - SamuraiWTF
  - BackTrack
- Open Source project
- Runs on Ubuntu LTS 10.04
  - we're sure you're familiar with it? ☺

So What's In It For Me?

- All the tools, none of the fat
- Everything you need, anytime you need it!

- Always improving
- Affordable!

Who Would Use This?

- IT Mobile Admins
  - Identify vulns and flaws in their mobile environment
- Security Consultants
  - Pen testing a client's mobile apps, devices, and services
- Forensics Analyst
  - Extract data from a mobile device to support an investigation

MobiSec Design Objectives

- Live testing environment on Intel computers
- Based on an OS *everyone* is familiar with
- Open source and distributable
- Structure aligned to testing methodology
- Easy to find & use tools
- Including dev kits and emulators
- Customizable
- Updateable

Constraints & Limitations

- Yeah, there are some

- Licensing and distribution restrictions
- If we can't include it, we provided info on where you can get it
- Doesn't everything run on Linux?

MobiSec Structure

- MobiSec is organized to categorize tools:
  - Development Tools
  - Device Forensics
  - Penetration Testing
  - Reverse Engineering
  - Wireless Analyzers

- Menu and directory structure
  - Similar to other testing environments you're already use to ☺

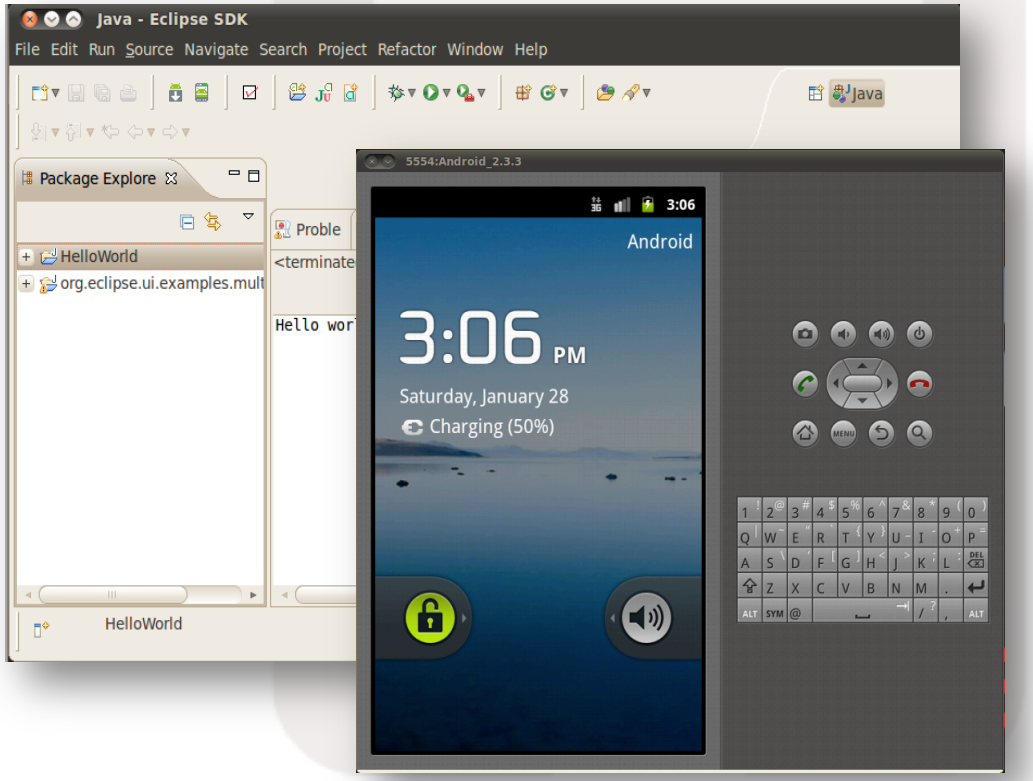
Mobile Testing Methodology

- We aligned the pen testing tools to a well known pen testing methodology
  - ✧ Reconnaissance
  - ✧ Mapping
  - ✧ Discovery
  - ✧ Exploitation

- If you're not using a testing methodology, then adopt a good one and USE IT!

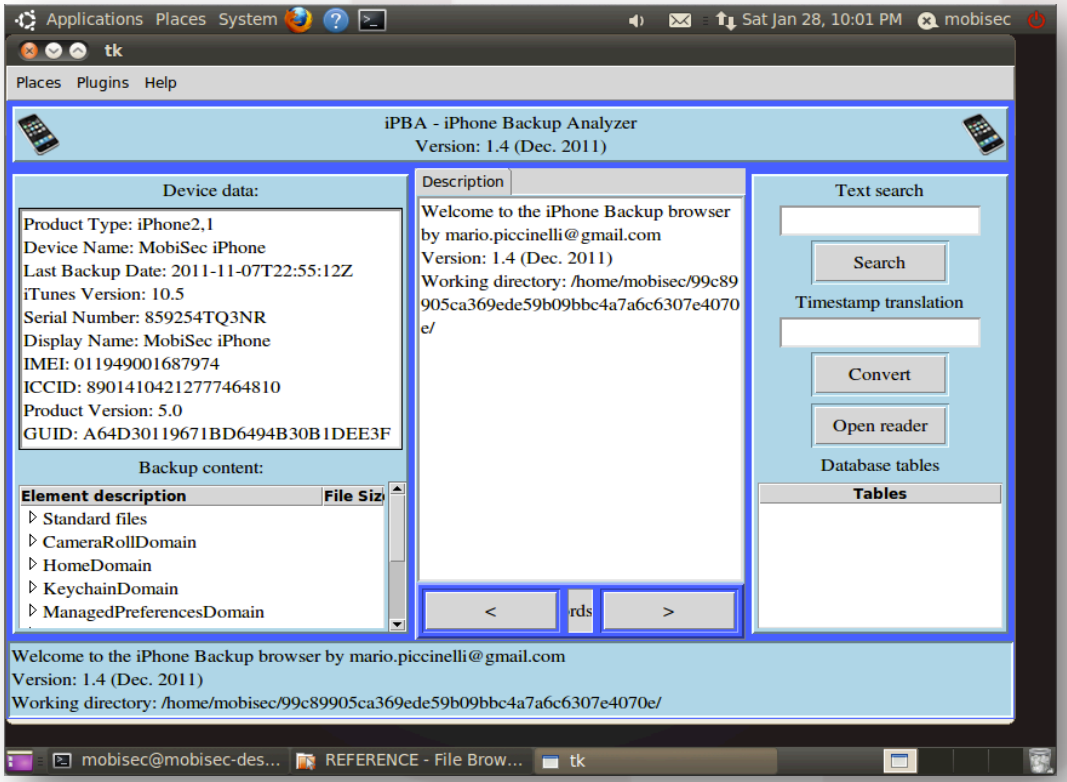
Development Tools

- Includes mobile device development environments, emulators and simulators
  - Android SDK
  - Android Emulators
  - Eclipse IDE



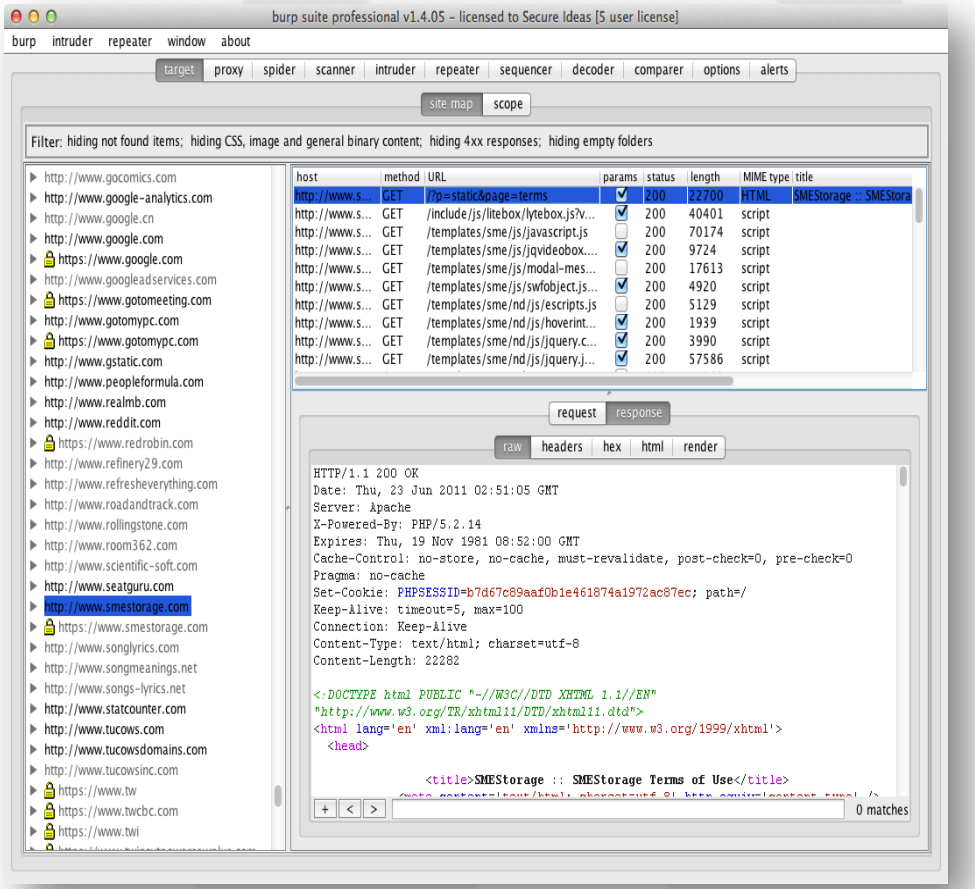
Forensics Tools

- Includes tools that provide the ability to perform forensics on mobile devices
  - BitPim
  - Foremost
  - iPhone Backup Analyzer
  - The Sleuth Kit



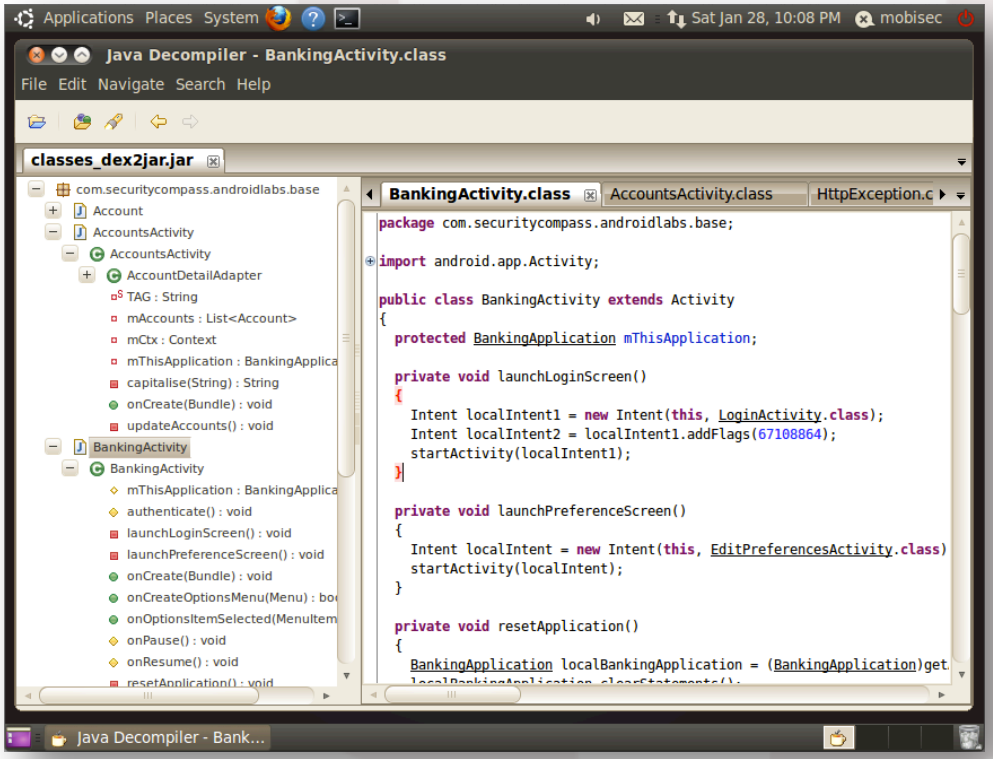
Penetration Testing Tools

- Reconnaissance
  - Maltego CE, SEAT
- Mapping
  - CeWL, DirBuster, Fierce, Nikto, nmap
- Discovery
  - Burp, Mallory, Spike, w3af, ZAP
- Exploitation
  - BeEF, Metasploit, SET



Reverse Engineering Tools

- Includes tools used for performing reverse engineering of mobile apps
  - APK Tool
  - Dex2Jar
  - Flawfinder
  - Java Decompiler
  - Strace



Wireless Analysis Tools

- Drivers and wireless tools for capturing and analyzing wireless traffic
  - Kismet
  - Ubertooth
  - Wireshark

MobiSec Build

- Run as Live Environment from DVD/USB/VM
- Hardware or VM Settings Specs:
  - Single 32-bit processor / Two processors preferred
  - 1GB Memory / More is preferred
  - 15GB HD / More if you want to customize
  - USB (for Ubertooth)
  - 802.11 (for WiFi analysis)
- Available in Feb at: http://mobisec.secureideas.net

DARPA CFT Program

- Great program that supports small cyber projects with focus of short time frames
- Secure Ideas turned to DARPA CFT to help fund the MobiSec Live Environment project
- Did you miss the talk on the DARPA CFT Program by Mudge?
  - Go to www.cft.usma.edu for more info

- The OWASP Mobile Security project was announced in Q3 2010
  - Currently very active
- It is geared toward providing resources for developers and security teams
  - Tools, guidelines and standards
- The project is lead by Jack Mannino
  - https://www.owasp.org/index.php/OWASP_Mobile_Security_Project
- Plan is to move MobiSec under this project
  - This is only the beginning!!!

Really Big THANK YOU

- Thanks to Mudge @ DARPA and the guys at Bit Systems
- Thanks to Chris Cuevas and Shawn Merdinger for all their help on MobiSec
- And a really big thank you and shout outs to all the developers of open source tools!
- And of course John Sawyer


Applications Places System
Sat Jan 28, 8:46 PM
mobisec
MOBISEC