Introducing the Smartphone Pentesting Framework

Georgia Weidman
Bulb Security LLC

Approved for Public Release, Distribution Unlimited

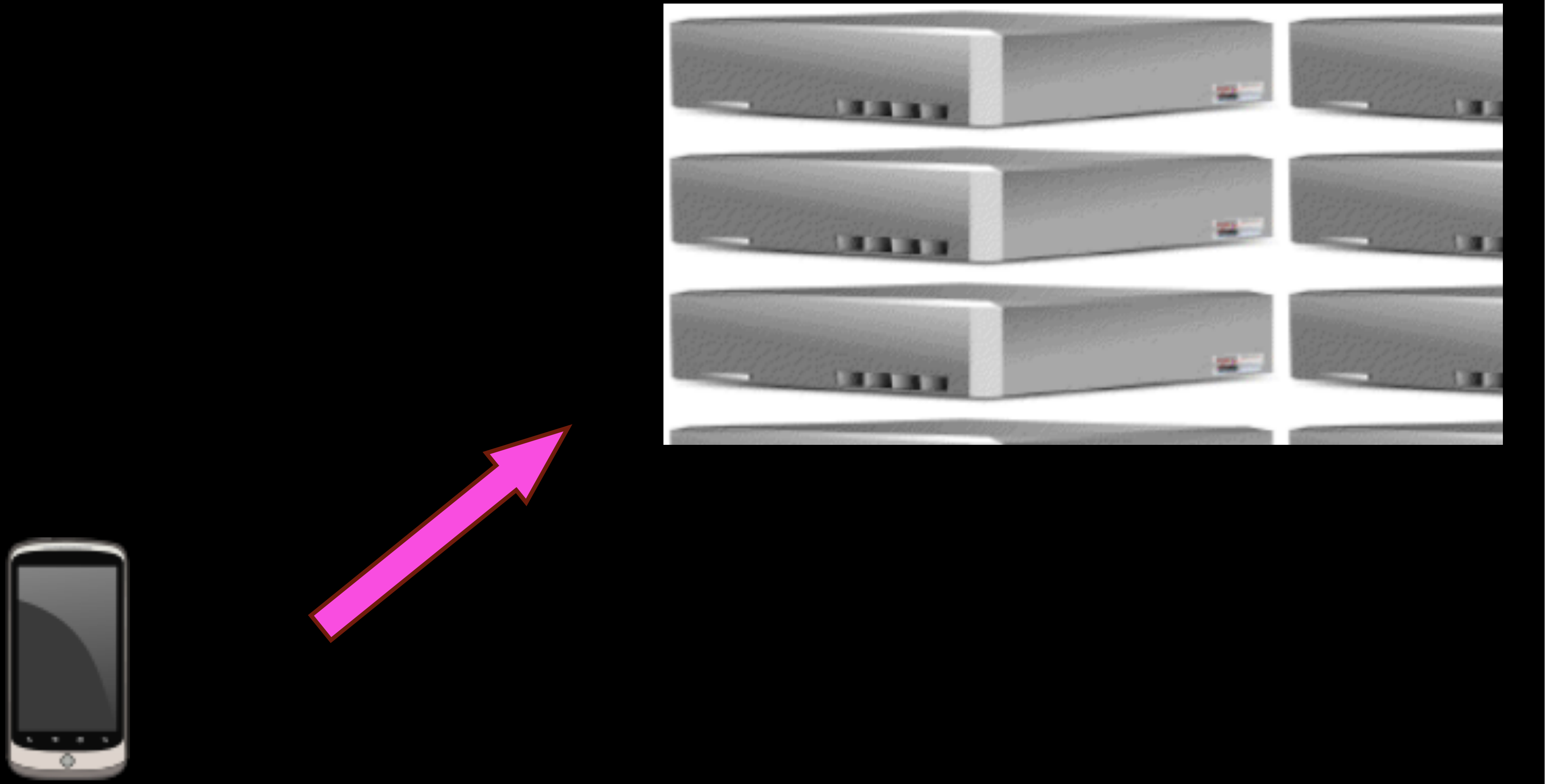
Disclaimer

“The views expressed are those of the author and do not reflect the official policy or position of the Department of Defense or the U.S. Government.” This is in accordance with DoDI 5230.29, January 8, 2009.

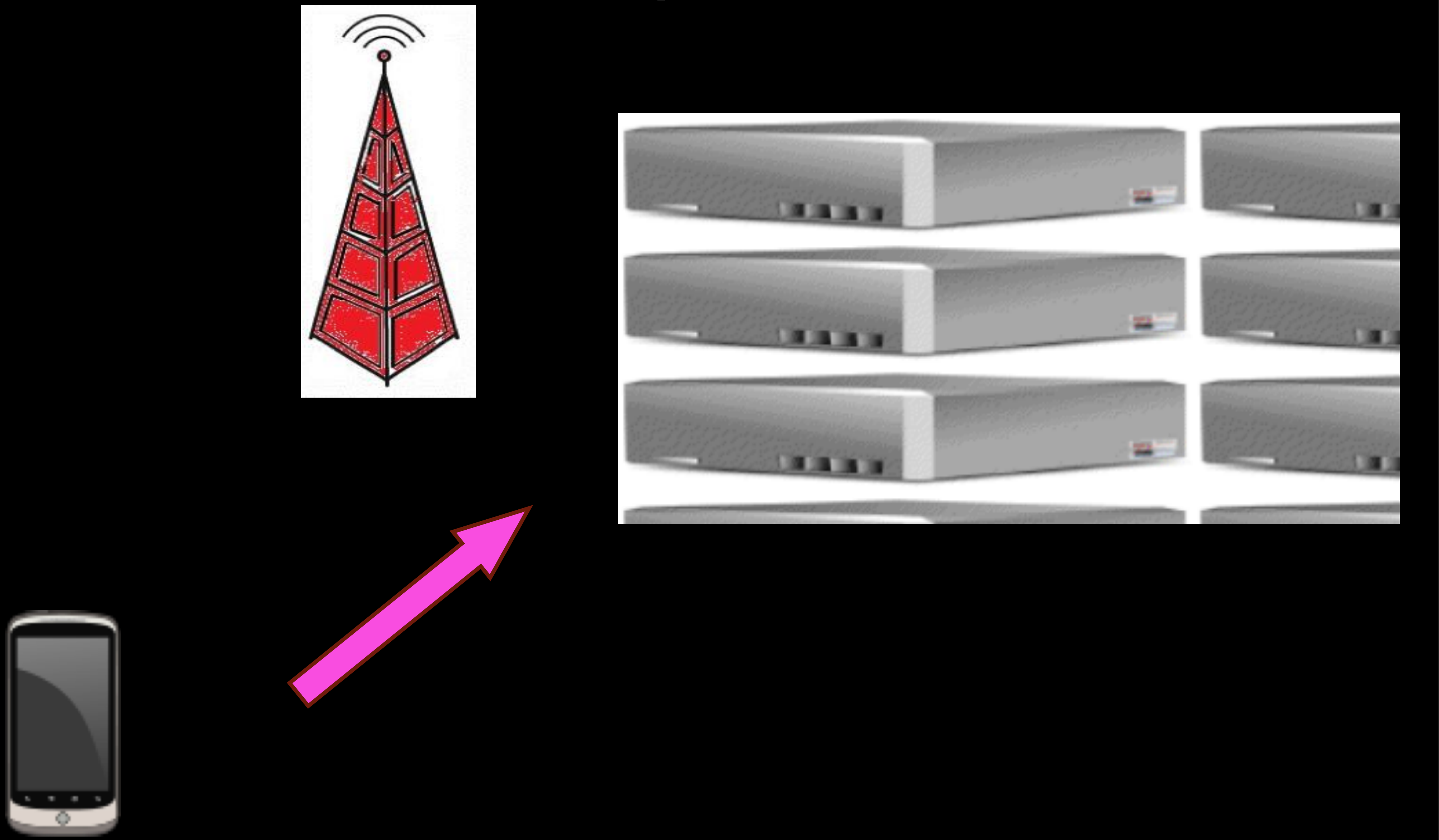
<3 to DARPA

- DARPA Cyber Fast Track program funded this project
- Without them I'd still be a junior pentester at some company
- Now I'm CEO!
- <3 <3 <3 <3 <3

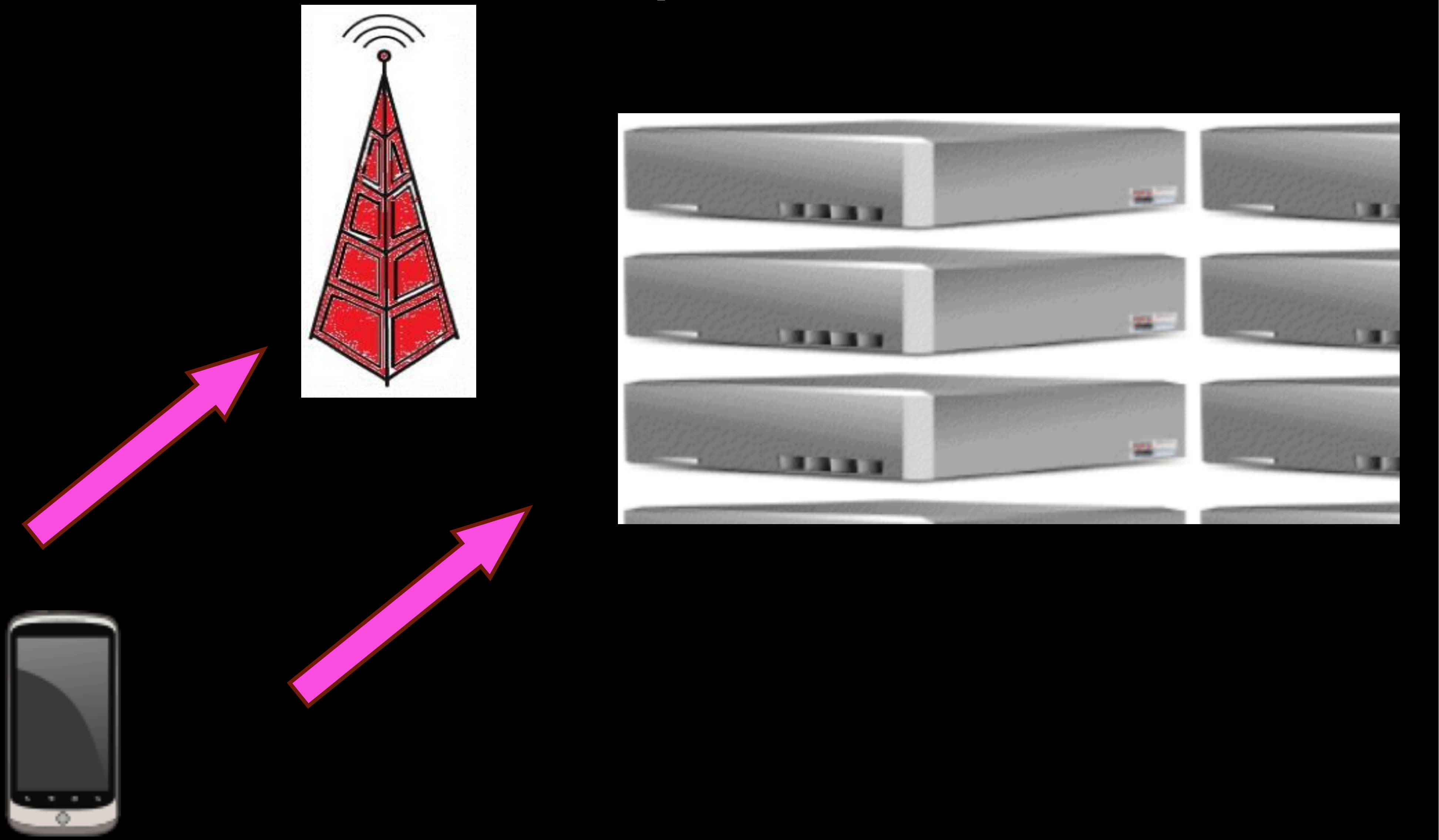
The Problem: Smartphones in the Workplace



The Problem: Smartphones in the Workplace



The Problem: Smartphones in the Workplace



Smartphones in the workplace

- Access your data
- Store company emails
- Connect to VPNs
- Generate 1 time passwords

Threats against smartphones: Apps

- Malicious apps steal your data, remotely control your phone, etc.
- Happens on all platforms. Some easier than others.
- If your employees have a malicious angry birds add-on what is it doing with your data?

Threats against smartphones: software bugs

- Browsers have bugs
- Apps have bugs
- Kernels have bugs
- Malicious apps, webpages, etc. can exploit these and gain access to data

Threats against smartphones: social engineering

- Users can be tricked into opening malicious links
- Downloading malicious apps

Threats against smartphones: jailbreaking

- Smartphones can be jailbroken
- Giving a program expressed permission to exploit your phone
- Once it is exploited, what else does the jailbreaking program do?

The Question

A client wants to know if the environment is secure

I as a pentester am charged with finding out

There are smartphones in the environment

How to I assess the threat of these smartphones?

What's out there now?

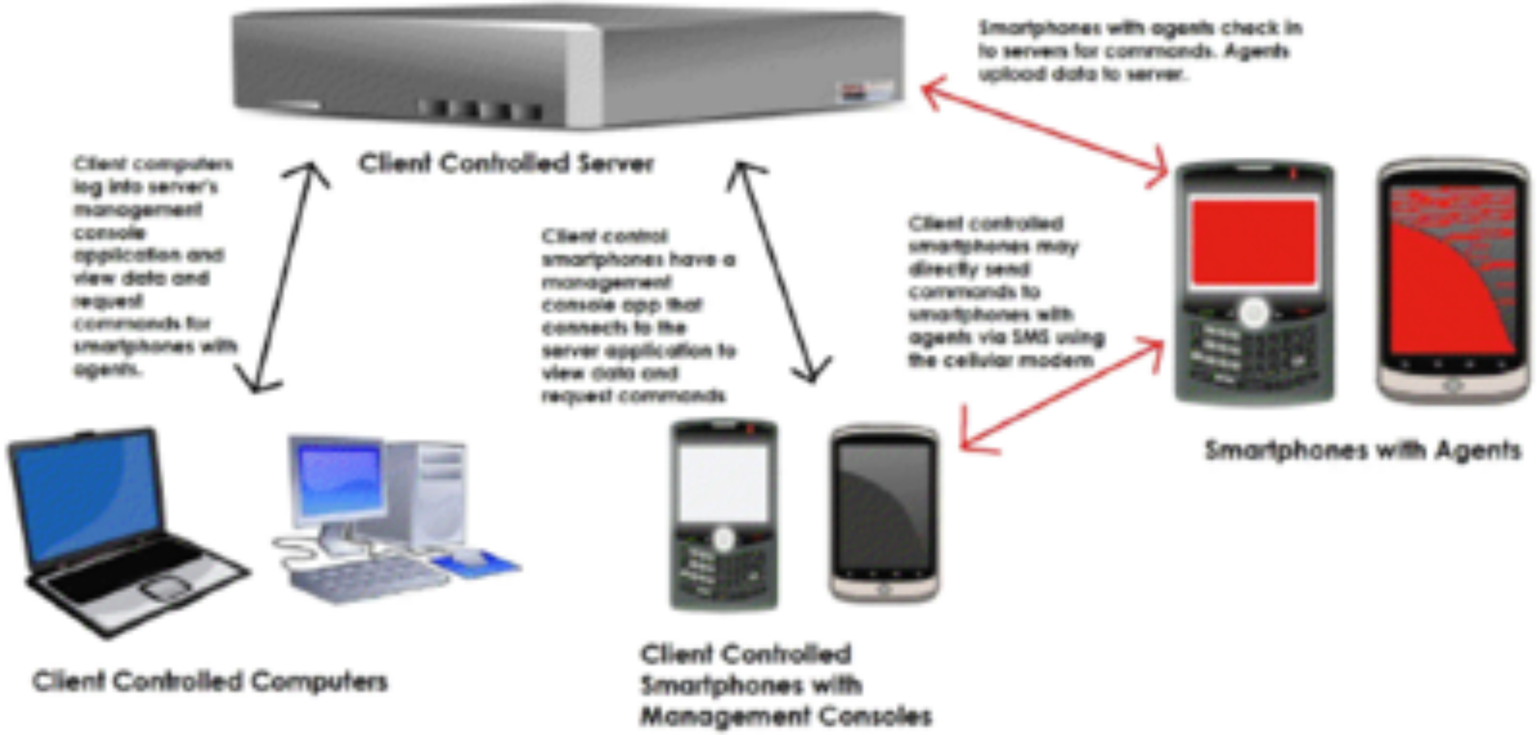
Pentesting from Smartphones: zAnti

Smartphone tool live cds: MobiSec (another DARPA project)

Pentesting smartphone apps: Mercury

Pentesting smartphone devices: ??

Structure of the framework


Client Controlled Server
Client Controlled Computers
Client Controlled Smartphones with Management Consoles
Smartphones with Agents

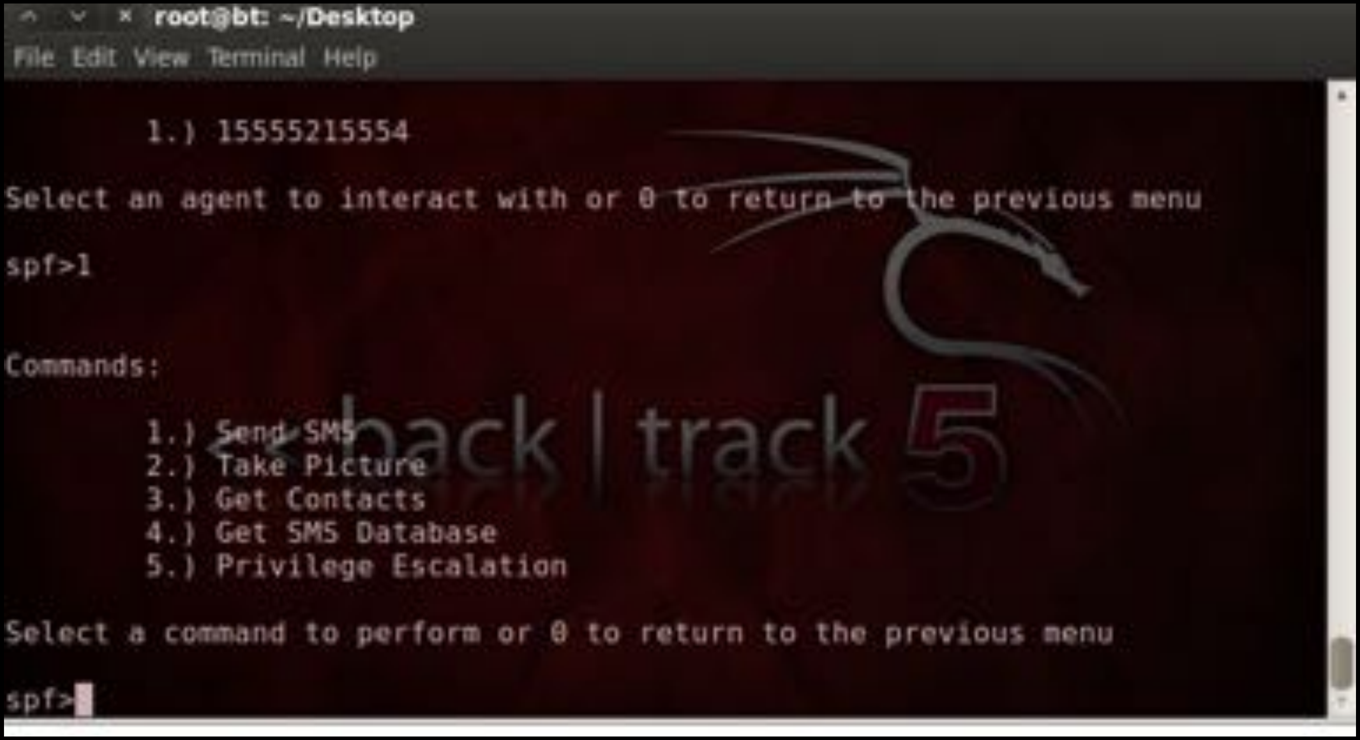
Client computers log into server's management console application and view data and request commands for smartphones with agents.

Client control smartphones have a management console app that connects to the server application to view data and request commands

Smartphones with agents check in to servers for commands. Agents upload data to server.

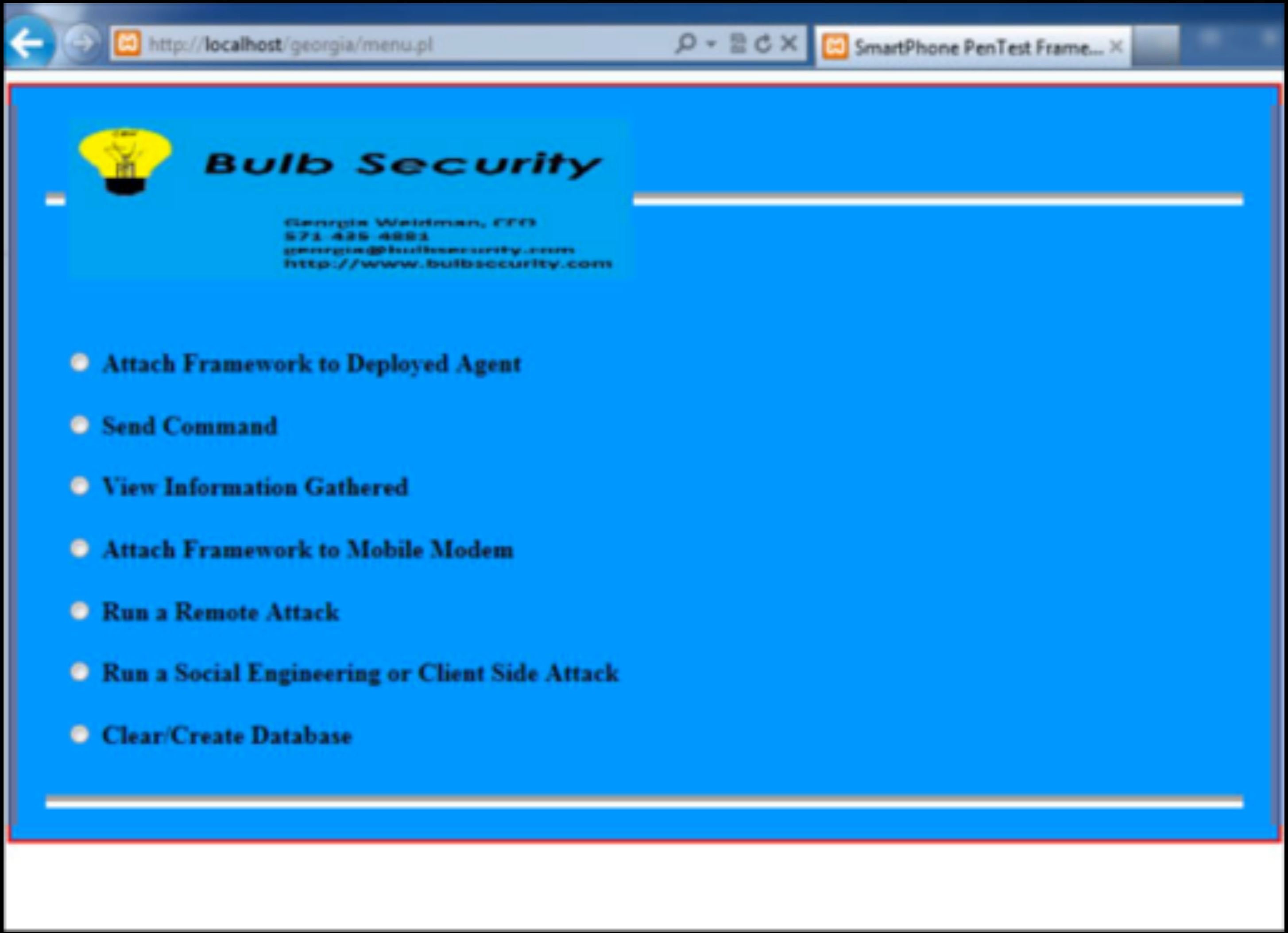
Client controlled smartphones may directly send commands to smartphones with agents via SMS using the cellular modem

Framework console



```
        1.) 15555215554

Select an agent to interact with or 0 to return to the previous menu

spf>1


Commands:

        1.) Send SMS
        2.) Take Picture
        3.) Get Contacts
        4.) Get SMS Database
        5.) Privilege Escalation

Select a command to perform or 0 to return to the previous menu

spf>
```

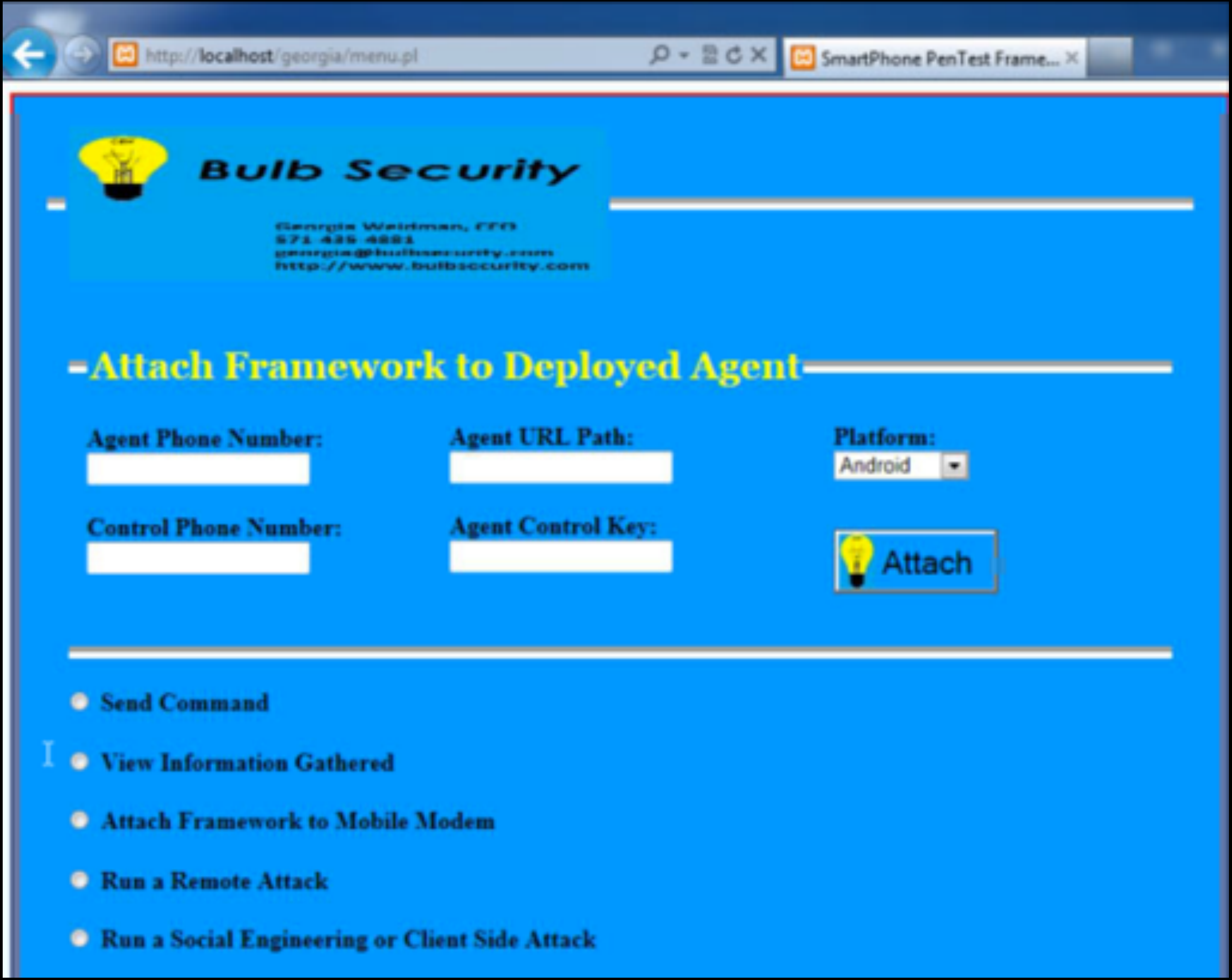
Framework GUI



Georgia Weidman, CEO
571 435 4881
georgia@bulbsecurity.com
http://www.bulbsecurity.com

- Attach Framework to Deployed Agent
- Send Command
- View Information Gathered
- Attach Framework to Mobile Modem
- Run a Remote Attack
- Run a Social Engineering or Client Side Attack
- Clear/Create Database

Framework GUI



Bulb Security

Georgia Weidman, CEO
571 435 4881
georgia@bulbsecurity.com
http://www.bulbsecurity.com

Attach Framework to Deployed Agent

Agent Phone Number:

Agent URL Path:

Platform: Android

Control Phone Number:

Agent Control Key:

○ Send Command

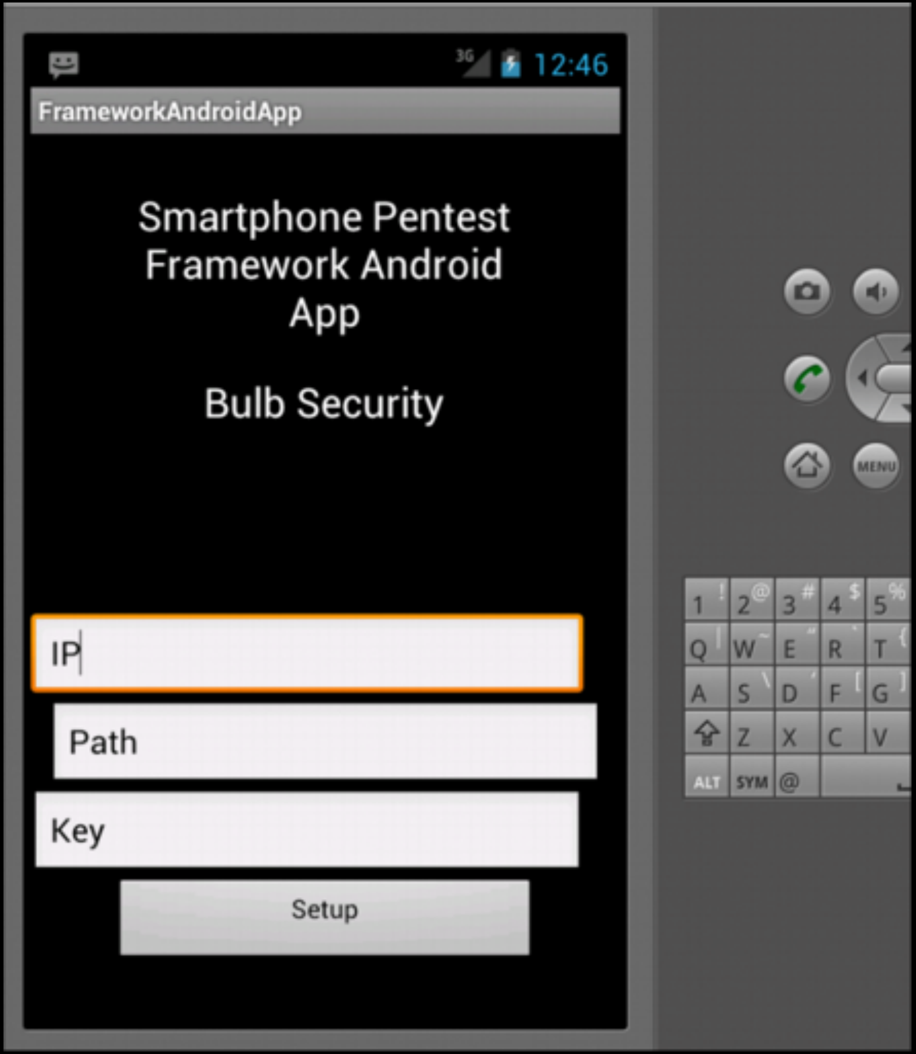
○ View Information Gathered

○ Attach Framework to Mobile Modem

○ Run a Remote Attack

○ Run a Social Engineering or Client Side Attack

Framework Smartphone App



Smartphone Pentest Framework Android App

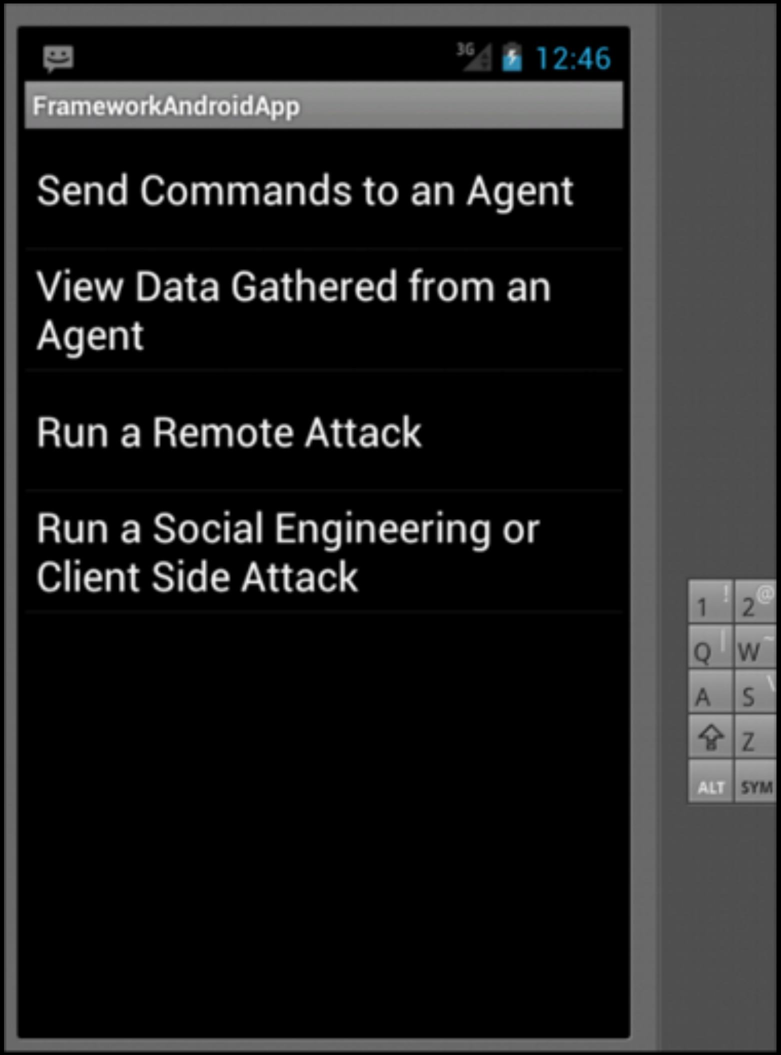
Bulb Security

IP

Path

Key

Framework Smartphone App



12:46

FrameworkAndroidApp

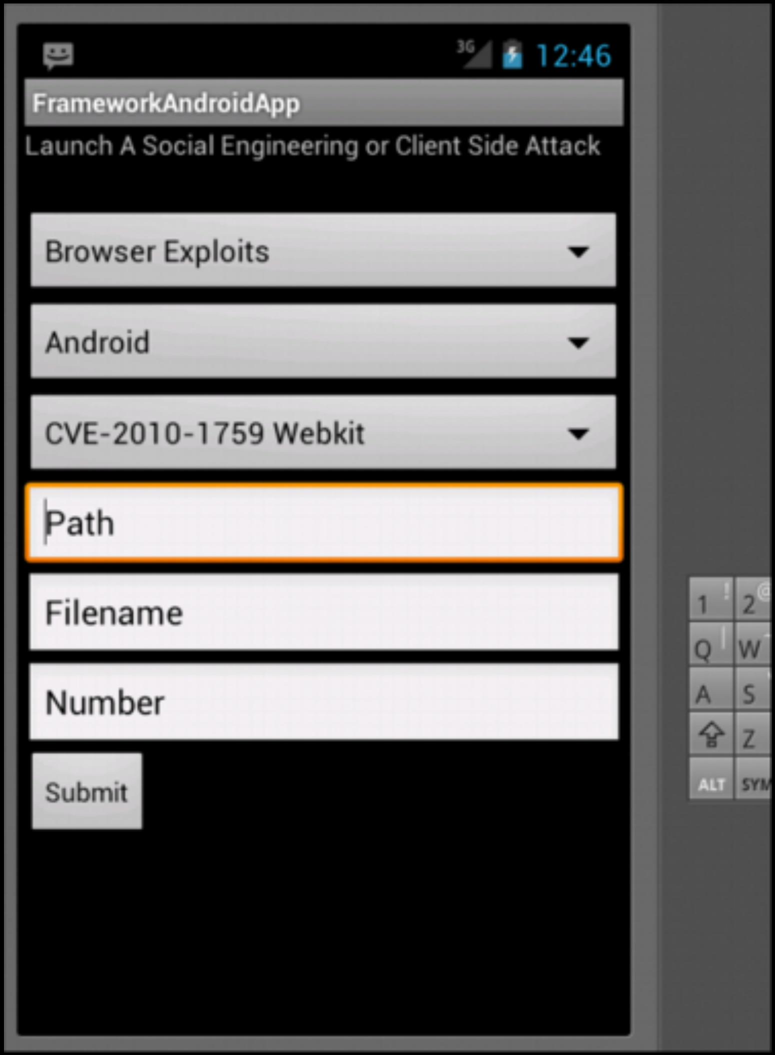
Send Commands to an Agent

View Data Gathered from an Agent

Run a Remote Attack

Run a Social Engineering or Client Side Attack

Framework Smartphone App



FrameworkAndroidApp

Launch A Social Engineering or Client Side Attack

Browser Exploits

Android

CVE-2010-1759 Webkit

Path

Filename

Number

What you can test for

Remote vulnerabilities

Client side vulnerabilities

Social engineering

Local vulnerabilities

Remote Vulnerability Example

Jailbroken iPhones all have the same default SSH password

How many jailbroken iPhones have the default SSH password (anyone can log in as root)?

Client Side Vulnerability Example

Smartphone browsers, etc. are subject to vulnerabilities

If your users surf to a malicious page their browsers may be exploited

Are the smartphone browsers in your organization vulnerable to browser exploits?

Social Engineering Vulnerability Example

SMS is the new email for spam/phishing attacks

“Open this website” “Download this app”

Will your users click on links in text messages?

Will they download apps from 3rd parties?

Local Vulnerability Example

Smartphones have kernel vulnerabilities

Used my jailbreaks and malicious apps

Are the smartphones in your organization subject to local privilege escalation vulnerabilities?

Post exploitation

Command shell

App based agent

Payloads: information gathering
local privilege escalation
remote control

Demos!

- Using the console
- Using the GUI
- Using the app
- Using an agent
- Using a shell
- Remote test
- Client side test
- Local test

Future of the Project

- More modules in each category
- More post exploitation options
- Continued integration with Metasploit and other tools
- Community driven features
- More reporting capabilities

Contact

Georgia Weidman

Bulb Security, LLC

georgia @ bulbsecurity.com

georgiaweidman.com bulbsecurity.com

@georgiaweidman