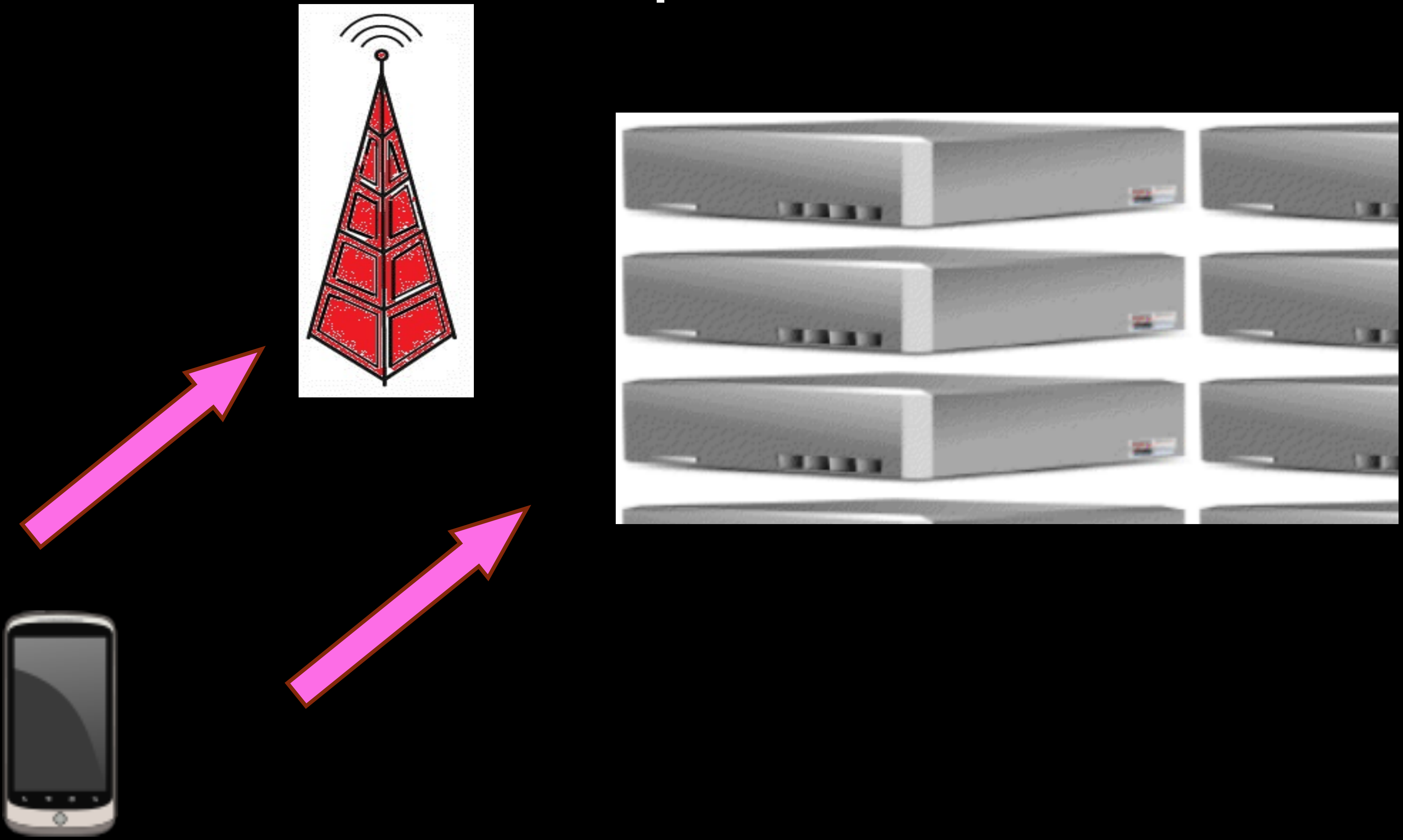
<3 to DARPA

- 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 Question

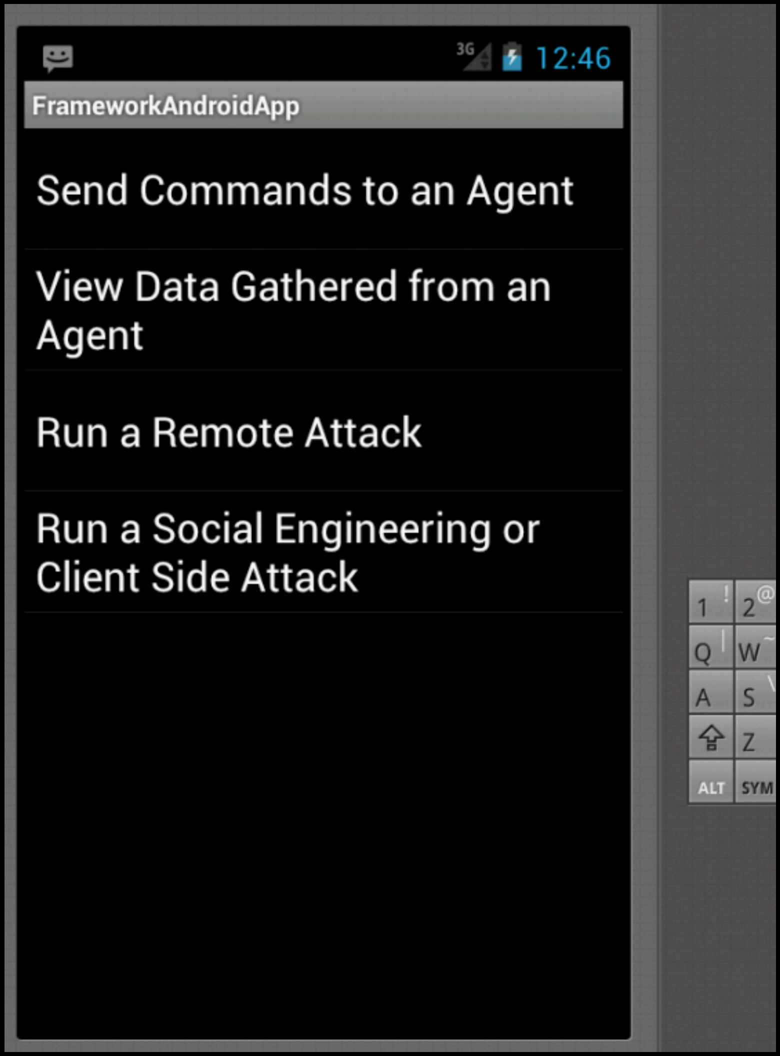
A client wants to know if the environment is secure

I as a pentester am charged with finding out

There are smartphones in the environment

How to I assess the threat of these smartphones?

Framework Smartphone App



FrameworkAndroidApp

Send Commands to an Agent

View Data Gathered from an Agent

Run a Remote Attack

Run a Social Engineering or Client Side Attack

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