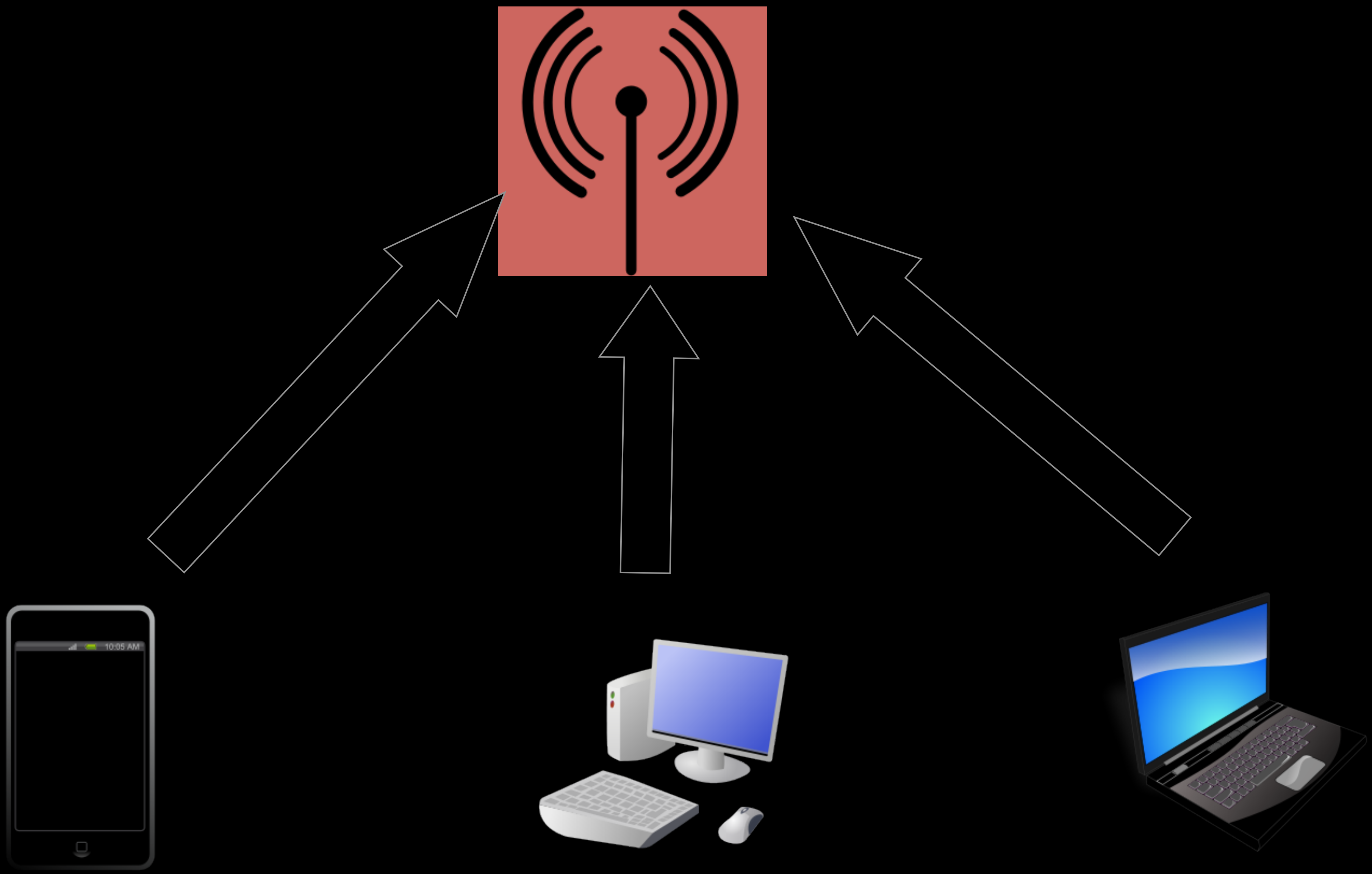
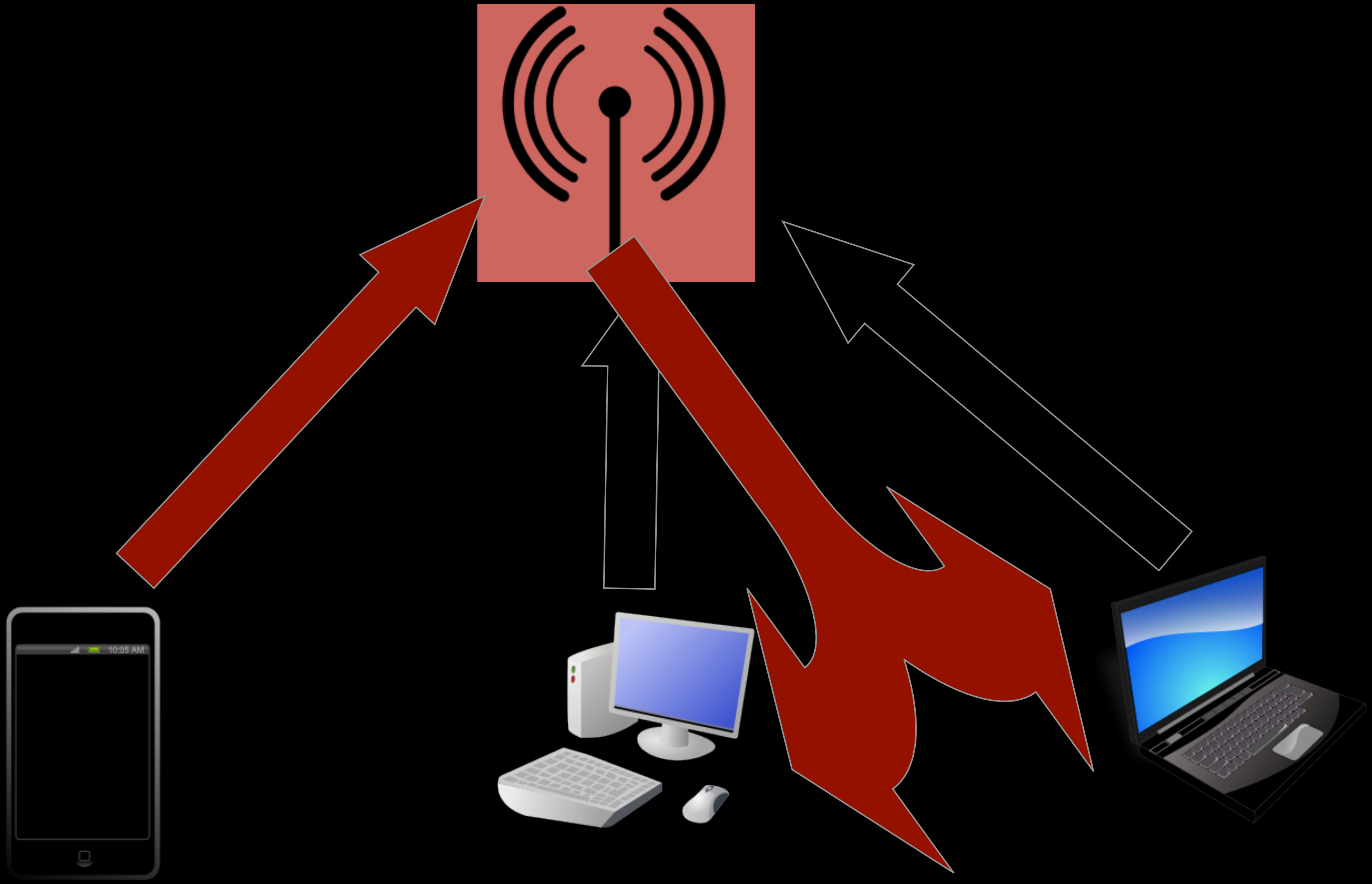
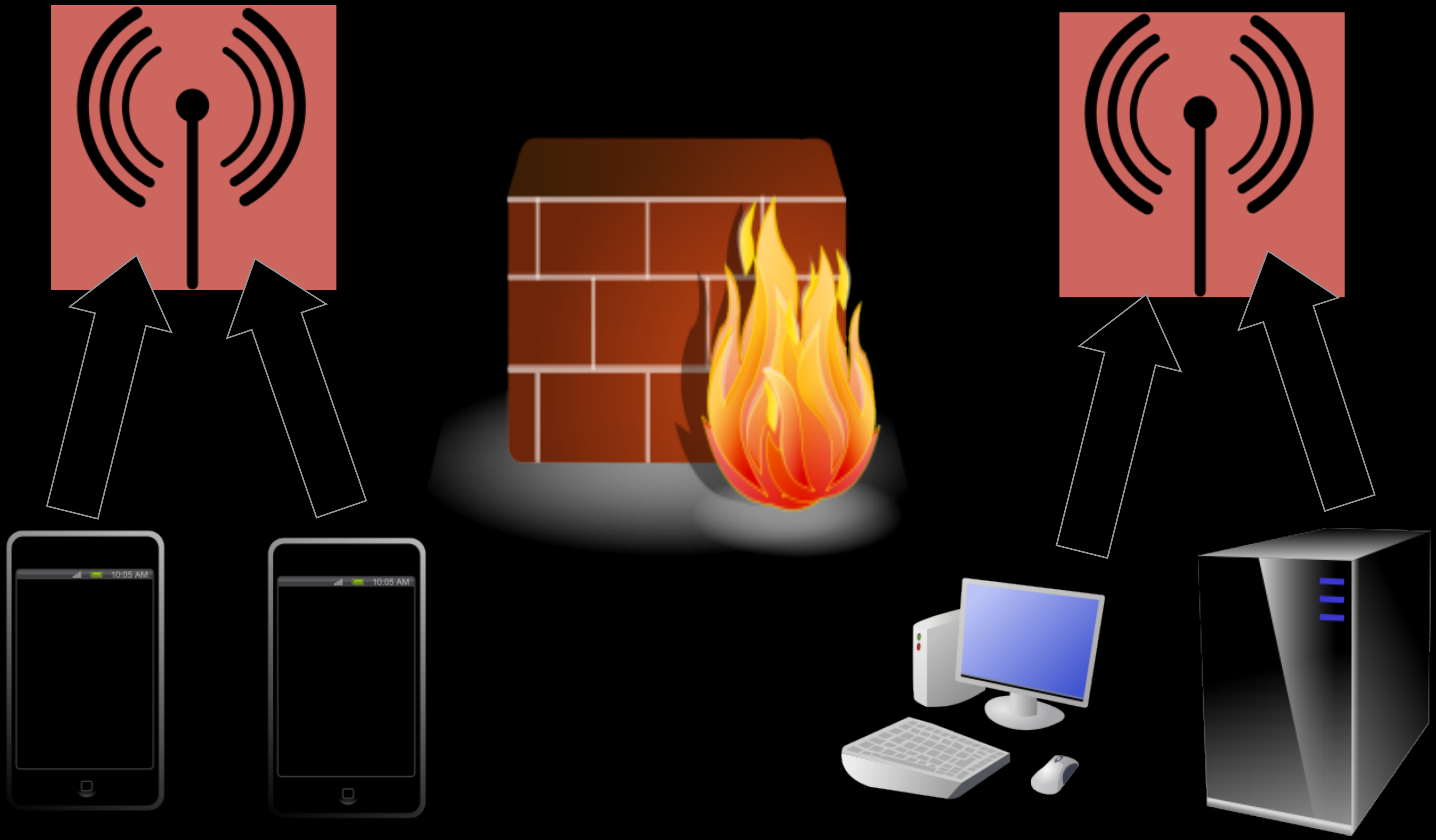
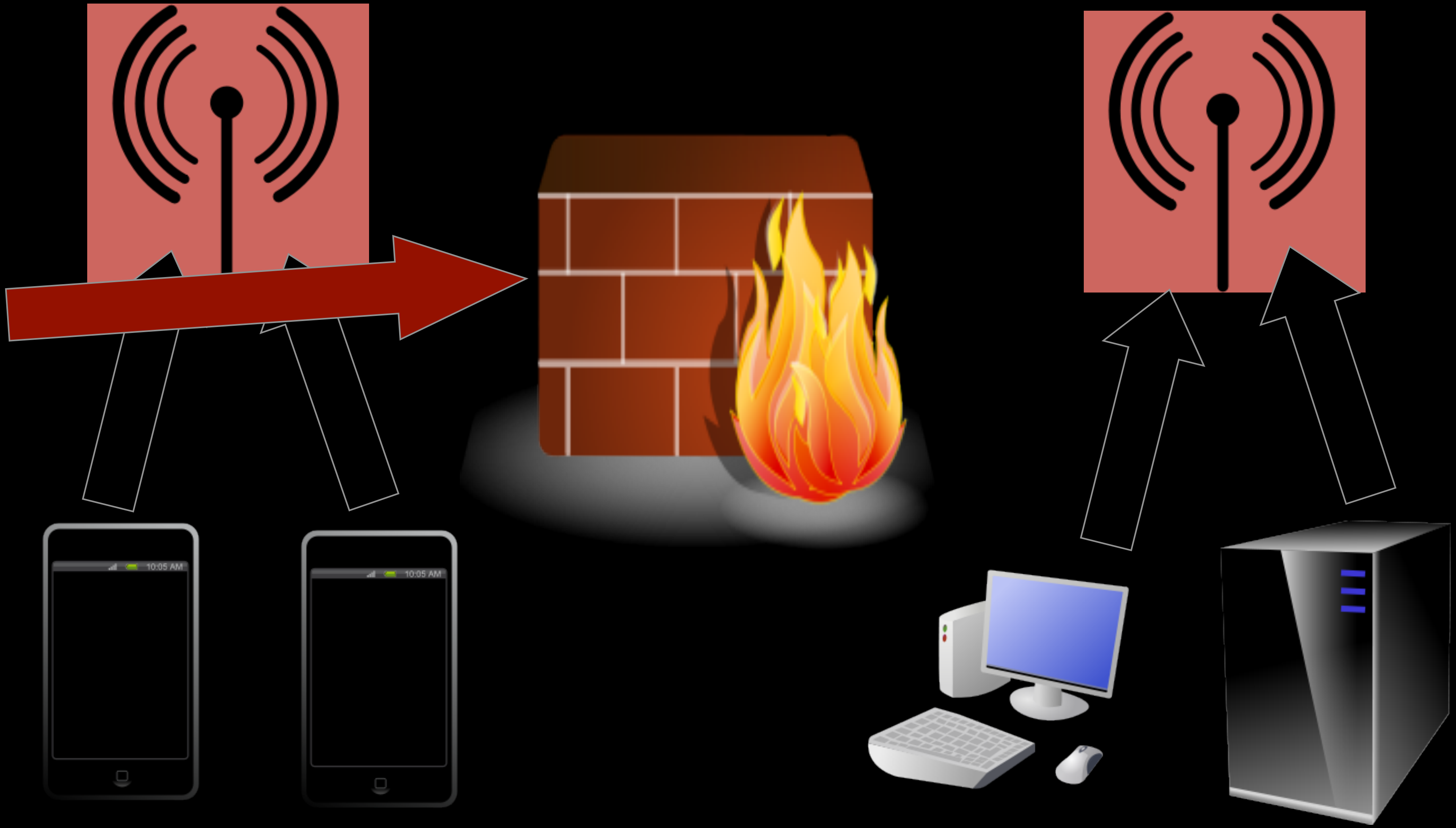
Leveraging Mobile Devices on Pentests

Georgia Weidman
Bulb Security LLC

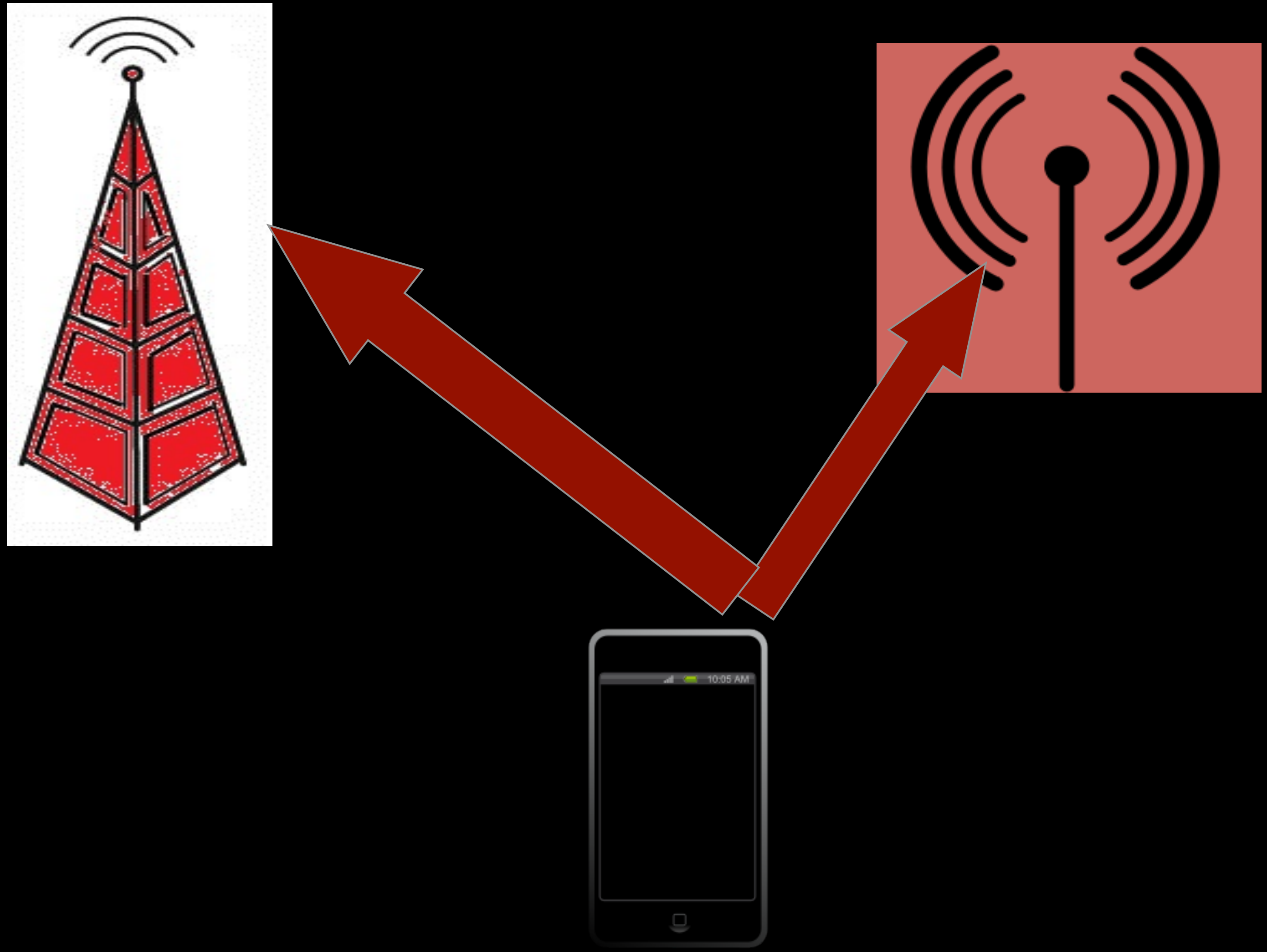

10:05 AM


10:05 AM

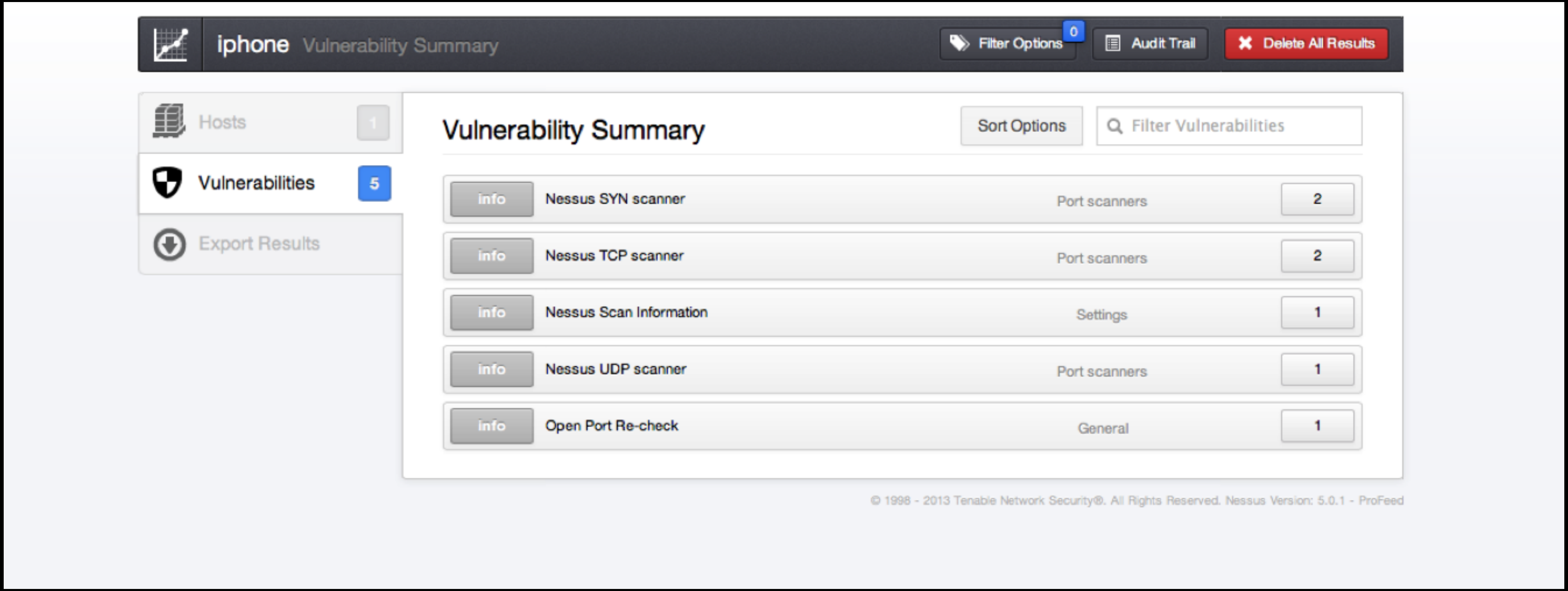

10:05 AM
10:05 AM


10:05 AM
10:05 AM

BYOD Is Not New


10:05 AM

Traditional Vulnerability Scanning



Vulnerability Summary

info	Nessus SYN scanner	Port scanners	2
info	Nessus TCP scanner	Port scanners	2
info	Nessus Scan Information	Settings	1
info	Nessus UDP scanner	Port scanners	1
info	Open Port Re-check	General	1

The iPhone in Question Is…

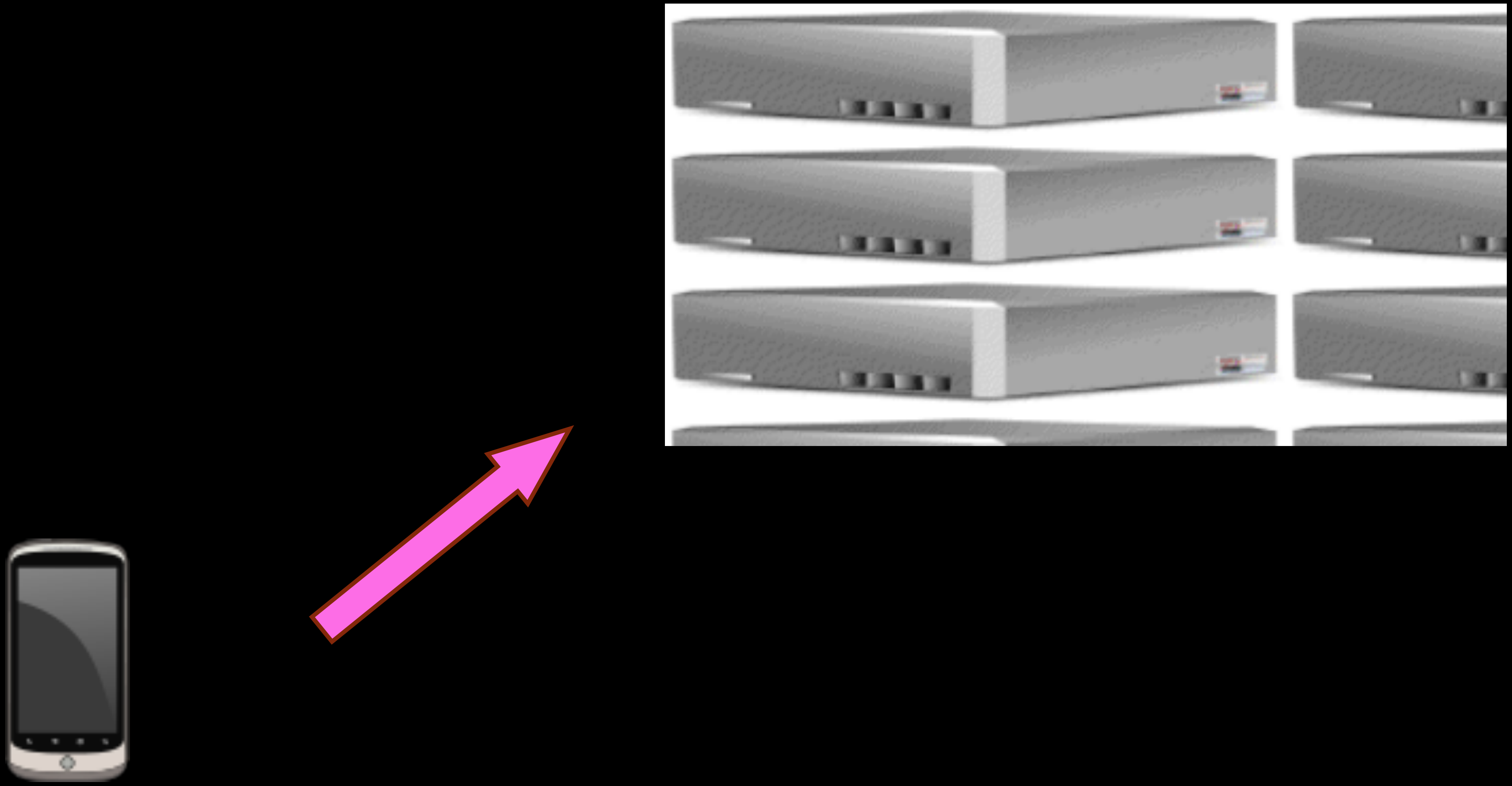
Jailbroken

Has SSH installed

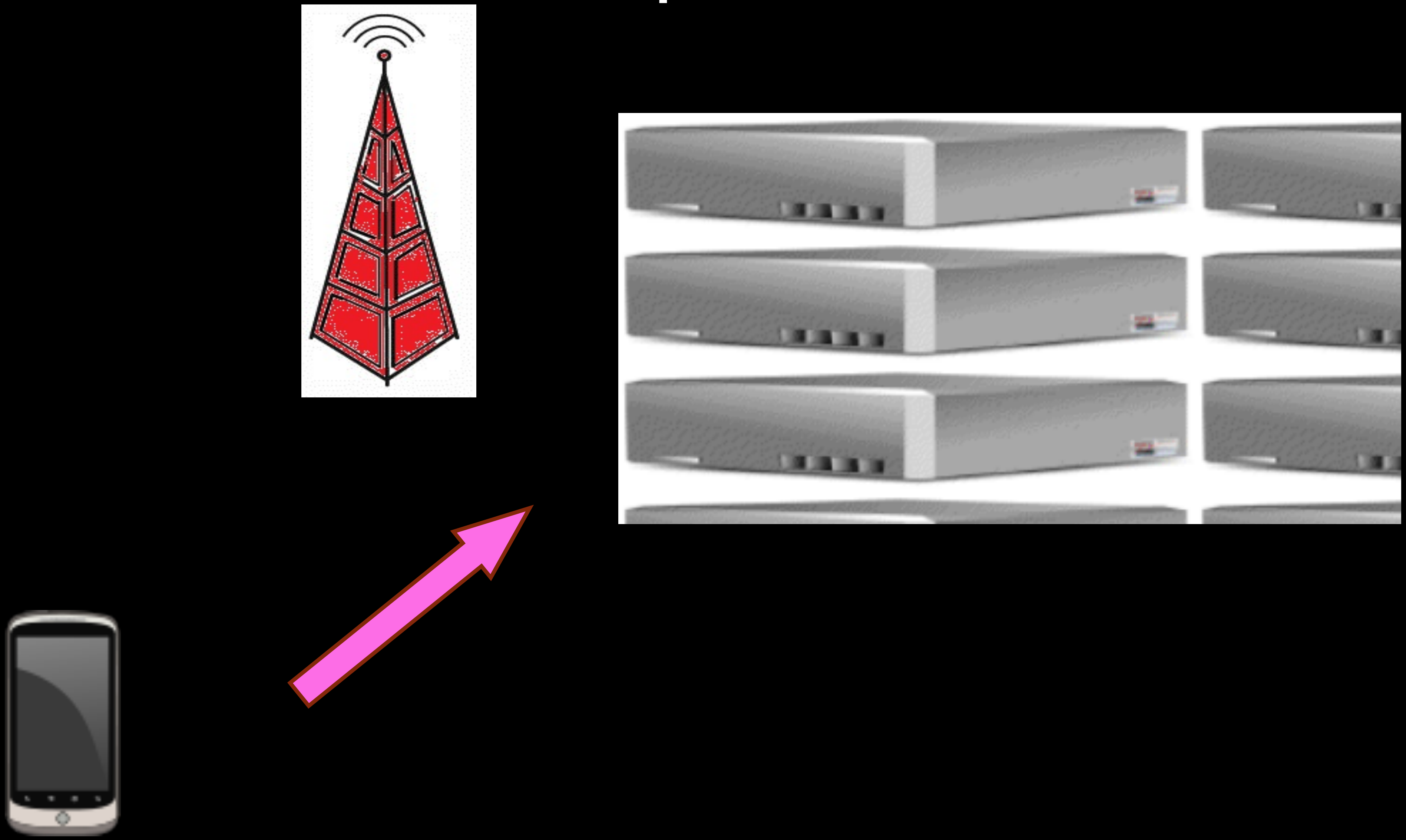
Has a default password

Is not subject to any MDM restrictions

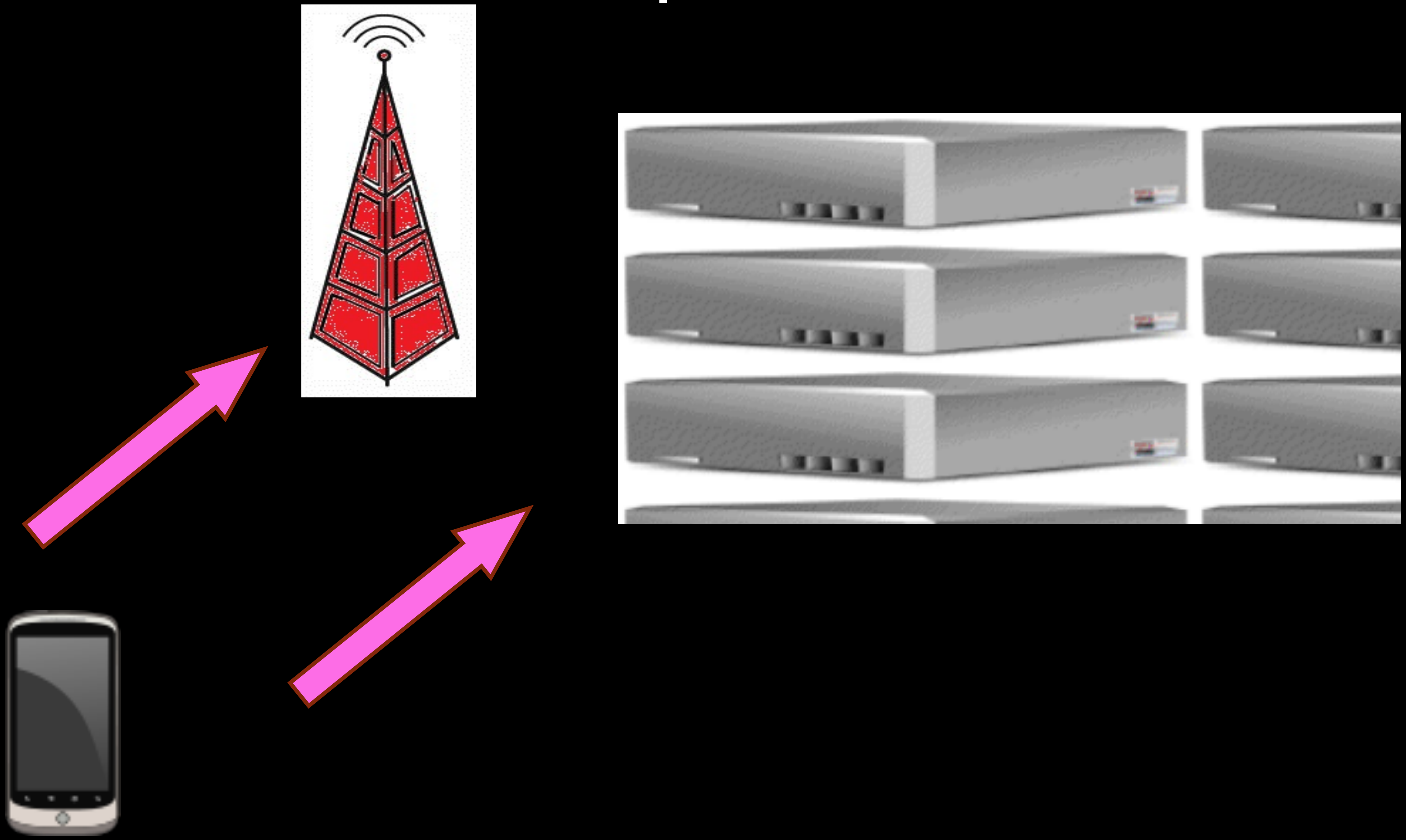
The Problem: Smartphones in the Workplace



The Problem: Smartphones in the Workplace



The Problem: Smartphones in the Workplace



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?

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

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 you can test for

Remote vulnerabilities

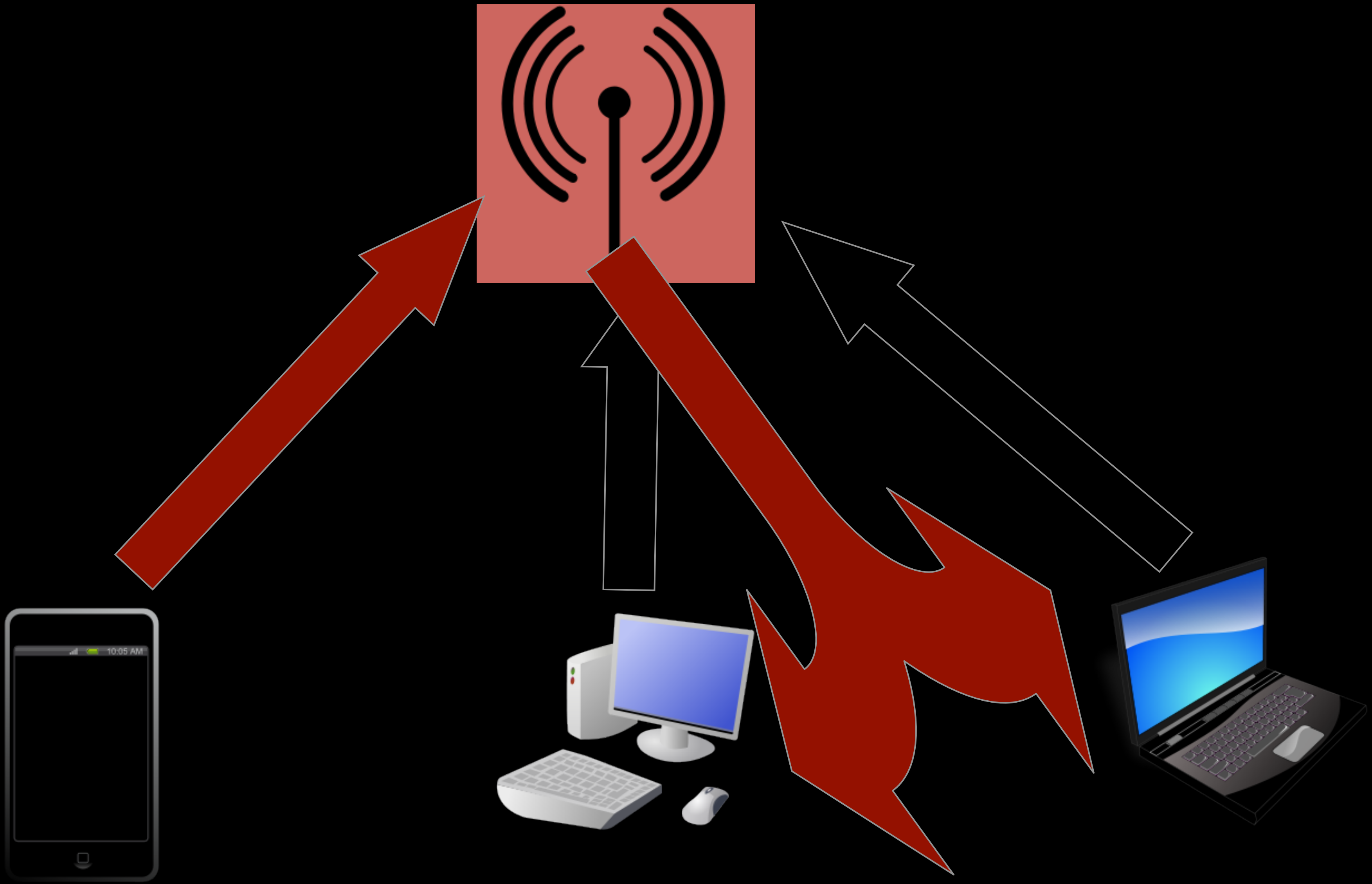
Client side vulnerabilities

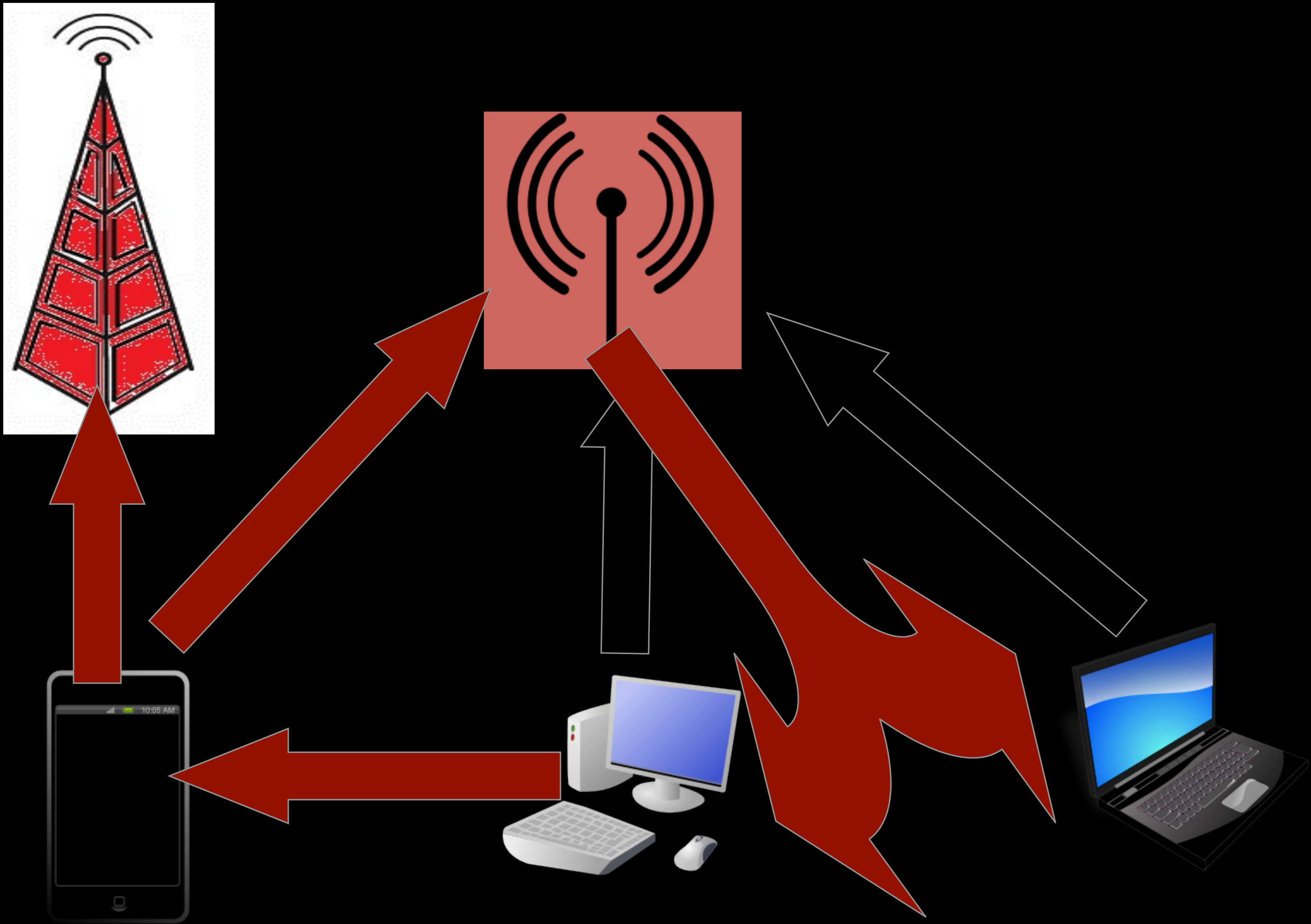
Social engineering

Local vulnerabilities

The Other Question

Once I get on your device, what else can I see?


10:05 AM


10:05 AM

Demos!

- Using SPF
- Getting on a device
- Scanning an internal asset from a compromised phone
- Exploiting an internal asset from a compromised phone

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

<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

Contact

Georgia Weidman

Bulb Security, LLC

georgia @ bulbsecurity.com

georgiaweidman.com bulbsecurity.com

@georgiaweidman