Penetration testing using mobile devices

Emerging Researcher Symposium

Presented by: Siyabonga Shelembe

Date: 10 October 2012

our future through science

Introduction

Purpose :

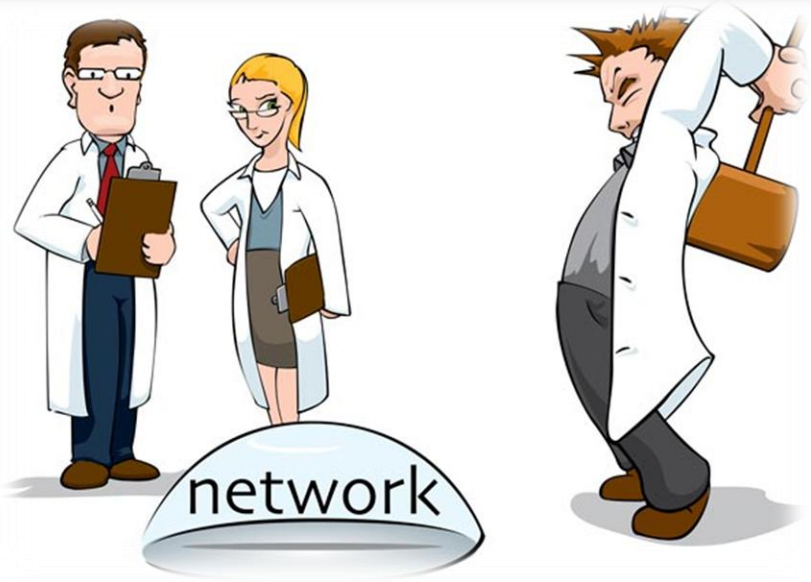
- To investigate the current state of mobile devices in penetration testing and future trends

Objectives:

- To review software developer communities' experience with the use of mobile devices in pen-testing
- To investigate the ***reasons*** behind the ***adoption*** of mobile device pen-testing
- To investigate the ***techniques*** used on mobile pen-testing
- To investigate the ***use*** of mobile device for pen-testing
- To present future trends

Definition

Pen-testing is:



- A process of attempting to gain access to resources without the knowledge of formal means of access such as usernames and passwords (Mancini et.al, 2006)

- **An attempt to compromise the security of the mechanism undergoing the test, it can be host or network based (Fiocca, 2009)**

Difference: pen-testing and hacking is ***permission***
Its **purpose** is to find system vulnerabilities

Previous/traditional methods

- Host-based vulnerability scanning
- Network based vulnerability scanning
- Application scanning
- Web Application Assessment Proxy

Previous/traditional methods

- **Advantage:** more reliable, it was used in the early 90s

- **Disadvantage**:
- Fixed workstations
- PCs need larger space
- PC set-up time
- Not easy to hide
- Lack portability

Traditional pen-testing is not complete - why?

- **Banning laptops** is not enough, cell-phones can hack too
- Pocket sized device is more convenient, since it is easy to carry around at anytime
- A power plug is not innocent, need to look for activity other than just traditional PCs / devices

Mobile device pen-testing

Pocket sized devices that connect to the internet and capable of running mobile Operating System (OS)

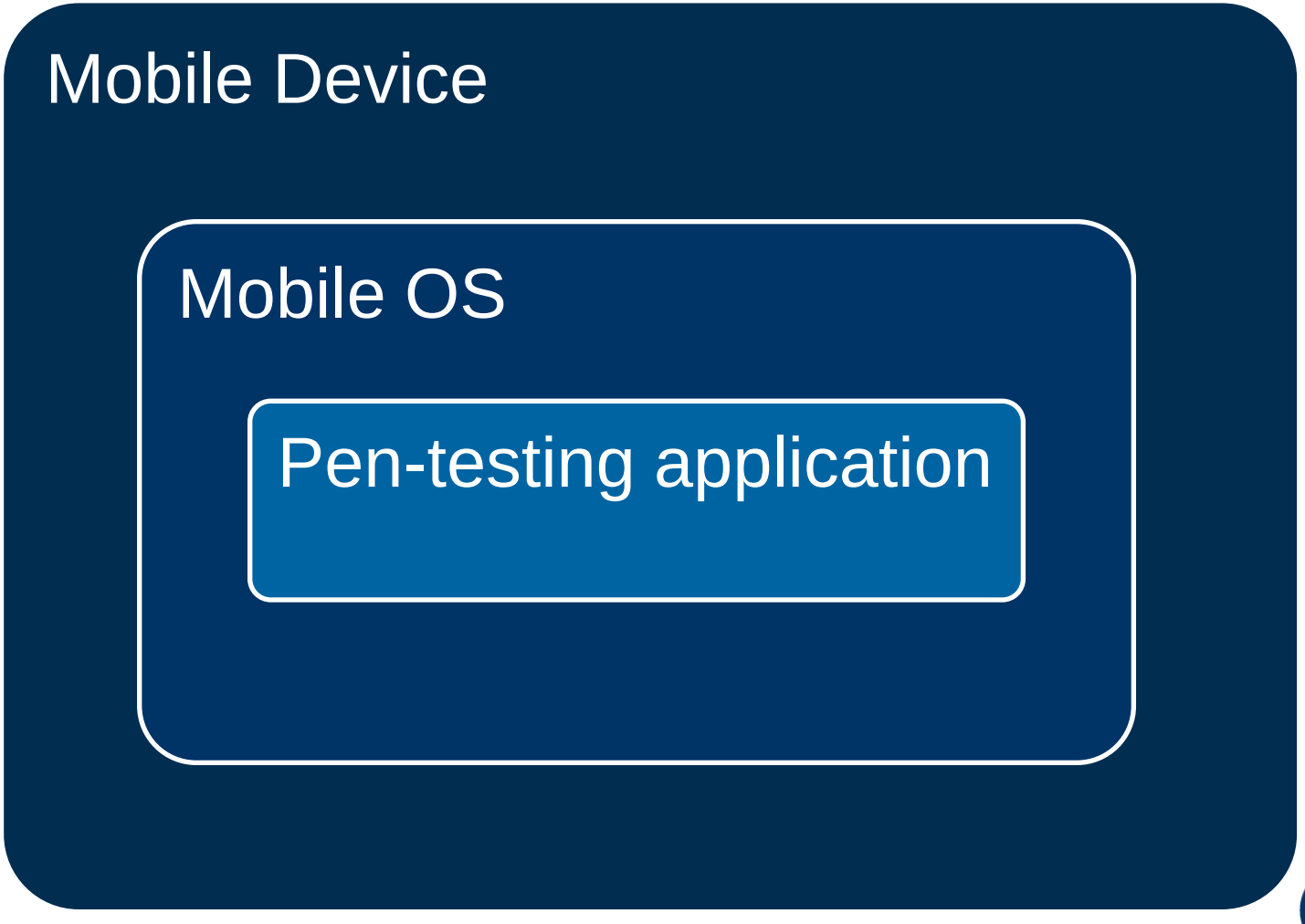
Examples:

- Cell phone
- PDA
- Tablet

Other:

- USB
- Power Strip

How it works



… How it works

Current Android hacking applications:

- WiFi Analyzer
- SpoofApp
- FaceNiff
- Penetrate Pro
- Anti-Android Network Toolkit
- ConnectBot
- Network Discovery
- Wireless Tether
- Shark for Root
- Remote Exploit Applications
- Mobile MITM Attack
- Data Siphon

….How it works

- **USB**: install appropriate OS, e.g. backtrack and pen-testing tools

- **Power plug**: attach it to a pc connected to the network

- **Own scripts**: using program like C4Droid (a C/C++ compiler designed for Android)

Mobile device pen-testing

Conducting pen-testing using mobile devices as a tool does not limit you to a specific network

Potential victims include:

- Medical devices
- Cars
- Cell phones
- Networks
- Stealing keystrokes
- Electricity meters etc.

Challenges of mobile pen-testing

- Emerging field
- Industrial psychology
- Limited number of academic literature
- Battery power
- Limited CPUs (getting better)

Conclusion

Bottom line:

- Pen-tests can only measure how bad a person's application is
- They're far less effective at measuring how good an application is

Challenge:

- Researchers should look at mobile pen-testing tool since it can be a great way of getting unexpected information out of a company

The more mobile / innocuous the pen-testing platform the better

Thank you

our future through science