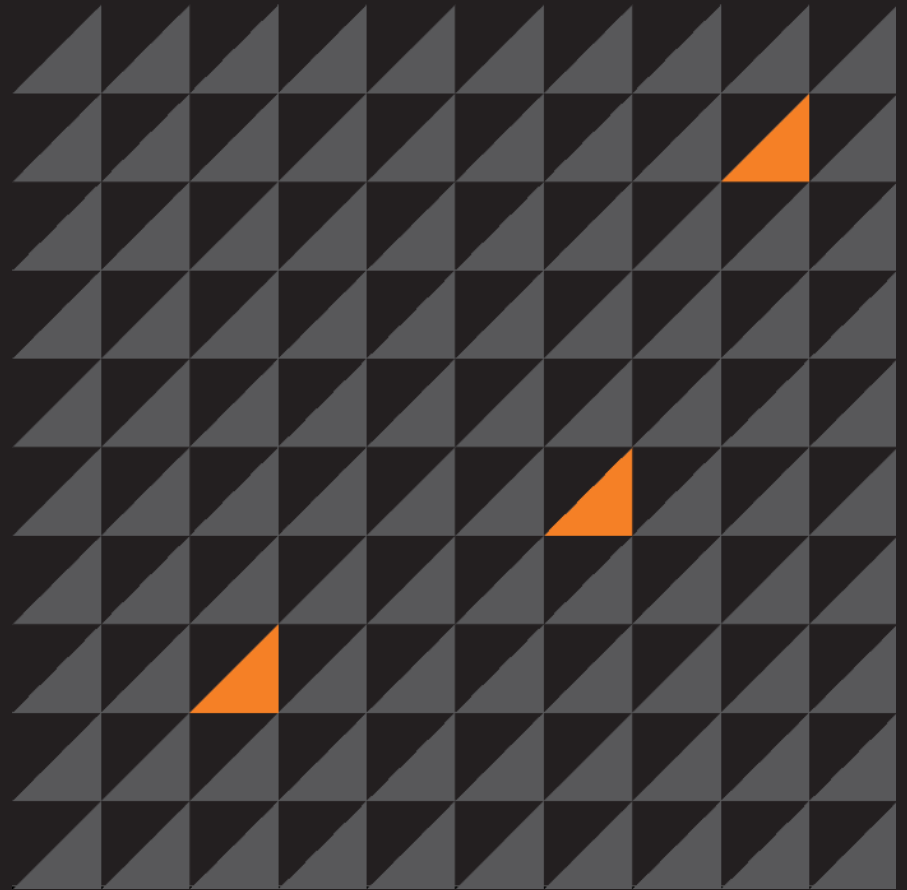


MWR Guest Lecture

UCT

2015-03-19





MWR InfoSecurity

Information Security Consultancy

Offices in London, Basingstoke, Manchester, Singapore, Dubai, Washington and Johannesburg

Started in the UK in 2003, opened SA offices in 2007

What do we do? - Consultancy

- Penetration Testing
 - Mobile Devices / Applications
 - Infrastructure
 - Web Applications
 - Hardware
 - **Red Team**
- Incident Response
- Social Profiling
- Forensics

What do we do? - Consultancy

- Penetration Testing
 - Mobile Devices / Applications
 - Infrastructure
 - Web Applications
 - Hardware
 - **Red Team**
- Incident Response
- Social Profiling
- Forensics

What don't we do?



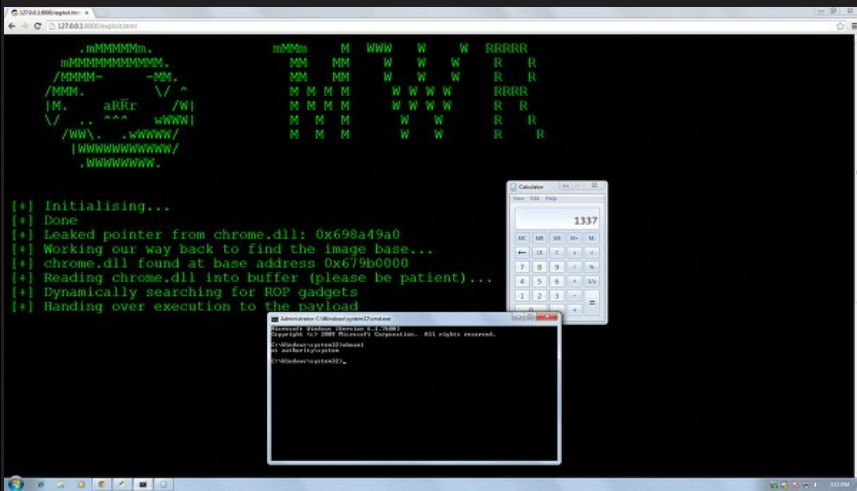
What do we do? - Research

- Malware reversing
- Tool dev
 - drozer
- Vulnerability dev
 - Remote code execution
- Hardware hacking
 - POS devices
 - ATMs



A look at past MWR research

- Won **Mobile Pwn2Own 2014** – Samsung Galaxy S5, Amazon Fire
- Won **Pwn2Own 2013** – Google Chrome
- Won **Mobile Pwn2Own 2012** – Samsung Galaxy S3
- First proof of concept and popularisation of hacking Android phones remotely using **JavaScript bridges**



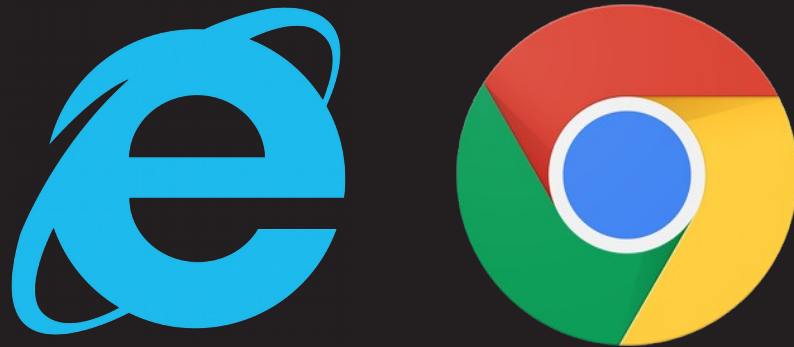
Pwn2Own to explain mobile security

- Attack surface of mobile devices
- Differences between devices
- Demo of a compromised device



Attack surface of mobile devices

▫ Mobile Web Browser



Attack surface of mobile devices

- Mobile Application/Operating System



Attack surface of mobile devices

- Short Distance:
 - Bluetooth, Wi-Fi, or Near Field Communication (NFC)



Attack surface of mobile devices

- Messaging Services:
 - Short Message Service (SMS), Multimedia Messaging Service (MMS), or Commercial Mobile Alert System (CMAS)



Attack surface of mobile devices

▯ Baseband



Differences between mobile devices

- Language
- Permissions
- Inter-process communication (IPC)
- Vendor addons



Demo of a compromised device

HackFu

- Set of challenges
- Hacking mindset necessary
- Sponsored trip to secret location in UK

mwr.to/hackfuchallenge2015

Questions