black hat EUROPE 2014

MAN IN THE BINDER:
HE WHO CONTROLS IPC, CONTROLS THE DROID

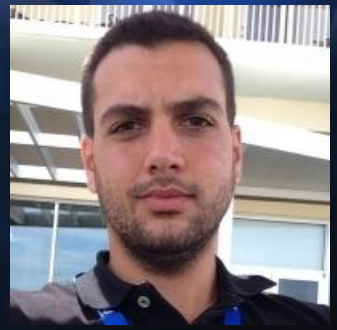
Nitay Artenstein - nitaya@checkpoint.com
Idan Revivo - idanr@checkpoint.com

Who Are We?

Nitay Artenstein

- Researcher at Check Point
- Used to do pentesting in Africa (with a machete)
- Now does more risky stuff, such as kernel exploits

Idan Revivo



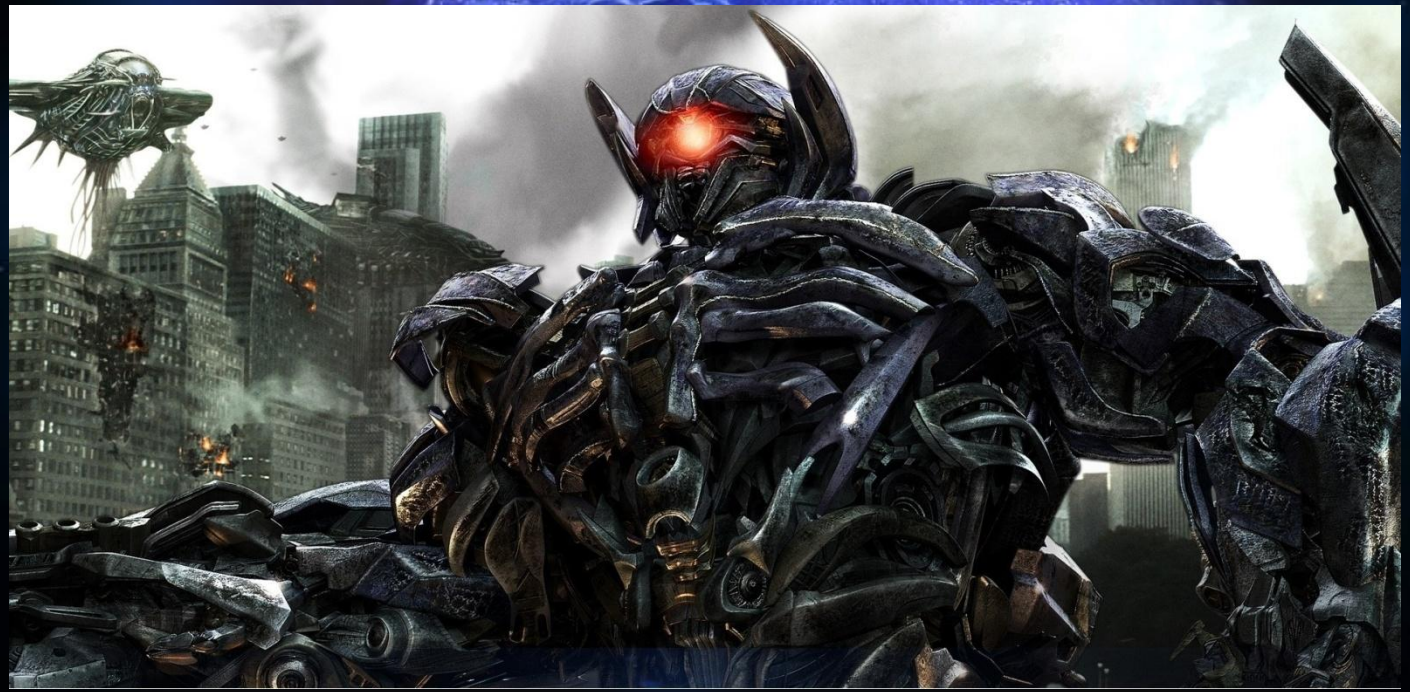
- Researcher at Check Point
- When he's not breaking Android, he breaks his trainees at the gym
- Contributor to Cuckoo Project


Overview
black hat
EUROPE 2014

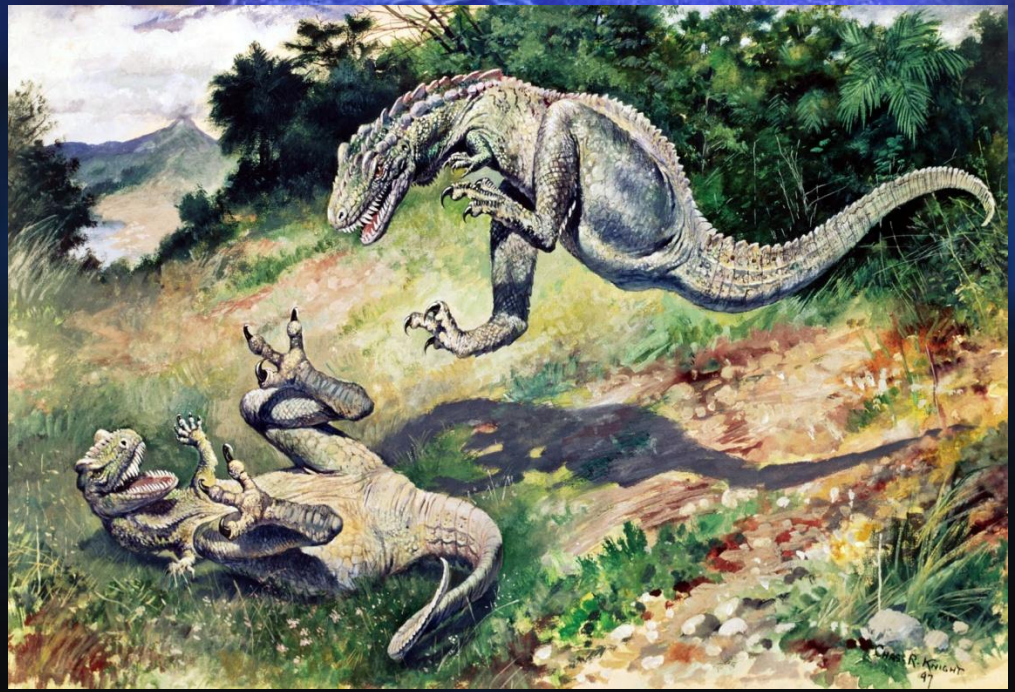
ev·o·lu·tion (ĕv'ə-lo͞o'shən, ē'və-)

n. A gradual process in which something changes into a different and usually more complex or better form

Malware on Windows



Malware on Android



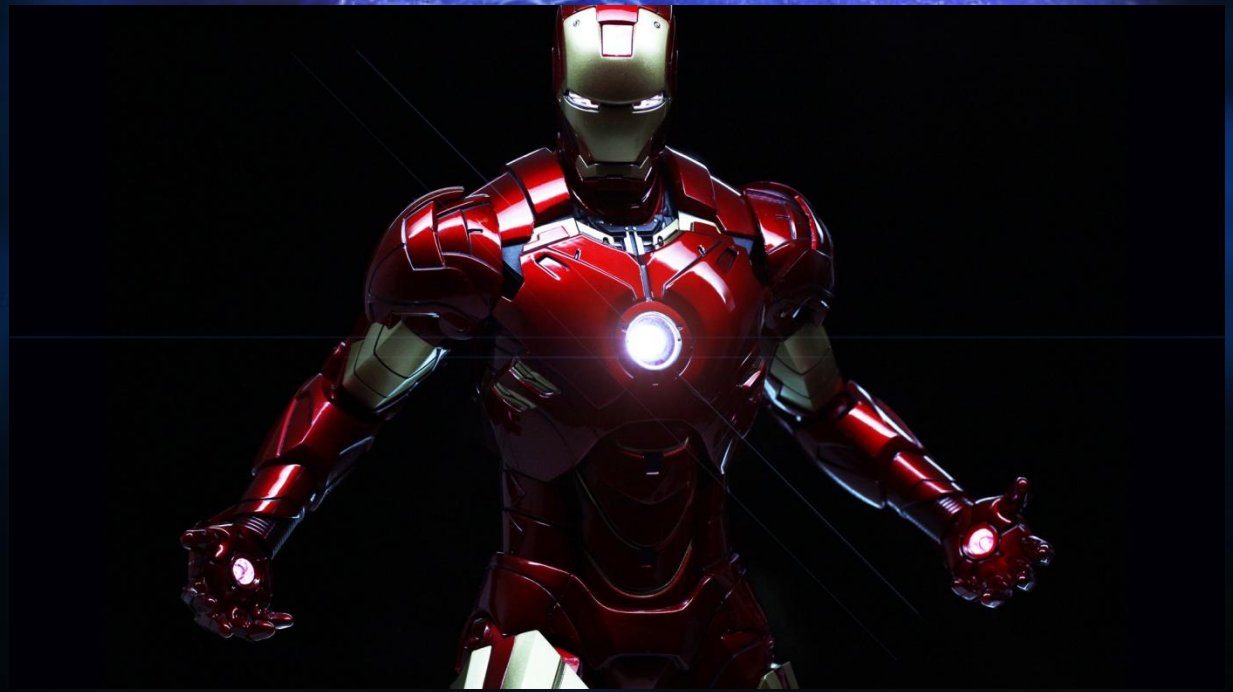
black hat EUROPE 2014

Why the Big Difference?

- The sandbox
- Android is a complicated environment
- Do we work in Java? JNI? C? Native ARM?

How to Write Malware in this Mess?

Welcome to Binder



Agenda

- Android Malware Today
- Developer Point-of-View
- What is Binder?
- Man In The Binder Attacks
- Possible Solutions

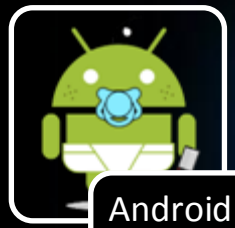
Android Malware Attacks

black hat
EUROPE 2014

What Do Mobile Malware Authors Want?

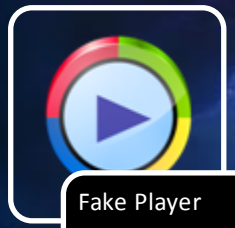
- Sending SMS to premium numbers
- Location tracking
- Secondary APK installation
- Link clicking
- Bank fraud
- Stealing personal information
- Etc..

Android Malware Evolution



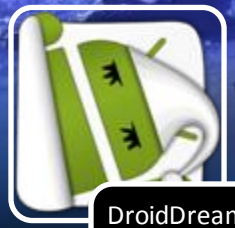
Android Was Born

- 9/2008



Fake Player

- 8/2010
- First SMS Trojan
- Just asks for SEND_SMS permission



DroidDream

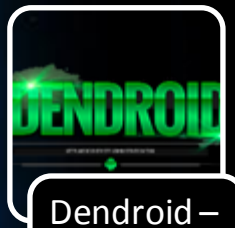
- 3/2011
- Uses root exploits
- Installs secondary APK
- 50 variants in app store

Spitmo – Zeus goes mobile

- 3/2011
- Banking malware

Obad – The most sophisticated Android trojan

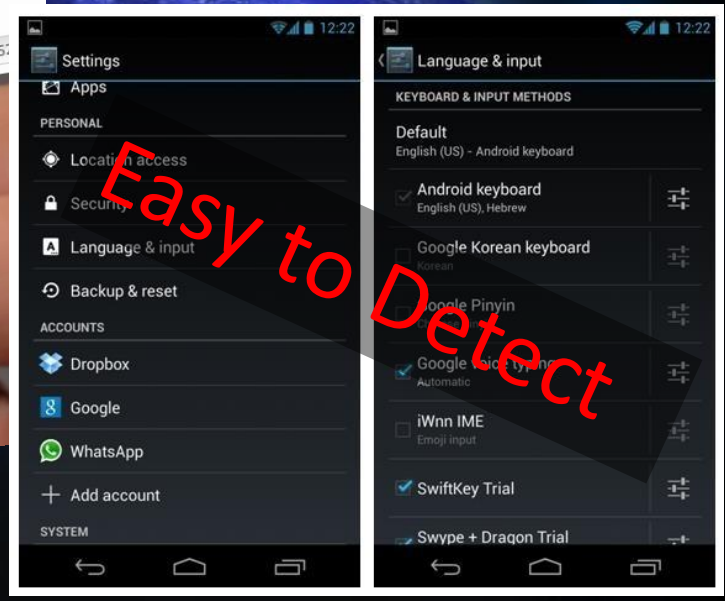
- 6/2013
- 3 exploits
- 1 backdoor
- SMS Trojan



Dendroid – Android RAT

- 5/2014

Keylogging – Swapping the Keyboard



Intercepting SMS – Just Ask Politely

```
if (messageBody.equals("somedata"))
    {

        Intent i  = new Intent(context,Webservice.class);//webservice validat
        i.putExtra("messageBody",messageBody)
        startService(i);

    // Stop it being passed to the main Messaging inbox
        abortBroadcast();
    }
```

Easy to Detect

```
<uses-permission android:name="android.permission.SEND_SMS" android:required="true" />
<uses-permission android:name="android.permission.WRITE_SETTINGS" android:required="false" />
<uses-permission android:name="android.permission.READ_PHONE_STATE" android:required="false" />
<uses-permission android:name="android.permission.WRITE_EXTERNAL_STORAGE" android:required="true" />
<uses-permission android:name="android.permission.CAMERA" android:required="true" />
<uses-permission android:name="android.permission.RECORD_AUDIO" android:required="false" />
<uses-permission android:name="android.permission.PROCESS_OUTGOING_CALLS" android:required="true" />
<uses-permission android:name="android.permission.RECEIVE_SMS" android:required="true" />
<uses-feature android:name="android.hardware.camera" android:required="false" />
```

Location Tracking – Again Just Ask Politely

```
@Override
public void onLocationChanged(Location location) {
    // TODO Auto-generated method stub

    int latitude = (int) (location.getLatitude());
    int longitude = (int) (location.getLongitude());

    Log.i("Geo_Location", "Latitude: " + latitude + ", Longitude: " + longitud
}
```

Easy to Detect

```
<uses-permission android:name="android.permission.ACCESS_NETWORK_STATE" android:required="true"/>
<uses-permission android:name="android.permission.READ_CONTACTS" android:required="true" />
<uses-permission android:name="android.permission.ACCESS_FINE_LOCATION" android:required="true" />
<uses-permission android:name="android.permission.GET_TASKS" android:required="true" />
<uses-permission android:name="android.permission.WAKE_LOCK" android:required="false" />
```

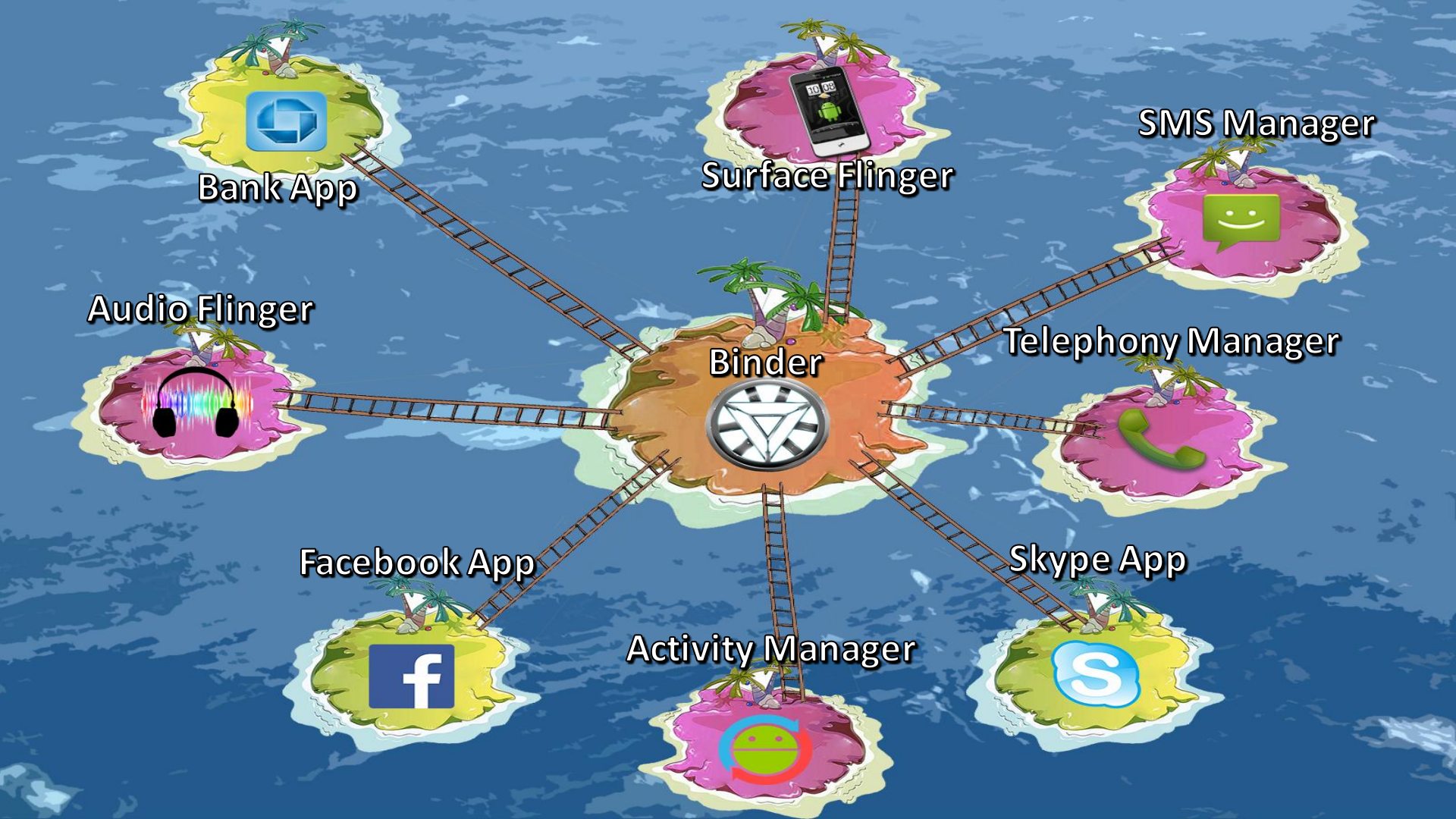

Developer Point-of-View
DROID
black hat
EUROPE 2014

Android Architecture Basics

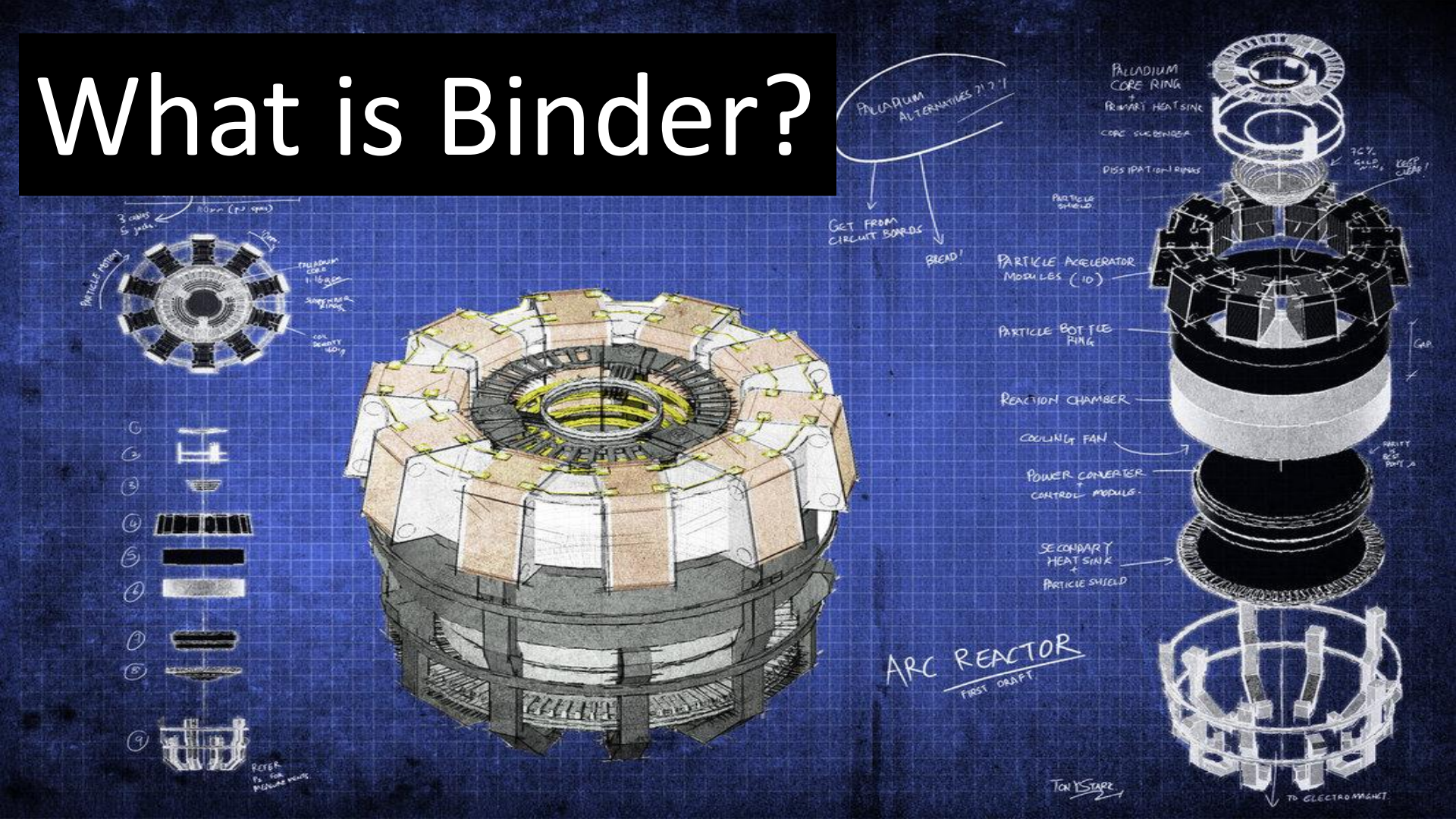
- Android is built on top of the Linux kernel
- An application doesn't talk to hardware
- Talking to the system – only via IPC

The Sandbox

- Each app runs with its own uid
- Privileges are given upon app installation
- Each privilege translates into a gid


Bank App
Surface Flinger
SMS Manager
Audio Flinger
Binder
Telephony Manager
Facebook App
Activity Manager
Skype App

What is Binder?



Return of the Microkernel

Andrew S. Tanenbaum

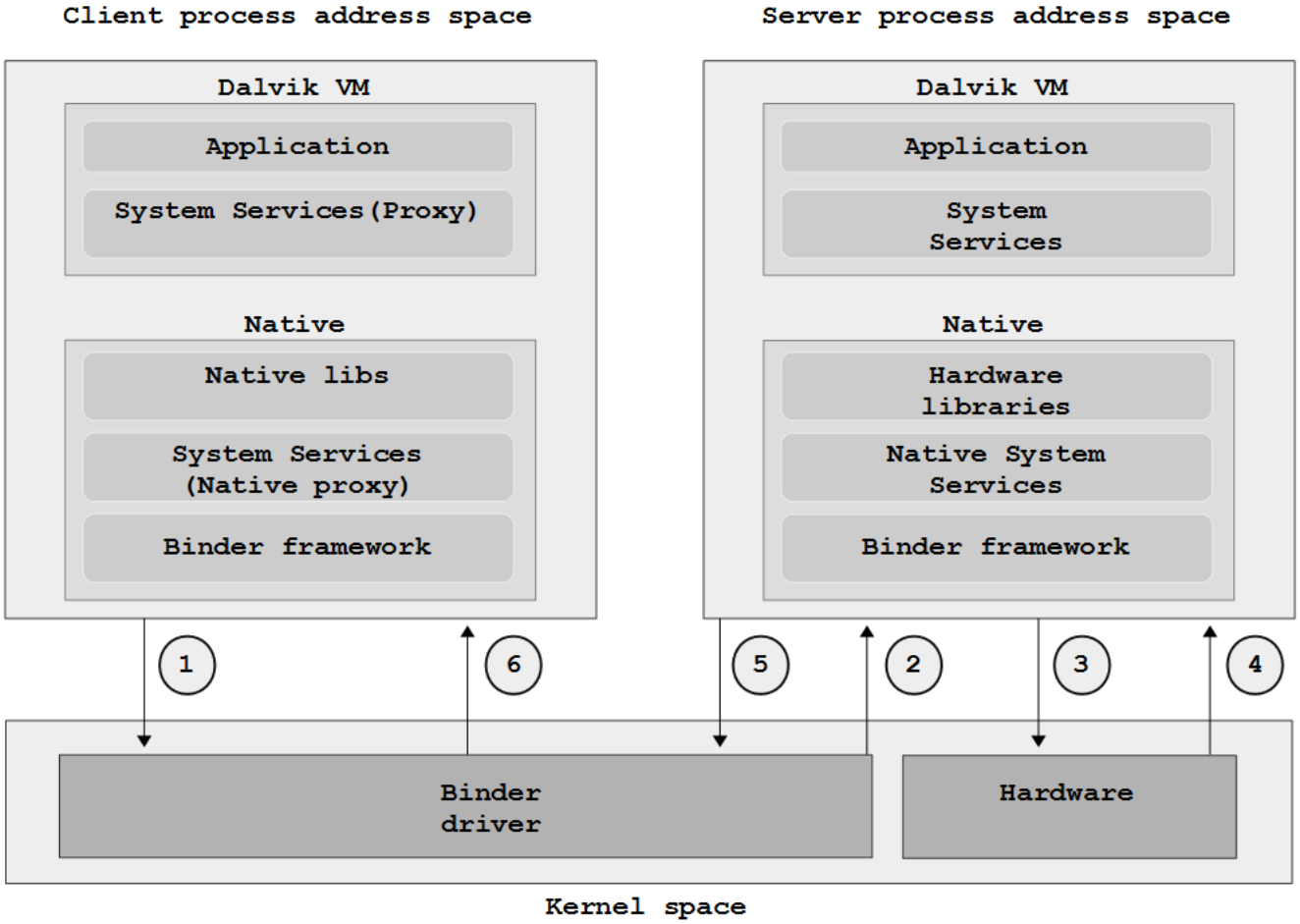
Dianne Hackborn

Darth Vader

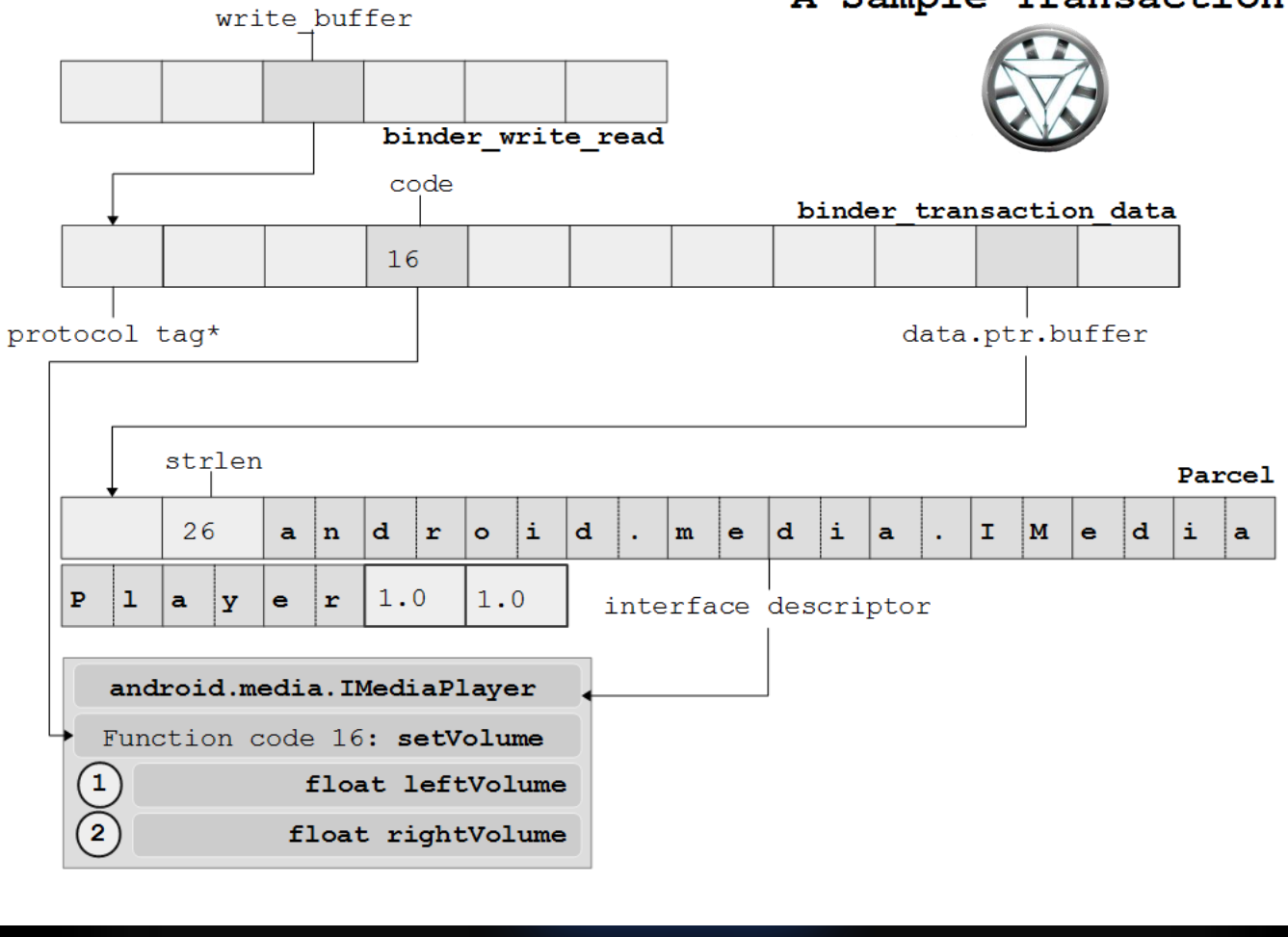
- Minimalist kernel, less attack surface
- Monolithic kernels won the war
- How to get the benefits of a microkernel anyway?

IPC is the Key

- Isolate the kernel from user apps
- Implement system servers in userland
- Control all communication via Binder


Client process address space
Server process address space
Dalvik VM
Application
System Services(Proxy)
Native
Native libs
System Services
(Native proxy)
Binder framework
Dalvik VM
Application
System
Services
Native
Hardware
libraries
Native System
Services
Binder framework
1
6
5
2
3
4
Binder
driver
Hardware
Kernel space

A Sample Transaction



Why Target Binder?

- Stealthy, difficult to detect
- Portable data interception
- Integration with the system architecture

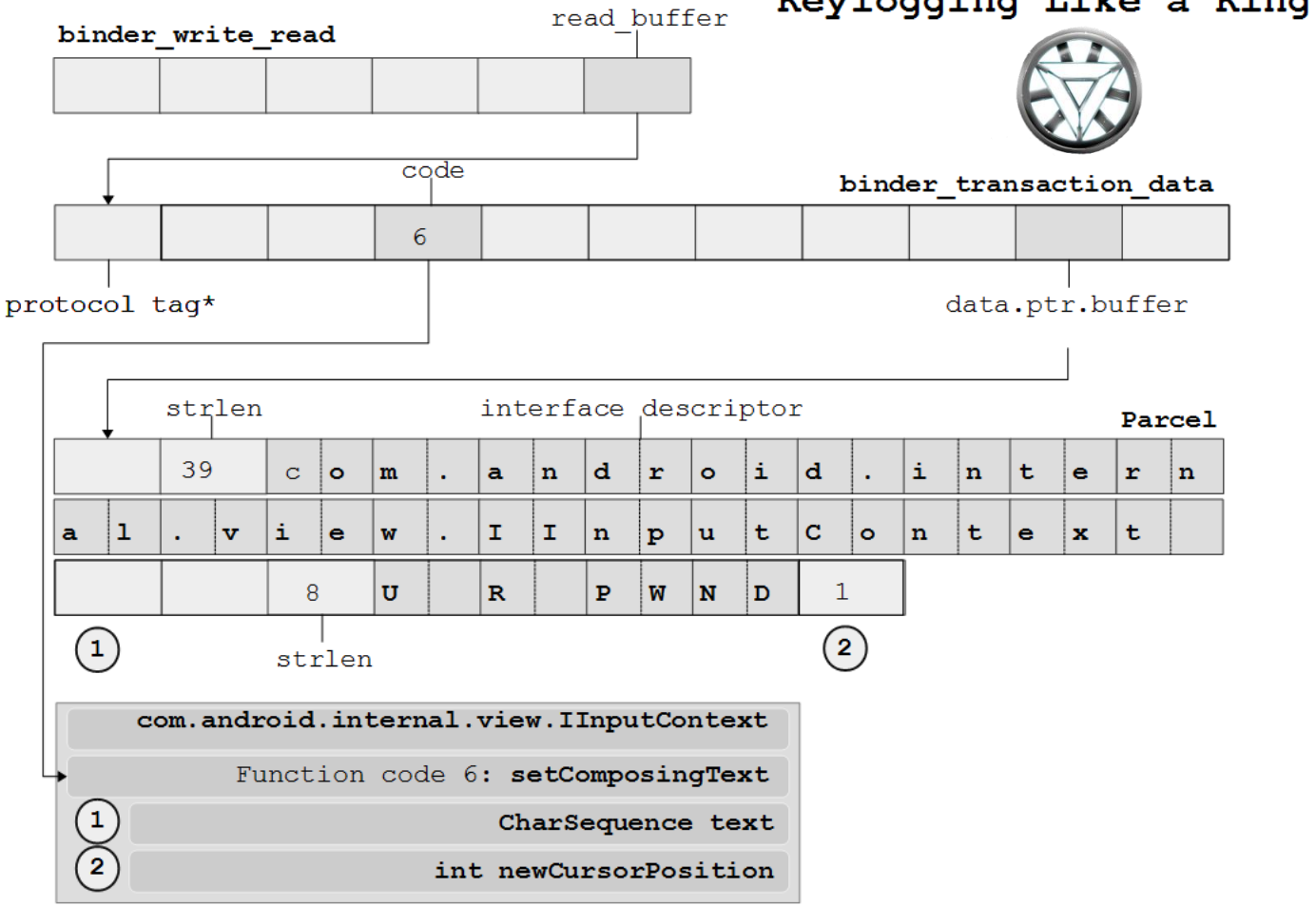
Ready for Some Fun?


First Attack: Keylogger
black hat
EUROPE 2014

Keyloggers, the Binder Way

- A thread in an app sets up a listener
- It is contacted by the InputContext interface when the user hits a key
- All communication is done via Binder

Keylogging Like a King




Keylogging Demo
DroID
black hat
EUROPE 2014

Second Attack: Data Grabbing

The Secret About Activities

- Most secure applications protect their data
- However, developers don’t bother to encrypt data moving between in-app Activities
- Surprise: This data goes through Binder

Yes, in-app data goes through Binder

…and we got the hex dump to prove it


Form Grabbing Demo
DROID
black hat
EUROPE 2014

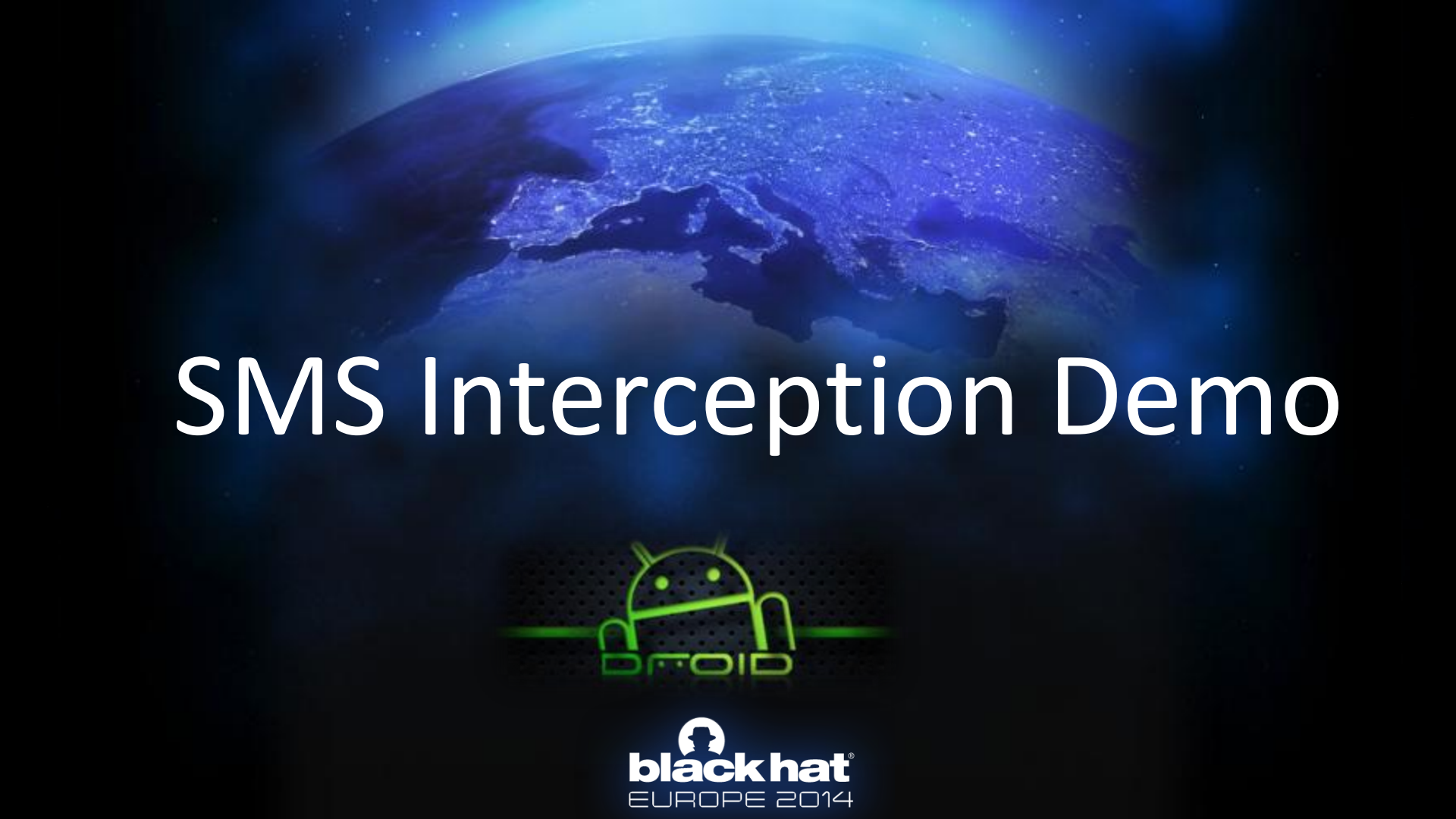
Third Attack: Intercepting SMS

What Happens When You Get An SMS?

- The Telephony Manager notifies the SMS app
- The app queries the TM's database
- The response is sent back as a Cursor object
- …but that's just a file descriptor!

Let's Grab It!

```
0x000000: 00 00 00 00 01 00 00 00 01 00 00 00 00 00 00 00 ................
0x000010: 01 00 00 00 50 c3 65 b6 48 01 00 00 03 00 00 00 ....P??H.......
0x000020: ec 01 00 00 0e 00 00 00 00 00 00 00 00 00 00 00 ?...............
0x000030: 00 00 00 00 03 00 00 00 fa 01 00 00 42 00 00 00 ............?...B...
0x000040: 01 00 00 00 00 00 00 00 00 00 00 00 2b 39 37 32 ............+972
0x000050: 35 38 36 32 32 31 37 30 31 00 43 6f 6d 65 20 6f 586221701.Come o
0x000060: 6e 2c 20 43 6f 68 61 61 67 65 6e 21 20 59 6f 75 n, Cohaagen! You
0x000070: 20 67 6f 74 20 77 68 61 74 20 79 6f 75 20 77 61  got what you wa
0x000080: 6e 74 2e 20 47 69 76 65 20 74 68 6f 73 65 20 70 nt. Give those p
0x000090: 65 6f 70 6c 65 20 61 69 72 21 20 00 01 00 00 00 eople air! .....
```


SMS Interception Demo
DROID
black hat
EUROPE 2014

How Do I Protect Myself?

- Do as much as you can in-app
- Audit your app to see what goes to IPC
- If it goes through Binder, encrypt it

Questions?

black hat EUROPE 2014