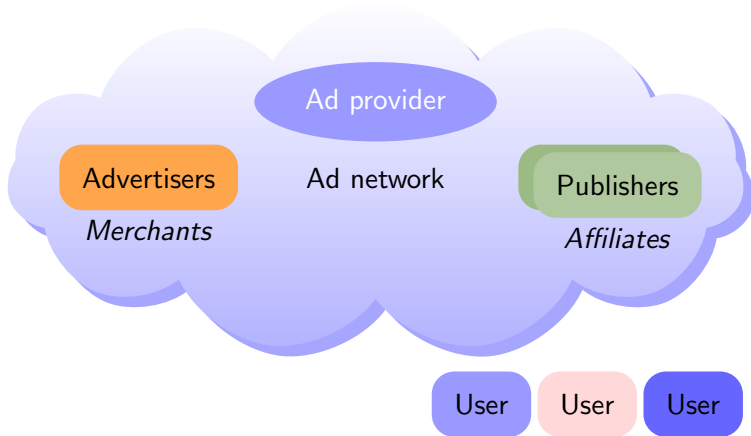
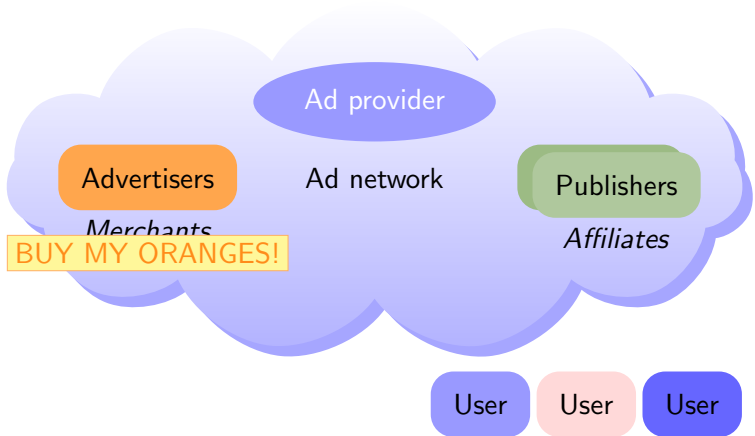


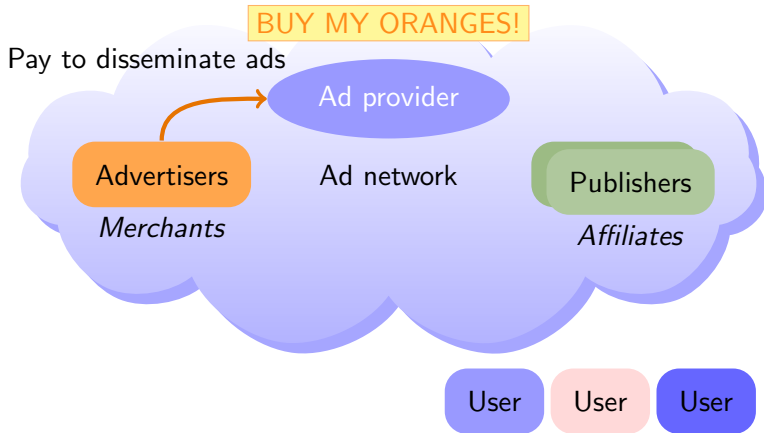
Online advertising model



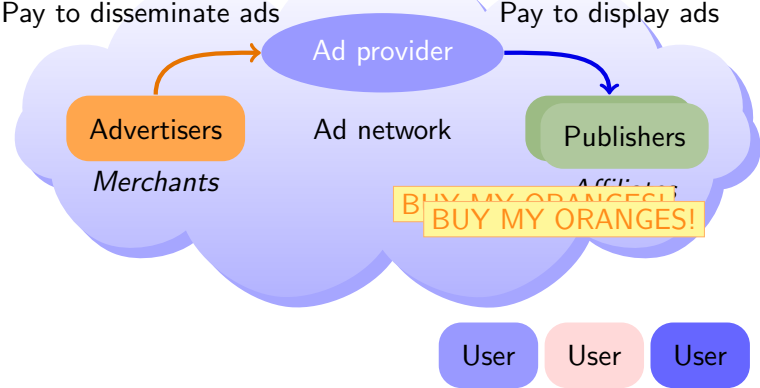
Online advertising model



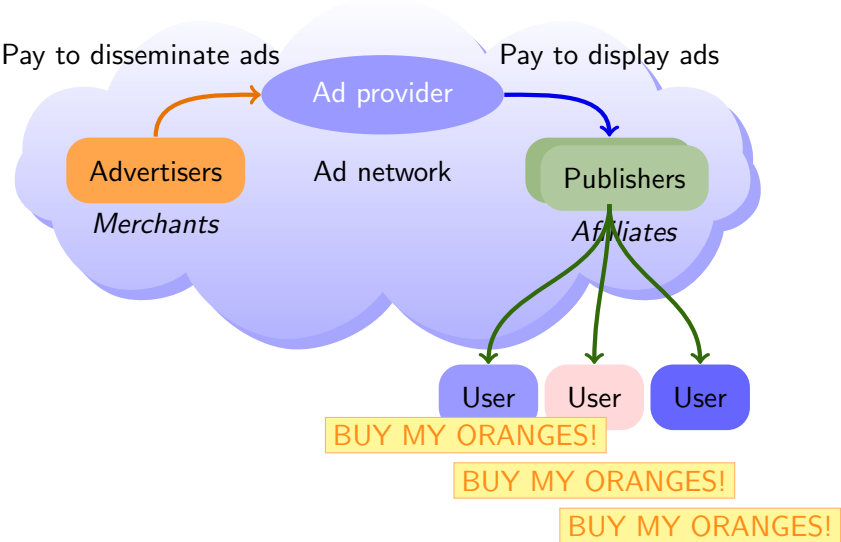
Online advertising model



Online advertising model



Online advertising model





All Your Privacy Are Belong To Us

They have built a huge **meta-data database** + correlate data



All Your Privacy Are Belong To Us

They have built a huge **meta-data database** + correlate data

Adkits hide their behaviour

They don't want us to know what they're doing



All Your Privacy Are Belong To Us

They have built a huge **meta-data database** + correlate data

Adkits hide their behaviour

They don't want us to know what they're doing

Put our phones at risk

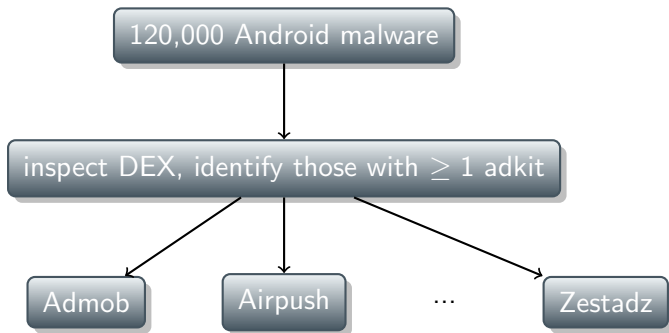
Expose security holes
Careless with our data

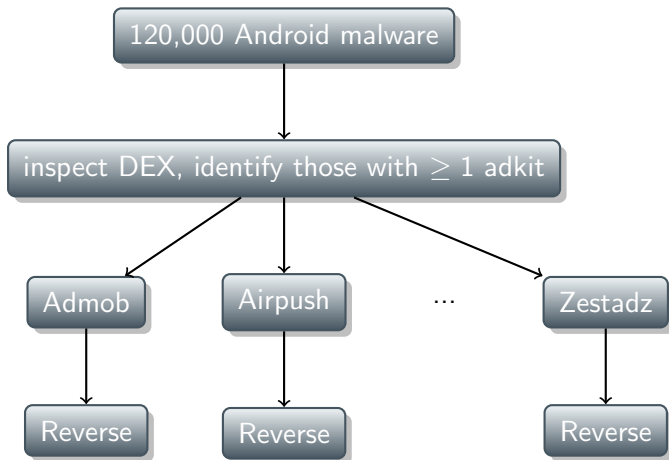
120,000 Android malware

120,000 Android malware

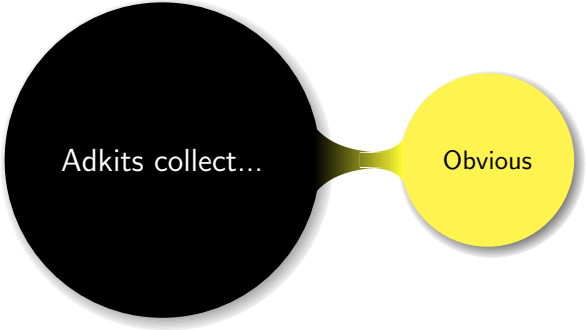


inspect DEX, identify those with ≥ 1 adkit





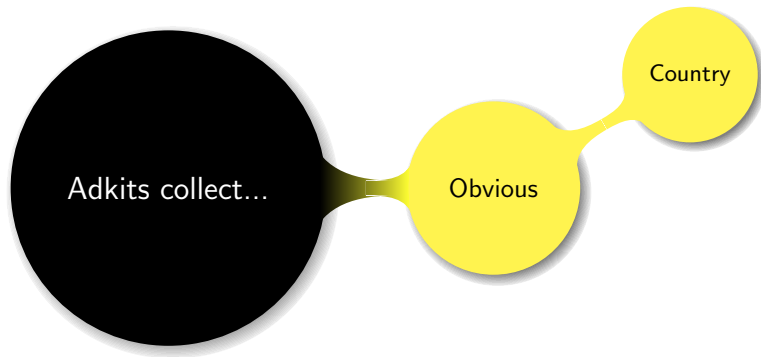
What are they collecting? Guess...



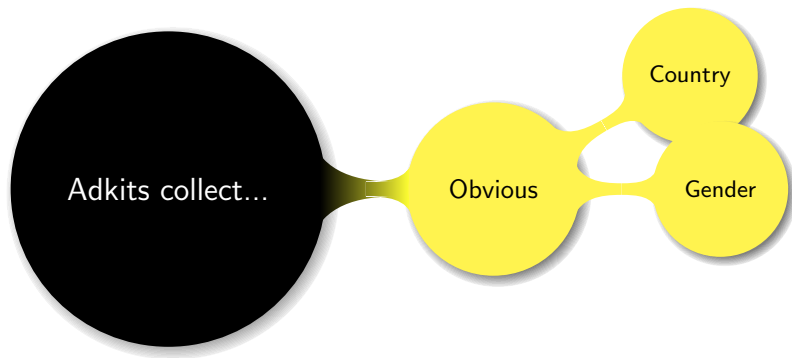
Adkits collect...

Obvious

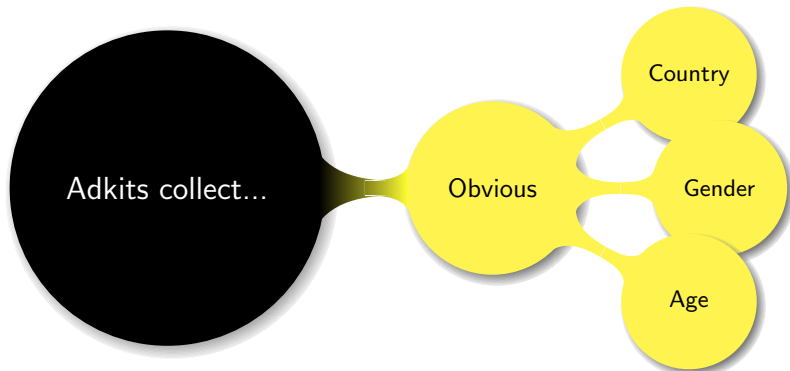
What are they collecting? Guess...

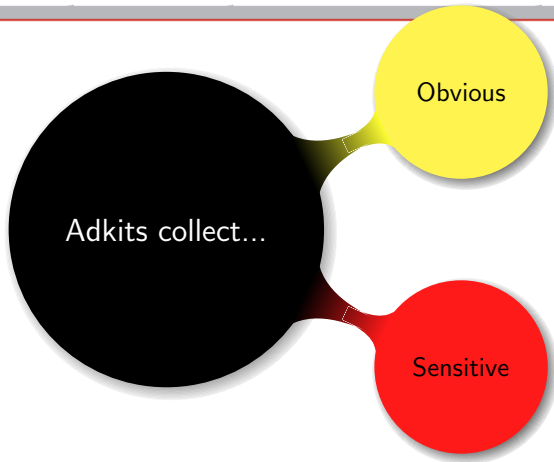


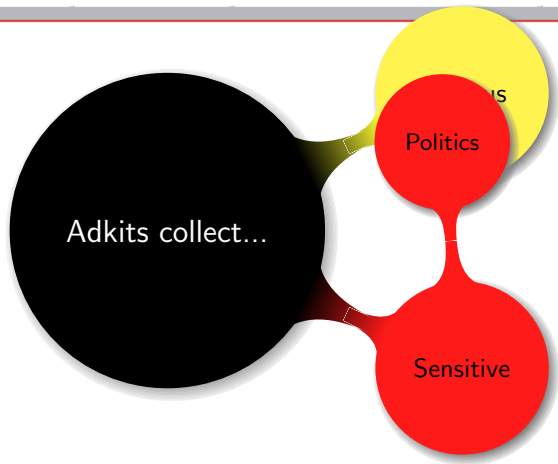
What are they collecting? Guess...

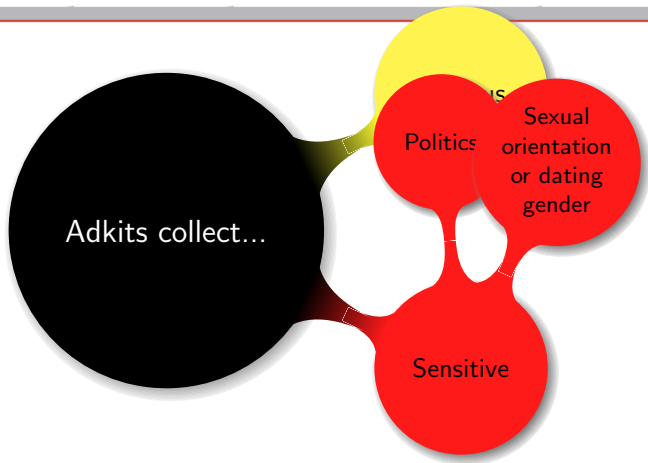


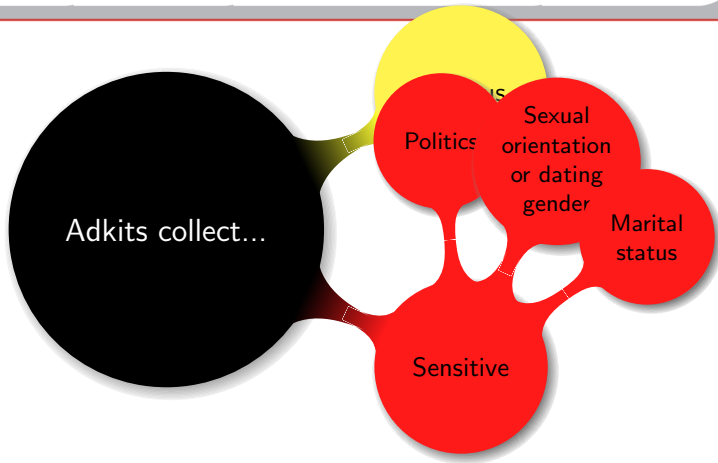
What are they collecting? Guess...

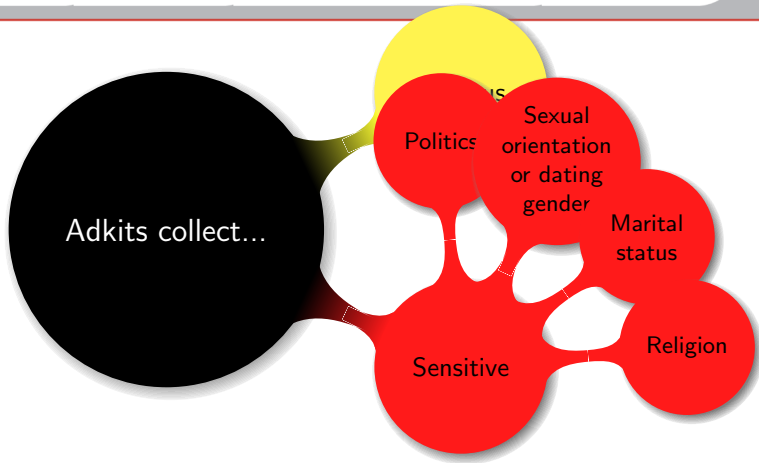


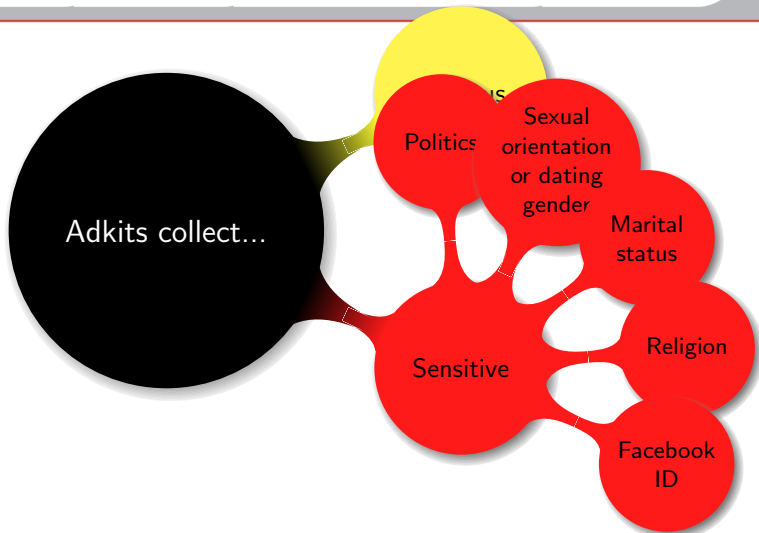


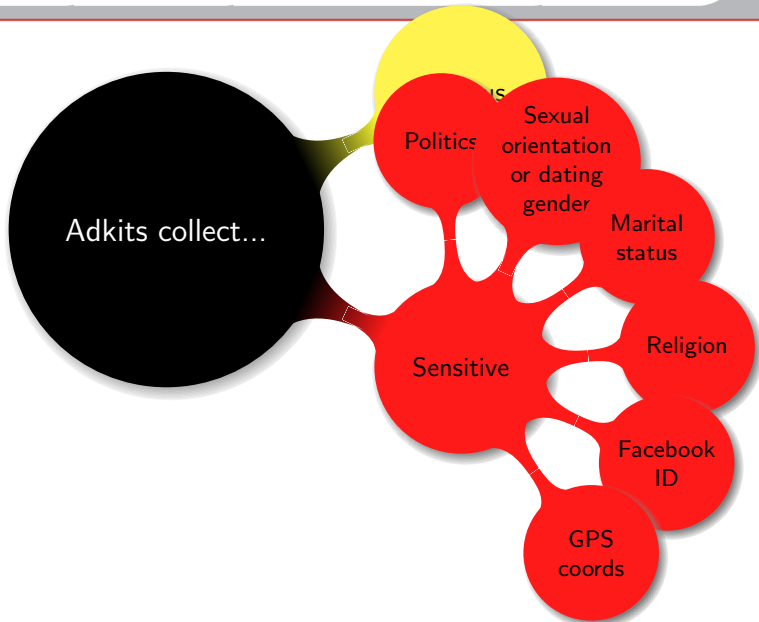




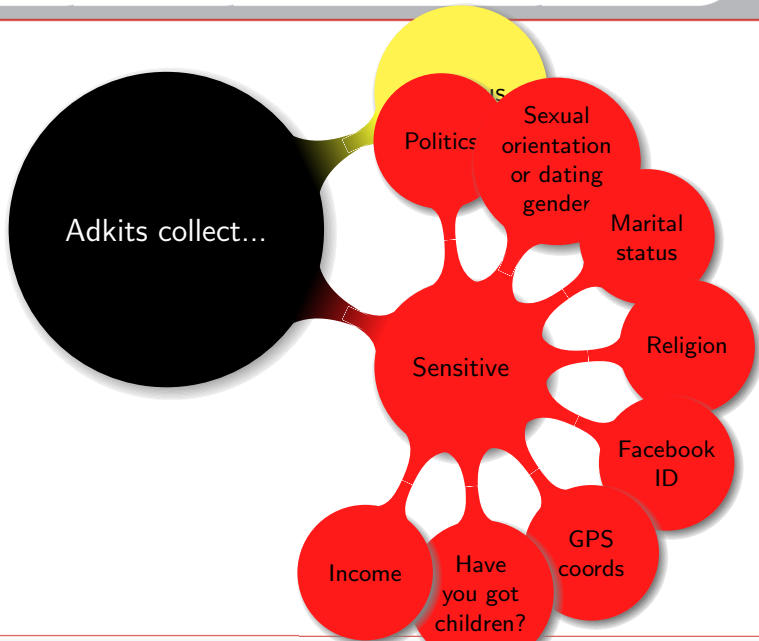


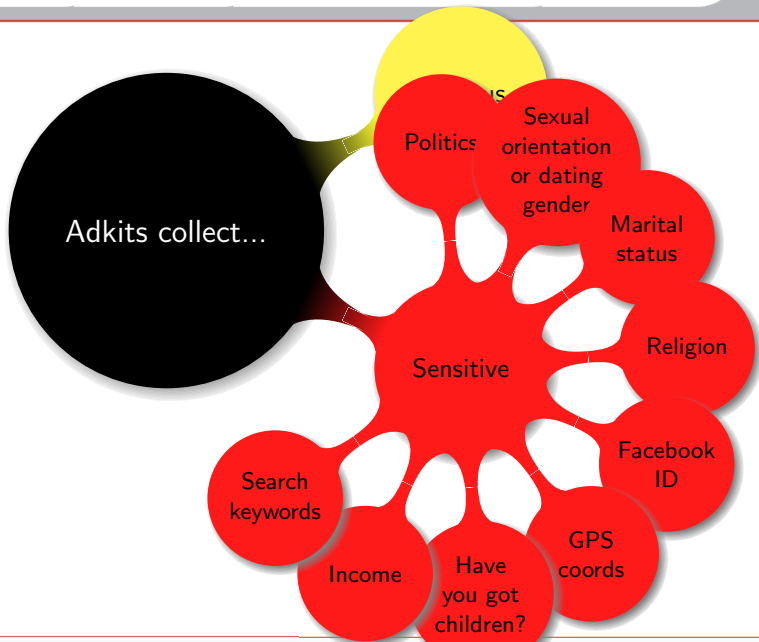




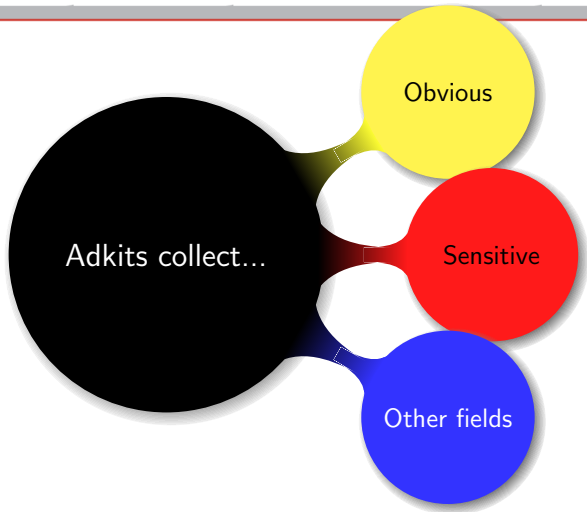




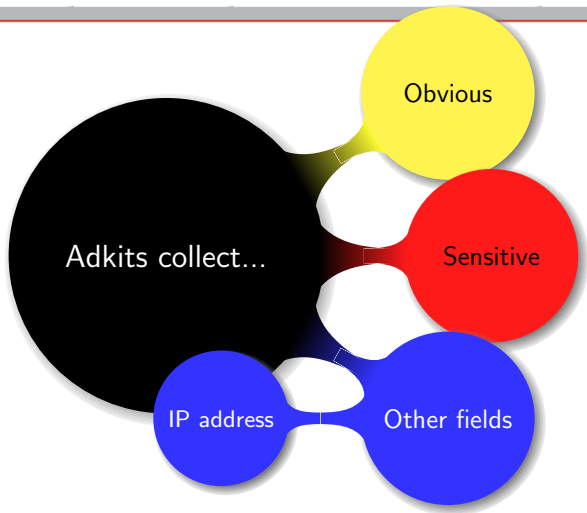




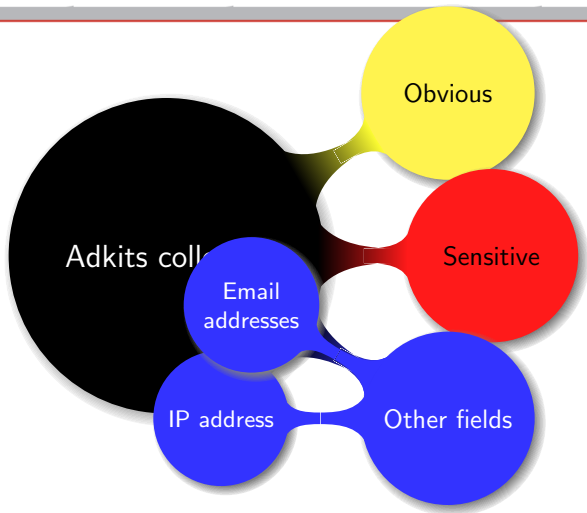
More than 50 fields!



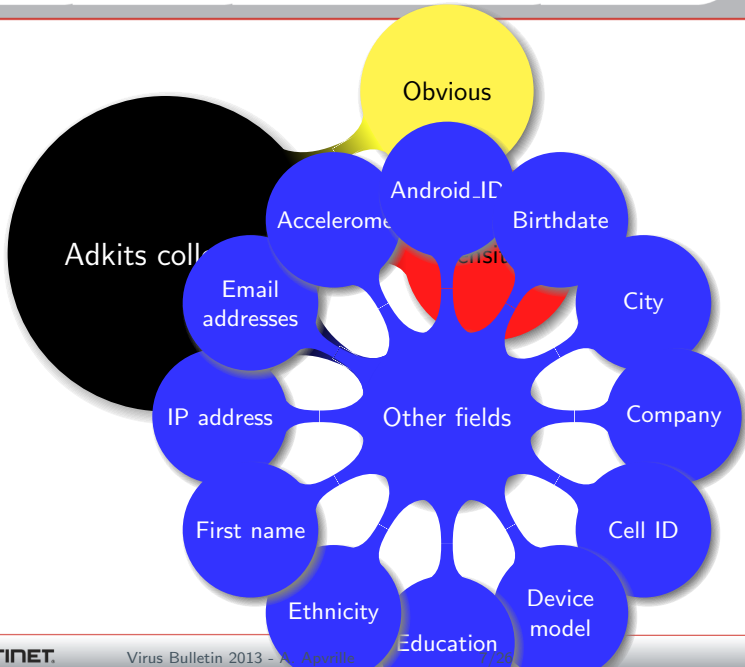
More than 50 fields!



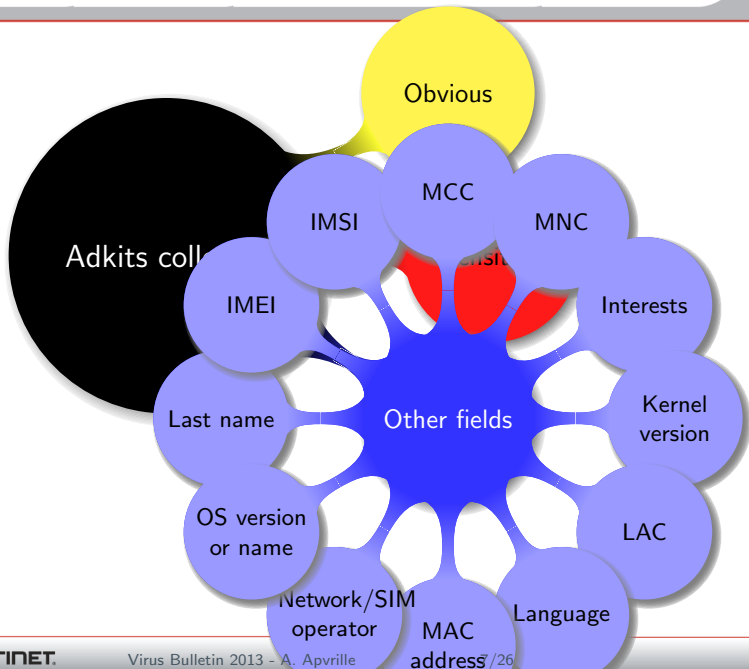
More than 50 fields!



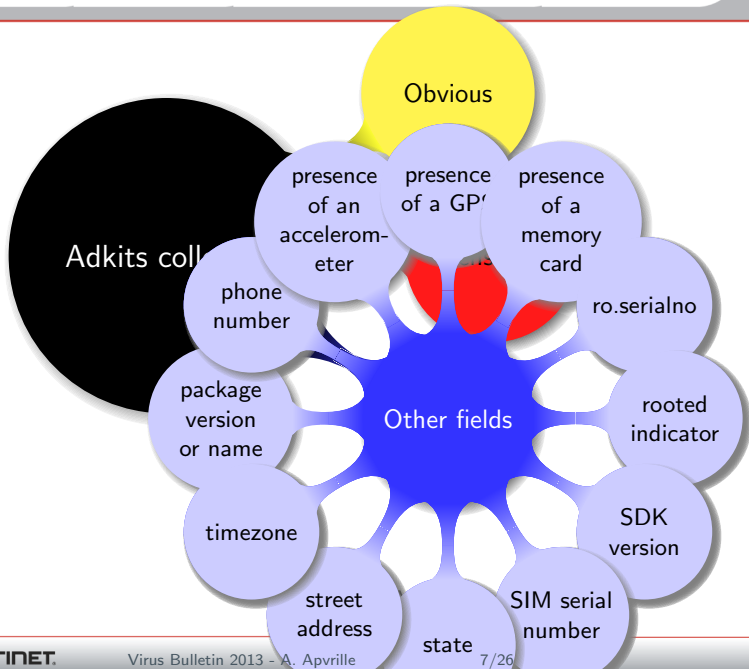
More than 50 fields!



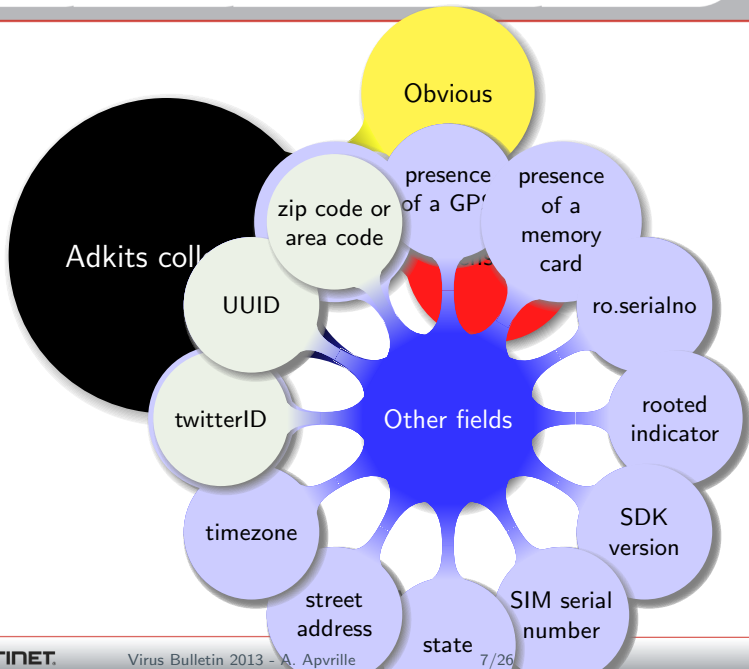
More than 50 fields!



More than 50 fields!



More than 50 fields!

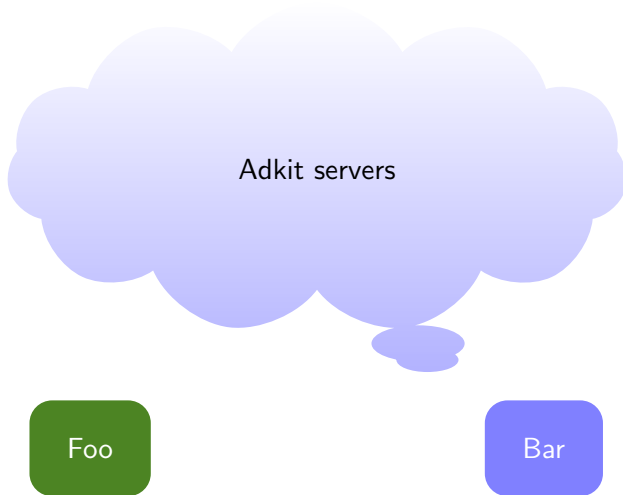


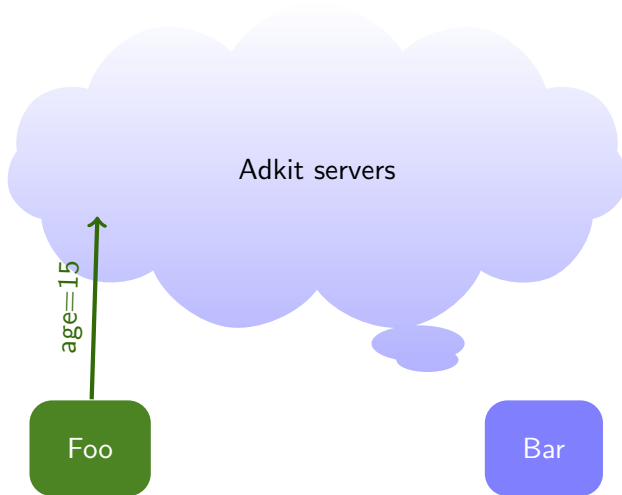
Where do they get those fields from?

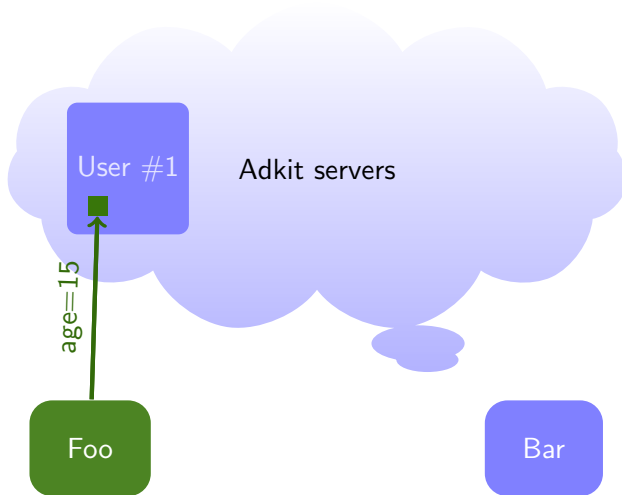


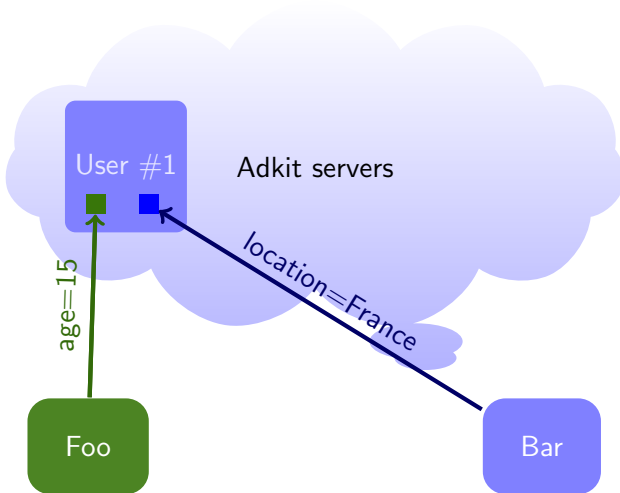
People provide the information

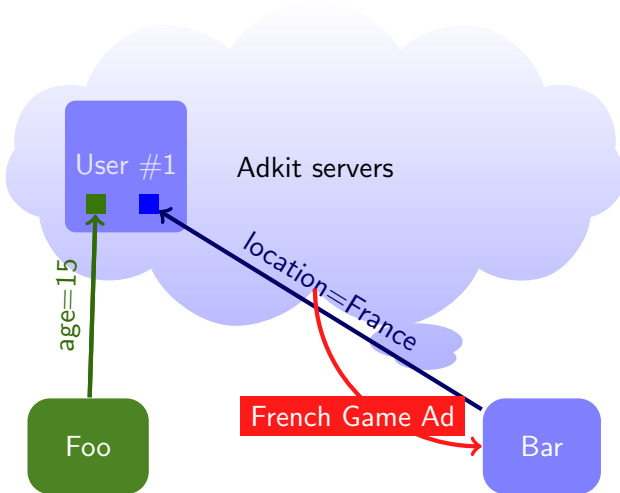
- ▶ Yes, but in a given context
- ▶ Not fully aware info can be re-used
- ▶ **User profiling.** Matching data in different db

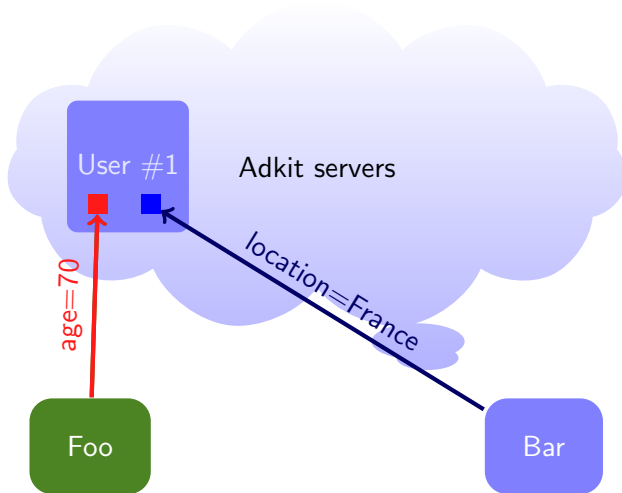




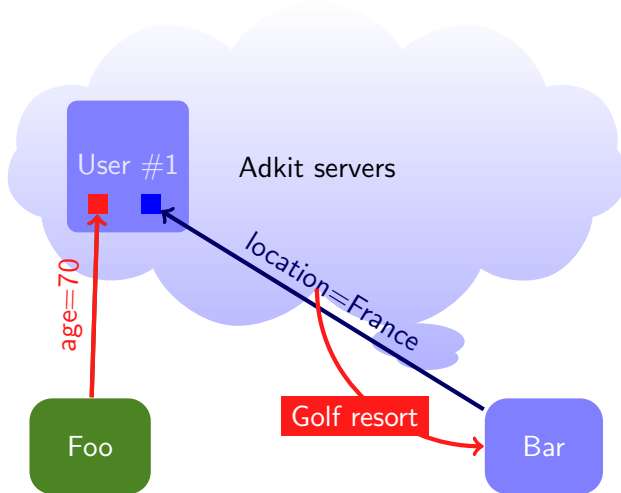


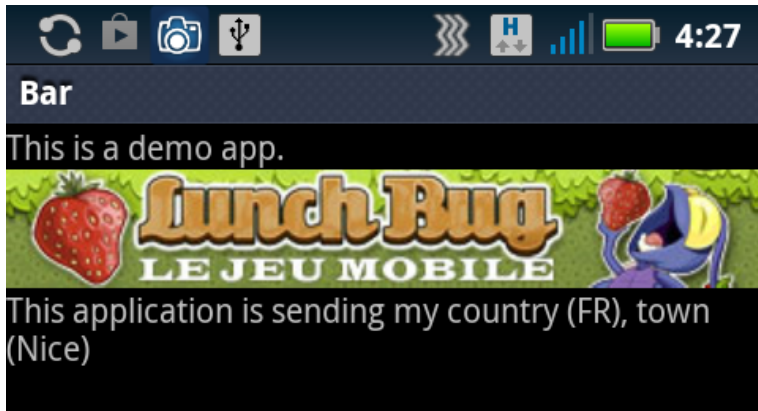






Information sharing and user profiling







Adkits retrieve information without explicit consent

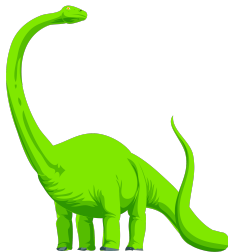
Example 1. Inexplicit permission

- ▶ `READ_PHONE_STATE`: *"Allows read only access to phone state."*
- ▶ Admogo, Adwo, Leadbolt, Pontiflex, Smaato (etc)
- ▶ use it to retrieve your **phone number** (`getLine1Number()`)



Example 2. Non-existent permission

- ▶ Mobclick 4.0.1 SDK checks if the device is rooted or not.
- ▶ No corresponding permission in Android
- ▶ Info is sent in clear text (`jb=BOOLEAN`)



Swinger?! Is it your business?

Millennial Media 3.6.3:

```
if ((this.marital == "single") ||
    (this.marital == "married") ||
    (this.marital == "divorced") ||
    (this.marital == "swinger") ||
    (this.marital == "relationship")
    || (this.marital == "engaged"))
    str = str + "&marital="
    + this.marital;
```

+ it is sent in **cleartext**...

Quattro Wireless SDK 2.1:
55 or 80, it's just the same,
you're a dinosaur!

- ▶ 12-17
- ▶ 18-24
- ▶ 25-34
- ▶ 35-49
- ▶ 50-54
- ▶ ≥ 55

50% use GPS coords

Most send them in **clear text**:

- ▶ AdYip 1.0
- ▶ LeadBolt 1.3
- ▶ MobFox SDK 1.2
- ▶ MoPub 1.6.0 and 4.0
- ▶ Wooboo SDK 1.1 ...

Ximad v2.2 posts GPS coords in HTTPS :)

Example:

`http://ads.mobclix.com?p=android...&ll=LATITUDE, LONGITUDE..`





Encrypting GPS coordinates

```
v1[1] = on.valueOf(((long) (p9.getLatitude() * ...
v1[2] = on.valueOf(((long) (p9.getLongitude() * ...
v1[3] = on.valueOf(((long) (p9.getAccuracy() * ...
com.google.ads.util.AdUtil.b(String.format("..."))
```

... with a hard-coded key

```
v0 = javax.crypto.Cipher.getInstance("AES/CBC/PKCS5...")
v3 = new byte[16];
v3 = {10, 55, 144, 209, 250, 7, ... }; // KEY !!!
v0.init(1, new javax.crypto.spec.SecretKeySpec(v3, "AES...")
v1 = v0.getIV();
v0 = v0.doFinal(p6.getBytes());
```


Approx. 40% use obfuscation

Airpush seen to obfuscate its *namespace*:

`com.klYv.TsrC111182`



Reprehensible when deliberate to hide reprehensible activity

- ▶ **deleting logs.** In Mobclick Agent 2.1.1:

```
private static String d(  
    android.content.Context p12)    {  
    ...  
    Runtime.getRuntime().exec("logcat -c");  
    ...  
}
```

- ▶ using **reflection** to hide retrieval of **account emails**

Operational emails are worthy

```
v5 = Class.forName("android.accounts.AccountManager");  
...  
v16 = v5.getMethod("get", v21);  
...  
v19 = v16.invoke(v5, v23);  
...  
v15 = v19.getClass().getMethod("getAccounts", v0);
```

Use of reflection is deliberate

Could have been retrieved directly (without reflection)

```
AccountManager mgr = AccountManager.get(this);  
Account[] accts = mgr.getAccounts();
```

Detect Android emulators

- ▶ AdsMOGO SDK 1.0.3: test **IMEI** = 0000000000000000
- ▶ Google Ads 4.3.1: Build.BOARD = unknown, Build.DEVICE = generic, Build.BRAND = unknown
- ▶ Mobfox 1.4: android_id = 0000000000000000 or 9774d56d682e549c
- ▶ Chartboost 2.0.1: Build.PRODUCT = sdk

Detect rooted devices

```
public boolean isDeviceRooted()    { ..  
    if (this.rooted == -1) {  
        Runtime.getRuntime().exec("su");  
        this.rooted = 1;  
  
        ...  
    } // Mobclix 4.0.1
```



Inspect this code in Applovin 3.4.4...

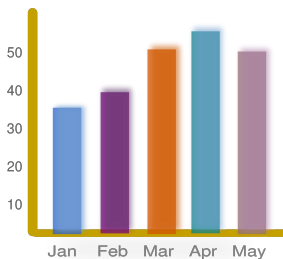
```
v2 = new java.io.File(p9.getDir("al_sdk", 0), v1);  
...  
    this.d = new SdkClassLoader(v2,  
                                p9.getDir("al_outdex", 0),  
                                SdkBootstrap.getClassLoader());  
}
```

- ▶ Retrieving files al_sdk and al_outdex
- ▶ Calling SdkClassLoader with those + class loader

SdkClassLoader class calls DexClassLoader

```
package com.applovin.sdk.bootstrap;
import android.util.Log;
import dalvik.system.DexClassLoader;
import java.io.File;
public class SdkClassLoader
    extends DexClassLoader {
    ..
}
```

- ▶ Loads the .dex without triggering a formal install
- ▶ Invisible to the end-user
- ▶ Potential security hole if adkit servers are compromised
- ▶ Hide one's behaviour?
- ▶ Also noticed in Android/Plankton (Startapp/Plankton) by *Grace et al.*



1 malware in 3 contains adkits

1 adkit in 2 uses **GPS** coordinates

(nearly) 1 adkit in 2 retrieves your **Android_ID**

Less than 20% care to hash or encrypt identifiers

Adkits seen to collect ≥ 50 **fields**

40% use some form of **obfuscation**

Are adkits *free*?

"73% apps are *free*" [Leontiadis, HotMobile'12]

Adkits ... **Free** ... as in beer?

No!

- ▶ Cost of data flow
- ▶ 65% of energy consumed in gaming app is for ad modules [Pathak et al., EuroSys'11]
- ▶ Indirect consumption



or **Free** ... as in speech?

No!!! → Loss of privacy

The dangers of mobile ads

Mobile phones carry personal data + camera, microphone, GPS...
Ad Server (located in the US?)

John Doe

Aged 32, Married, lives in San Francisco

Eats too much pizza, hates cats

Bought a scarf for Barbara

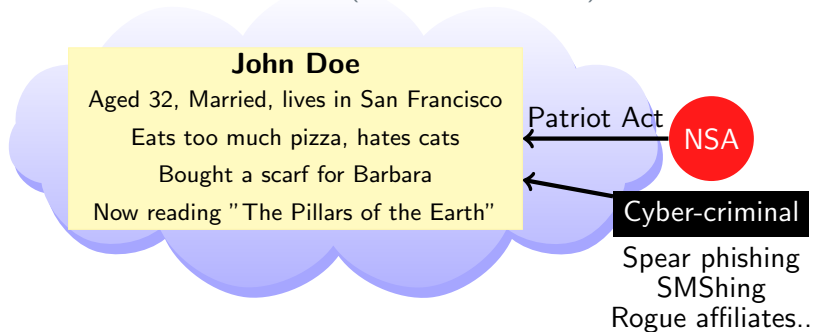
Now reading "The Pillars of the Earth"

Patriot Act

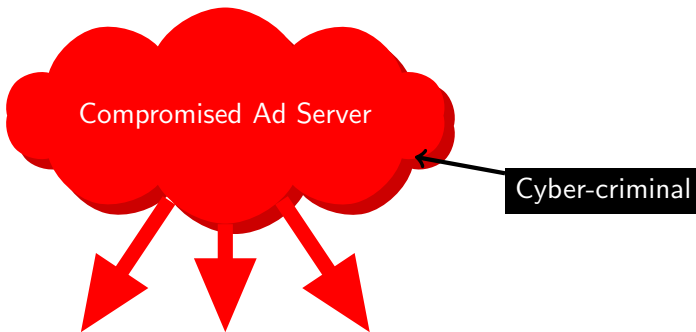
NSA

The dangers of mobile ads

Mobile phones carry personal data + camera, microphone, GPS...
Ad Server (located in the US?)



Mobile phones carry personal data + camera, microphone, GPS...



Are advertisements bad?

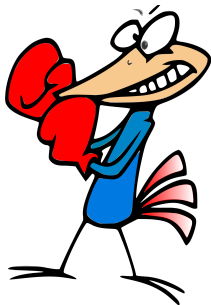


Ads are everywhere

- ▶ Since the 19th century [Wikipedia]
- ▶ Paper, streets, TV, radio, PC...

Intrusion

- ▶ *Untargeted ads are okay*
- ▶ **Targeted ads** are *borderline* TV, radio...
- ▶ **Mobile ads** go one step further: retrieve our **personal data**



Adware or Malware?

Where's the limit?

What can we do?

- ▶ Separate permissions for apps and adkits
- ▶ Opt-in/Opt-out mandatory for all adkits
- ▶ Move to non-targeted ads? then detect all privacy leaking adkits as malware
- ▶ Promote ad-less apps?
- ▶ Auto-destructible data would be great :)

Thank You !

FortiGuard Labs

Follow us on twitter: **@FortiGuardLabs**
or on our blog <http://blog.fortinet.com>

Me

twitter: @cryptax
e-mail: aapvrille at fortinet dot com



Are those PowerPoint slides? No way! It's L^AT_EX + TikZ + Beamer + [Lobster](#)