

A H E A D

Bezpečnost a mobilní aplikace

13. 4. 2017

Jakub Jeřábek
jakub.jerabek@ahead-itec.com

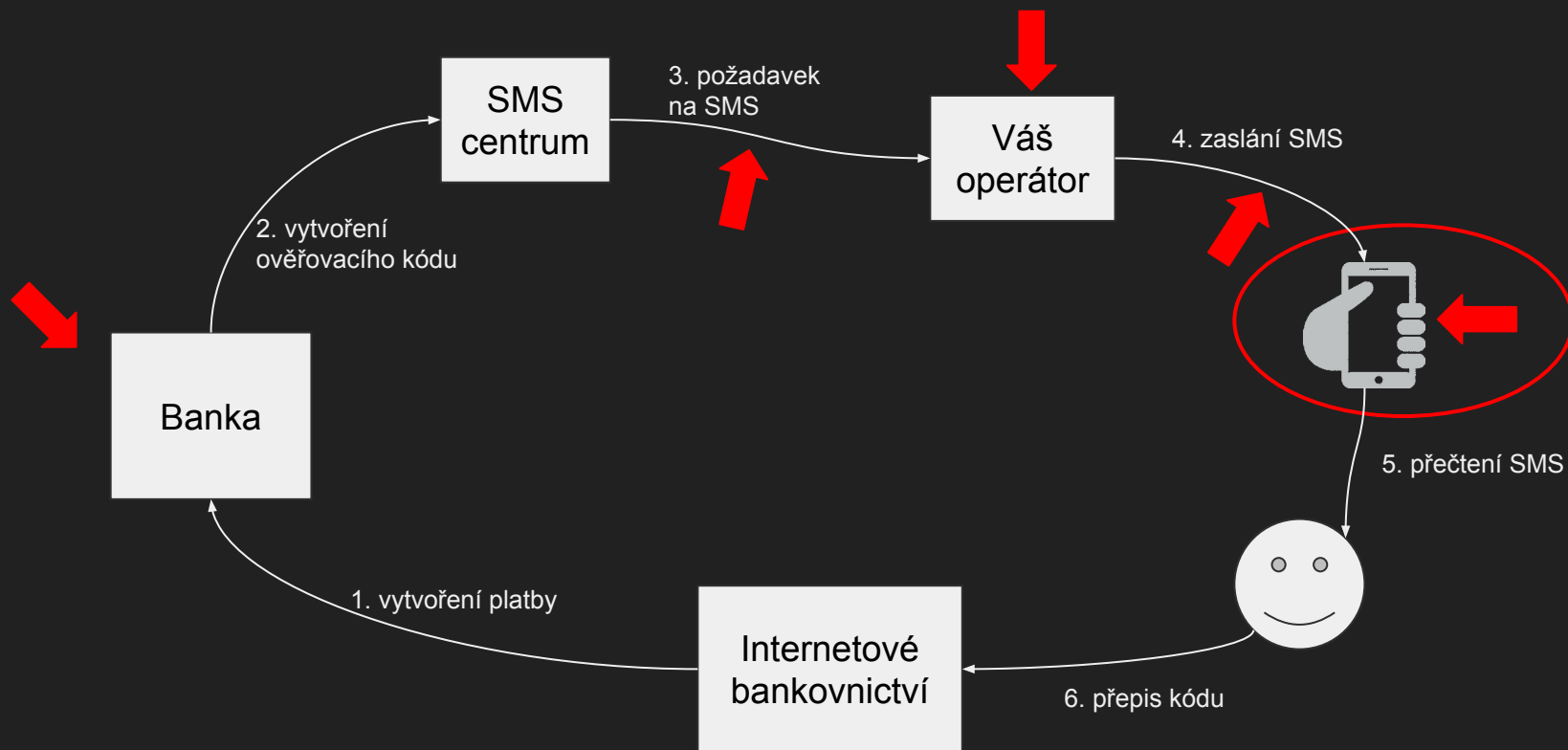


Co nás dnes čeká

1. Věříte SMS zprávám vaší banky?
2. Jak zabezpečit kód aplikace před okopírováním
3. Jak zabezpečit aplikaci před zneužitím



Věříte SMS zprávám vaší banky?



Jak Android zpracovává příchozí SMS

1. OS Android přijímá SMS zprávu
2. OS Androidu posílá zprávu všem aplikacím *
3. Aplikace, se samy rozhodují, jak s SMS zprávou naloží

* Všem, které mají zaregistrovaný receiver `android.provider.telephony.SMS_RECEIVED` a oprávnění `android.permission.RECEIVE_SMS` .

Praktická ukázka

Potřebujeme:

- zdánlivě neškodnou aplikaci
- sběrné místo SMS
- oběti

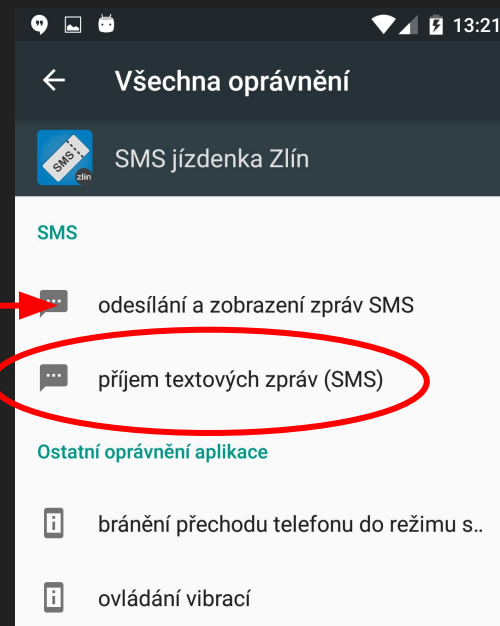
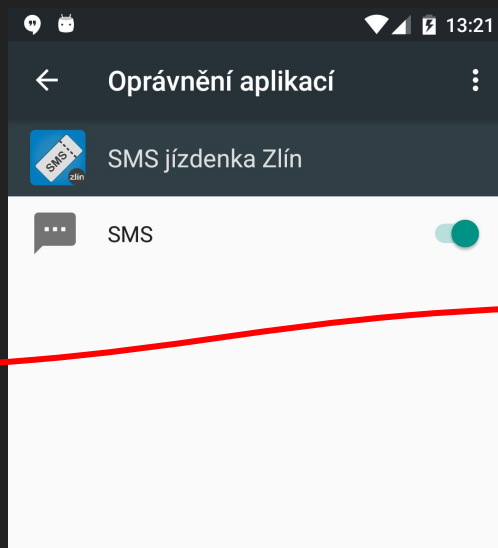
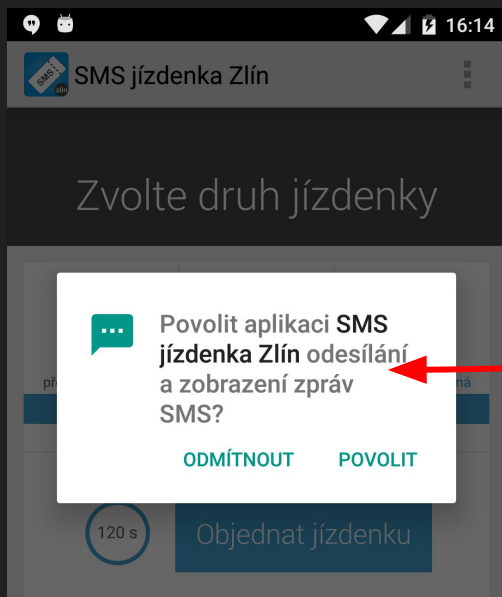
Máme:

- SMS jízdenka Zlín
 - <http://bit.ly/GPlaySMSJizdenka>
- <http://bit.ly/StolenSMS>
- Počet stažení: 1-5 tisíc

Oprávnění na Androidu 6 a 7

- krok vpřed
- `targetSdkVersion 23`
- rozdělení na *normal* a *dangerous*
 - <https://developer.android.com/guide/topics/permissions/normal-permissions.html>
 - <https://developer.android.com/guide/topics/permissions/requesting.html#normal-dangerous>
- ale...

Jak získat oprávnění bez povšimnutí



Jak je to možné?

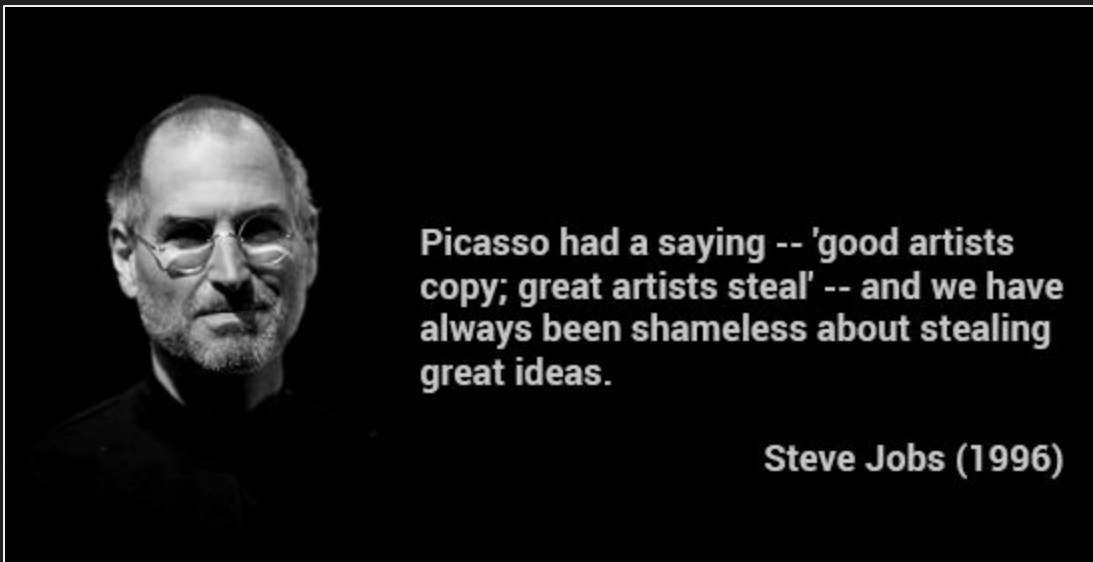
```
6 <uses-permission android:name="android.permission.SEND_SMS" />
7 <uses-permission android:name="android.permission.RECEIVE_SMS" />
8 <uses-permission android:name="android.permission.WAKE_LOCK" />
9 <uses-permission android:name="android.permission.VIBRATE" />
10 <uses-permission android:name="android.permission.INTERNET" />
```

SMS

- SEND_SMS
- RECEIVE_SMS
- READ_SMS
- RECEIVE_WAP_PUSH
- RECEIVE_MMS

- If an app requests a dangerous permission listed in its manifest, and the app already has another dangerous permission in the same permission group, the system immediately grants the permission without any interaction with the user. For example, if an app had previously requested and been granted the `READ_CONTACTS` permission, and it then requests `WRITE_CONTACTS`, the system immediately grants that permission.

YOU	CHALLENGE ACCEPTED 		 CHALLENGE COMPLETED
THIEF	 BITCH PLEASE	 LOL	 problem?



Picasso had a saying -- 'good artists copy; great artists steal' -- and we have always been shameless about stealing great ideas.

Steve Jobs (1996)

Ochrana kódu - proč?

- Softwarové patenty?
 - <https://webshop.ffii.org/>
- Flappy Birds
 - 300 klonů, 238 infikovaných
 - posílání SMS, hovory, GPS, adresáře [1]

Praktická ukázka

Potřebujeme:

- vytáhnout APK z telefonu
- dekompilovat APK
- umět číst v cizím kódu

Máme:

- TCMD, APK extractor, ...
- APK Tool [\[1\]](#)
- ???

Pozor na řetězce!

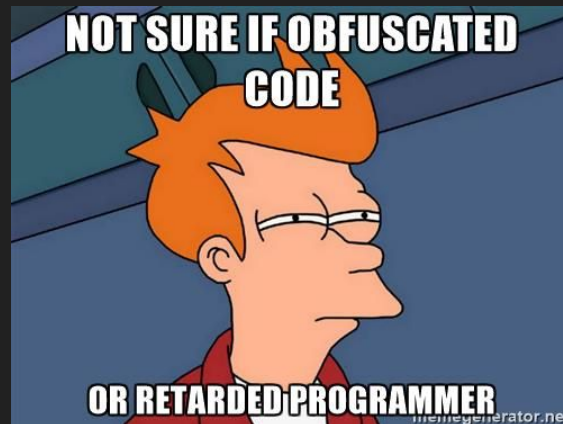
Pro zájemce: <https://www.fi.muni.cz/research/laboratories/crocs.xhtml.cs>

Ochrana kódu - jak?

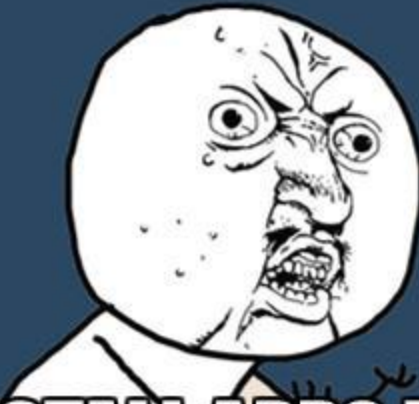
- Obfuskace při buildu [\[1\]](#)
 - SDK/tools/proguard/proguard-android.txt

```
14  buildTypes {
15      debug {
16          minifyEnabled false
17          proguardFiles 'proguard-rules.pro'
18      }
19      release {
20          minifyEnabled true
21          proguardFiles 'proguard-rules.pro'
22      }
23  }
```

- Obfuskace při psaní



APP DOWNLOADERS



**Y U INSTALL APPS FROM
ULOZ.TO?**

memegenerator.net

Ochrana aplikace - proč?

- Reputace
- Ochrana klientů / komunity

Ochrana aplikace - jak?

- Kontrola certifikátu APK
- Kontrola původu APK
 - Google Play
 - odjinud
- Knihovna: <https://github.com/SandroMachado/AndroidTampering>

Děkuji za pozornost

Prostor pro vaše dotazy