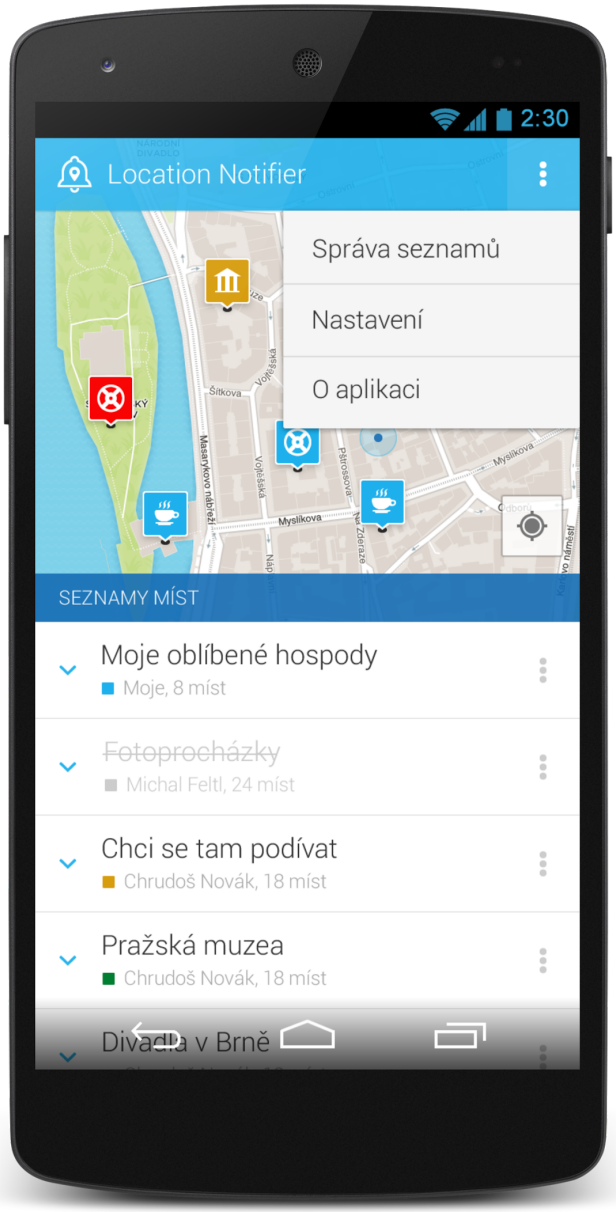
Jak zabezpečit Android aplikaci?

workshop, Michal Vojtíšek

The NFL Mobile App, so popular these days due to the Super Bowl kick off approaching, has been found to leak the log-in credentials, as well as the email address, of the user during calls to the nfl.com domain.

http://news.softpedia.com/news/NFL-Mobile-App-Leaks-User-Credentials-Email-Address-471365.shtml

2 000 000 stažení


2:30
Location Notifier
Správa seznamů
Nastavení
O aplikaci
SEZNAMY MÍST
Moje oblíbené hospody
Moje, 8 míst
Fotoprocházky
Michal Feltl, 24 míst
Chci se tam podívat
Chrudoš Novák, 18 míst
Pražská muzea
Chrudoš Novák, 18 míst
Divadla v Brně


Čtyřdílná
5. května

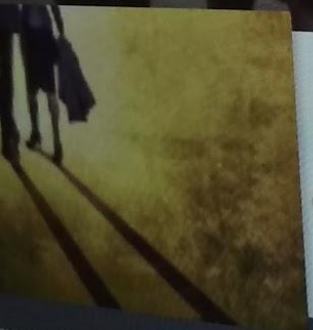

t group are employees
pot. Second group ar
eir cars in TMCZ
d second group upon
Without first group n
ery and without lot


CZECH
GLASS
NTBR3902
lenovo
X230
Augmented
FACE
EPSON


M.A.D.S.
Ioan Grozav
Marian Jaworski
Dragoș Iftimi
Vassil Angelov
Sándor Bokor
Georg Hofmann
Michal Vojtíšek
mbed
Enabled
QC
1421

Qool - kulturní přehled

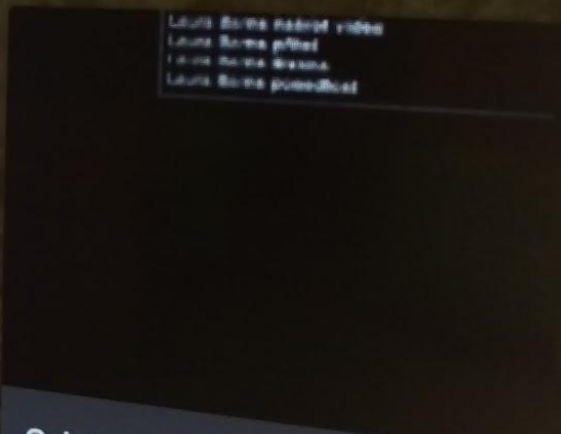
ové premiéry 2015



ma ve zlatém
min, 75%, 25. 6. 2015

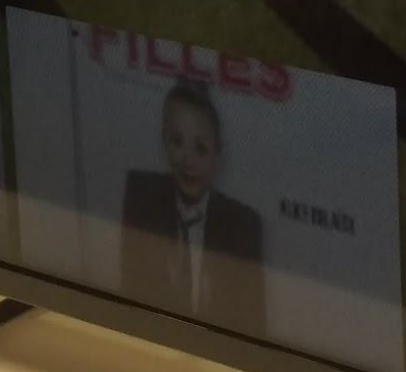
Mimoni
25. 6. 2015

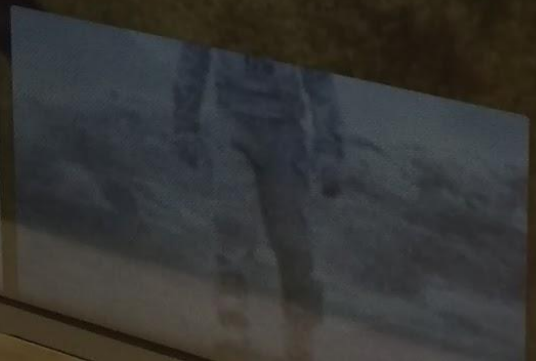
Andílek na nervy
105 min, 18. 6. 2015



Odebrat z přátel
83 min, 59%, 18. 6. 2015

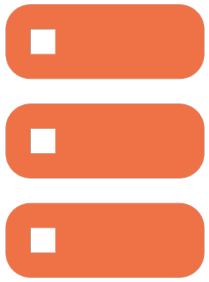
imové premiéry 2014





Jak zabezpečit Android aplikaci?

Může to udělat někdo jiný?



Data

Security model

Nástroje

Guidelines

Zabezpečení aplikace

Veřejná

RSS, počasí, fotky, hledání, web

Zabezpečená

Kontrolované přístupy
twitter, facebook, google plus, vlaky

Podepsaný přístup
Google Apis

Privátní

Identita uživatele
e-mail, historie nákupů, kalendář, letenky, pozice, finance, oblíbená místa

Zabezpečené API

Klíče

Security model

kde Android pomáhá?

Android Security State of the Union 2014

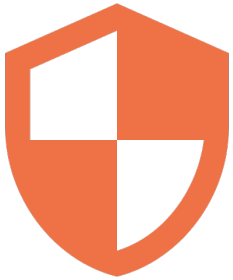
```
<?xml version="1.0" encoding="utf-8"?>
<manifest xmlns:android="http://schemas.android.com/apk/res/andr
    package="com.example.app">

    <uses-permission android:name="android.permission.INTERNET"

    <permission
        android:name="com.example.app.permission.C2D_MESSAGE"
        android:protectionLevel="signature" />

    <uses-permission android:name="com.example.app.permission.C2

    <application
        android:icon="@midmap/ic_launcher"
        android:label="@string/app_name">
```



Security model

kde Android pomáhá?

Obecně

- **Symetrické šifry**

  DES, AES
- **Asymetrické šifry**

  RSA, SSL

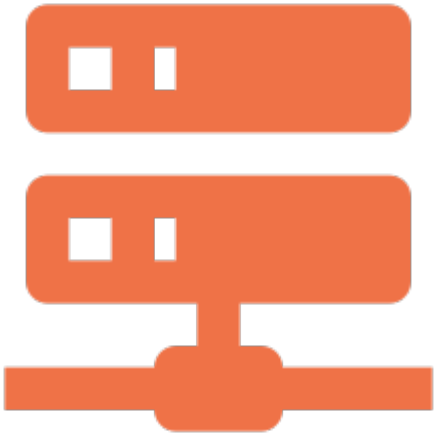
Android

- <permission name="..." />
- KeyChain
- Fingerprint API
- podpis aplikace

Jak(é) nástroje pomůžou?

Kontroluje to někdo?!

Kolega



Build server

Google Play

Co požadují různé security guidelines a jak jim vyhovět

bezpečně uložená
zabezpečená data

šifrovaná
privátní data

privátní klíč
od uživatele

Možnosti zabezpečení dat při přenosu i ukládání

JAVA

```java
HttpsURLConnection
  .setDefaultHostnameVerifier(new HostnameVerifier() {
      public boolean verify(String hostname, SSLSession session) {
          return true;
      }
  });
  .setDefaultSSLSocketFactory(getContext().getSocketFactory());

SSLContext
  .getInstance("TLS")
  .init(null, new X509TrustManager[] {
      new X509TrustManager() {
          ....
      }
  }, new SecureRandom());
```

Možnosti zabezpečení dat při přenosu i ukládání

JAVA

```java
public class CryptoDemo {

    static {
        System.loadLibrary("crypto-jni");
    }

    public native String getInitVector();

    public native String getKey();
}
```

Možnosti zabezpečení dat při přenosu i ukládání

JAVA

```
Intent intent = KeyChain.createInstallIntent();
byte[] p12 = readFile("keystore-test.pfx");
intent.putExtra(KeyChain.EXTRA_PKCS12, p12);
startActivity(intent);
```

Workshop

Jak se bránit?

Má to vůbec cenu?

Díky

http://michal.vojtisek.cz