



FAKULTA  
INFORMATIKY  
Masarykova univerzita

# Detekcia prebalených aplikácií v OS Android

---

Diplomová práca  
Martin Styk

## Ciele práce

- Preskúmať problematiku prebaľovania aplikácií
- Navrhnúť systém detekcie prebalených aplikácií
- Vytvoriť mobilnú aplikáciu na získavanie metadát o aplikáciách
- Implementovať mechanizmus detekcie potenciálne modifikovaných aplikácií

# Prebalené aplikácie

*Možnosti a hrozby modifikácie Android aplikácií*

- Aplikácie distribuované ako inštalačné APK balíčky
- Jednoduchá modifikácia
- Postup prebalenia
  - Stiahnutie originálu
  - Rozbalenie a dekompilácia
  - Pridanie škodlivej funkcionality
  - Zabalenie
  - Podpis
  - Distribúcia
- Spôsob šírenia malvéru

# Systém detekcie prebalených aplikácií

## Požiadavky a návrh

### Požiadavky

- Sprístupnenie užívateľom
- Určenie, ktorá aplikácia je originál a ktorá je prebalená kópia
- Detekcia prebalených aplikácií pochádzajúcich výhradne z alternatívnych obchodov
- Dynamická aktualizácia dát potrebných na detekciu prebalených súborov

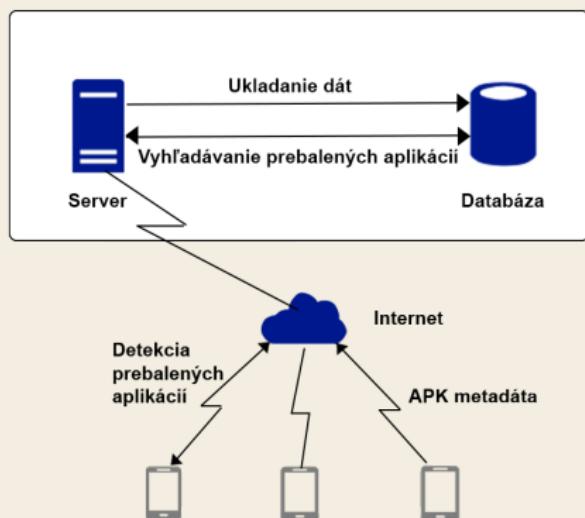
### Etapy detekcie prebalených aplikácií

- Extrakcia dát o aplikáciách
- Určenie prebalených aplikácií

# Systém detektie prebalených aplikácií

## Návrh

- Mobilná aplikácia
  - Extraktia metadát o aplikáciách
- Zdieľaná databáza
  - Úložisko metadát
- Server
  - Algoritmus detektie prebalených aplikácií



# Mobilná aplikácia Apk Analyzer

## Úvod

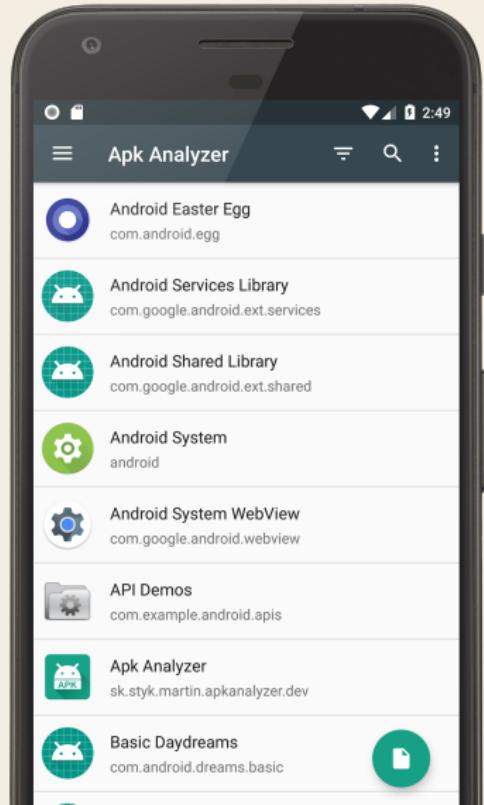
- Analýza nainštalovaných aplikácií
  - Prezentácia dát užívateľom
  - Extrakcia pre detekciu prebalenosť
- Presadiť sa medzi ostatnými aplikáciami
  - Google Play - vysoká konkurencia
  - Lepšie služby ako konkurencia
  - Lepšie používateľské rozhranie



# Mobilná aplikácia Apk Analyzer

## Zoznam aplikácií

- Všetky nainštalované aplikácie
- Filtrovanie
  - Názov
  - Meno balíka
  - Zdroj (Google Play, predinštalované,...)
- Výber nenainštalovanej aplikácie



# Mobilná aplikácia Apk Analyzer

## Detail aplikácie

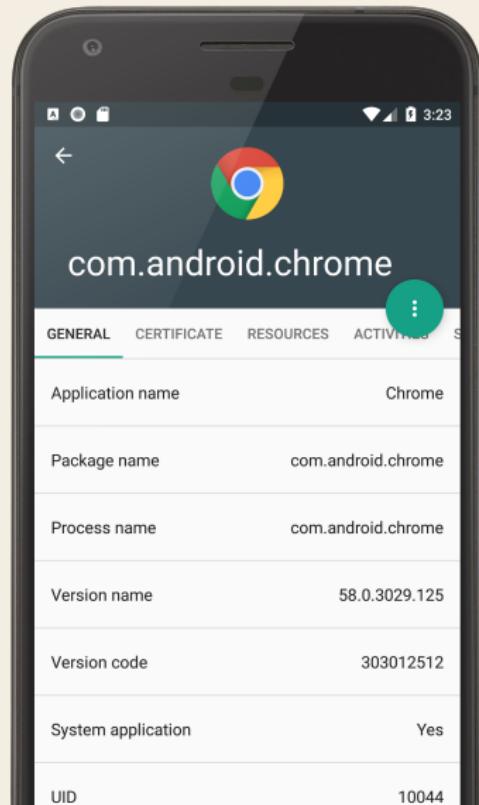
- Všeobecné informácie
- Podpis aplikácie
- Zdrojové súbory
- Komponenty
- Bezpečnostné povolenia
- Vyžadované vlastnosti zariadenia
- DEX súbor



# Mobilná aplikácia Apk Analyzer

## Operácie s aplikáciami

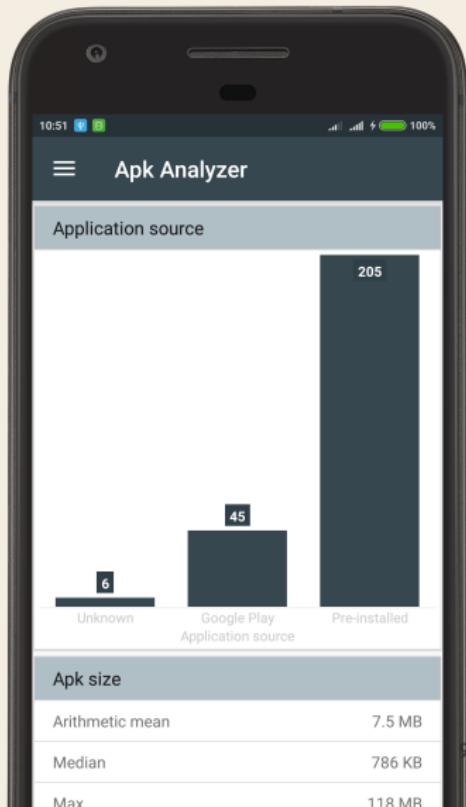
- Zobrazenie  
AndroidManifest.xml
- Kontrola originality (detekcia prebalenosť)
- Export inštalačného súboru
- Zdieľanie inštalačného súboru
- Export ikony



# Mobilná aplikácia Apk Analyzer

## Štatistiky

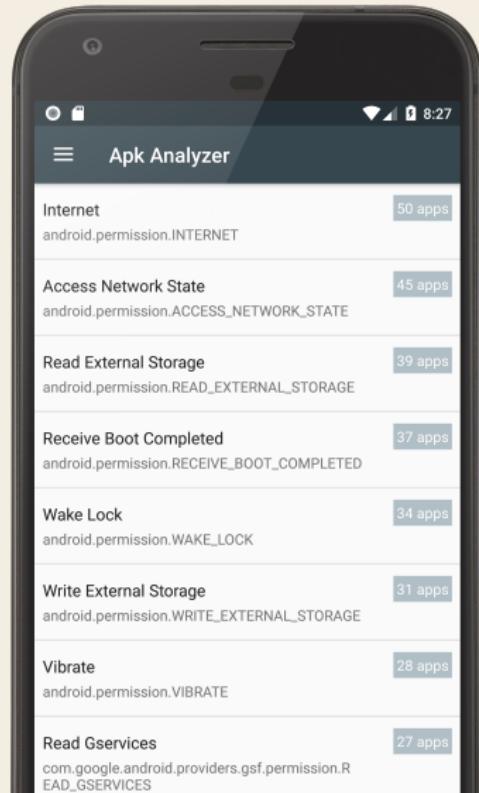
- Podporované verzie Android
- Algoritmus podpisu
- Inštalačná politika
- Zdroj aplikácie
- Veľkosť aplikácie
- Počet povolení
- Počet obrázkov
- Počet obrazoviek



# Mobilná aplikácia Apk Analyzer

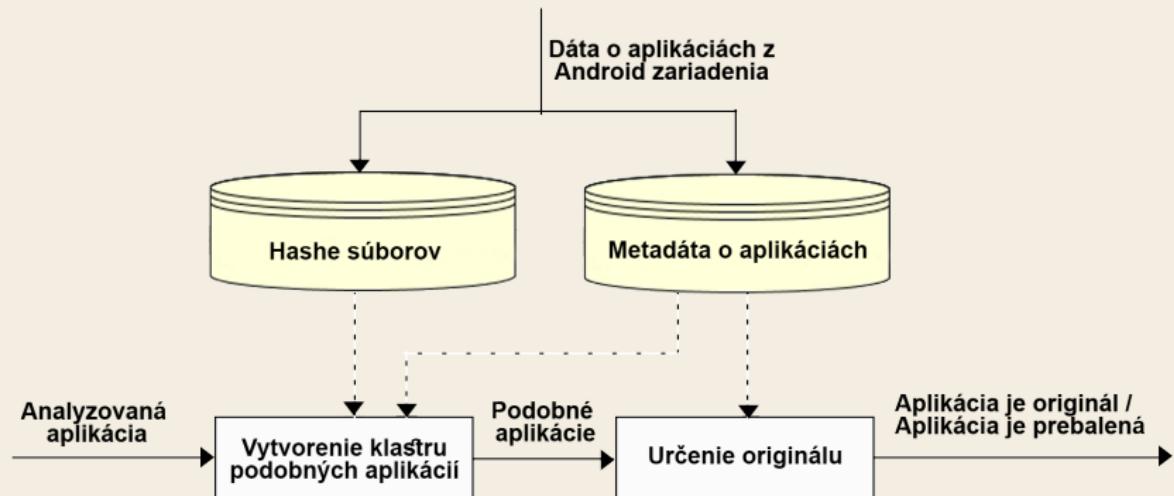
## Bezpečnostné povolenia

- Zoznam všetkých povolení
- Počet aplikácií vyžadujúcich povolenie
  - Udelené
  - Neudelené
- Skupina povolenia
- Popis povolenia



# Detekcia prebalených aplikácií

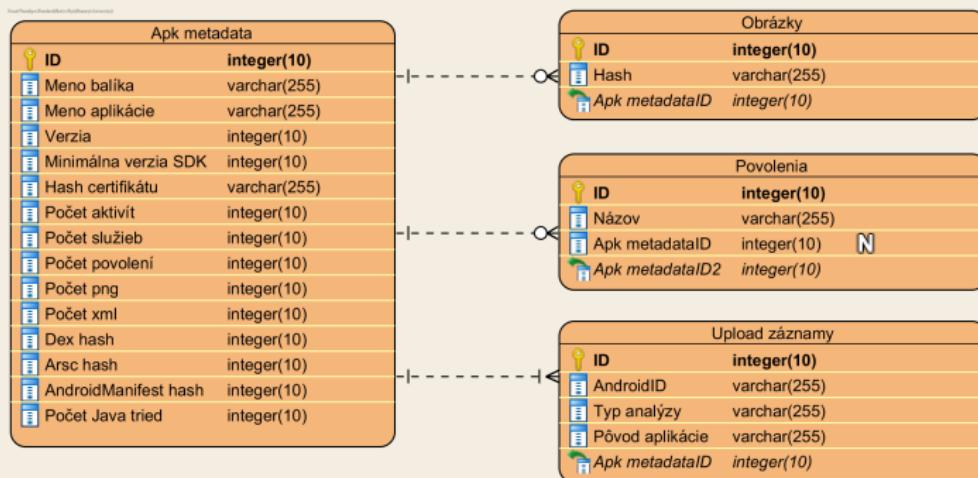
## Model detektie



# Detekcia prebalených aplikácií

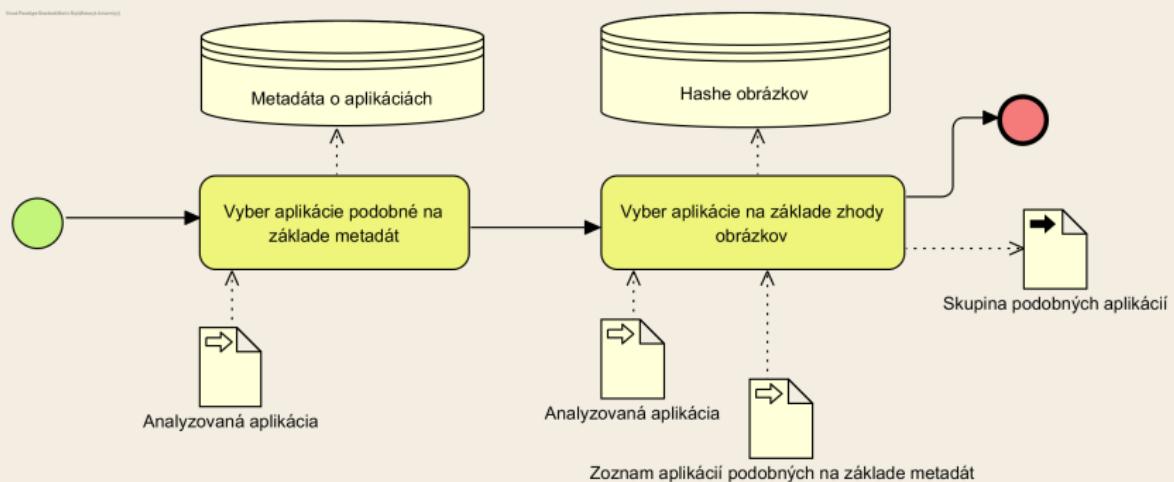
## Databáza

- Metadáta získané od mobilnej aplikácie
- Zamedzenie duplikáciám



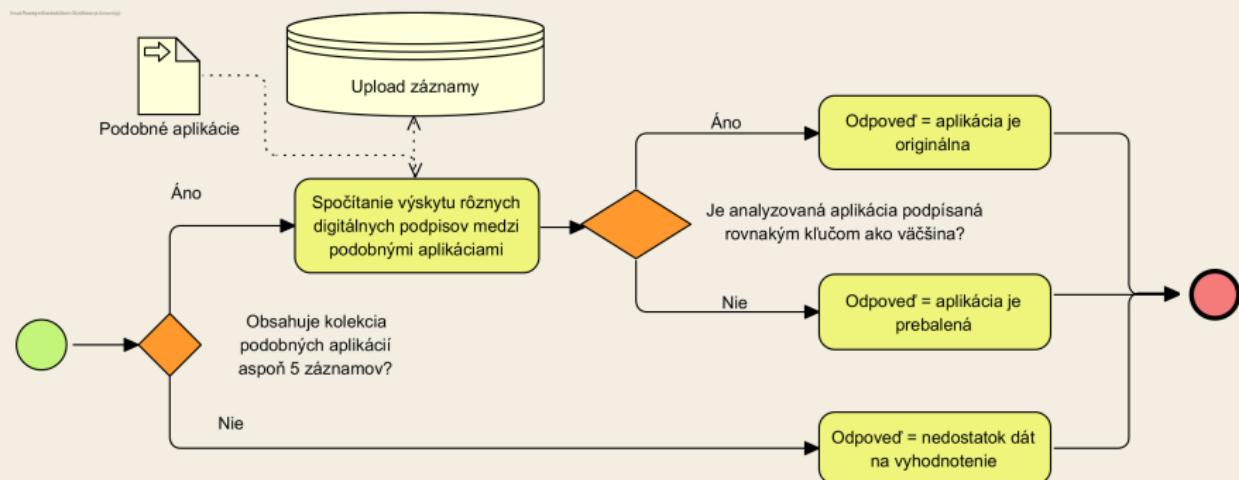
# Detekcia prebalených aplikácií

## Klaster podobných aplikácií



# Detekcia prebalených aplikácií

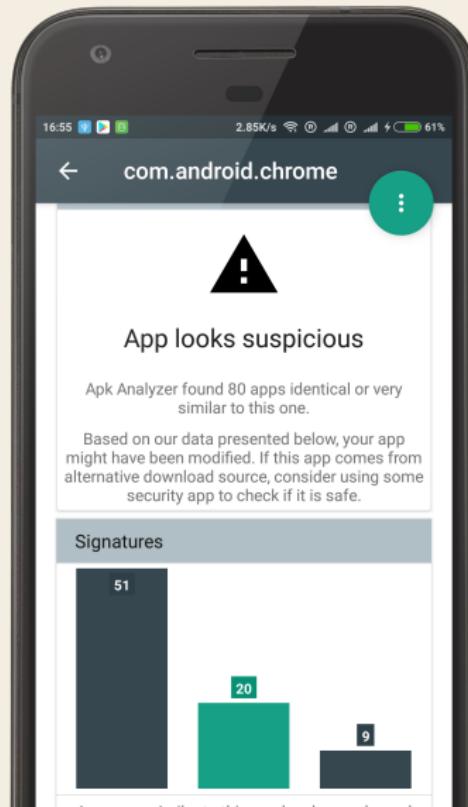
## Určenie originálu



# Detekcia prebalených aplikácií

## Výstup v mobilnej aplikácii

- Výstup detektie
- Počet identifikovaných podobných aplikácií
- Rôzne digitálne podpisy medzi podobnými aplikáciami



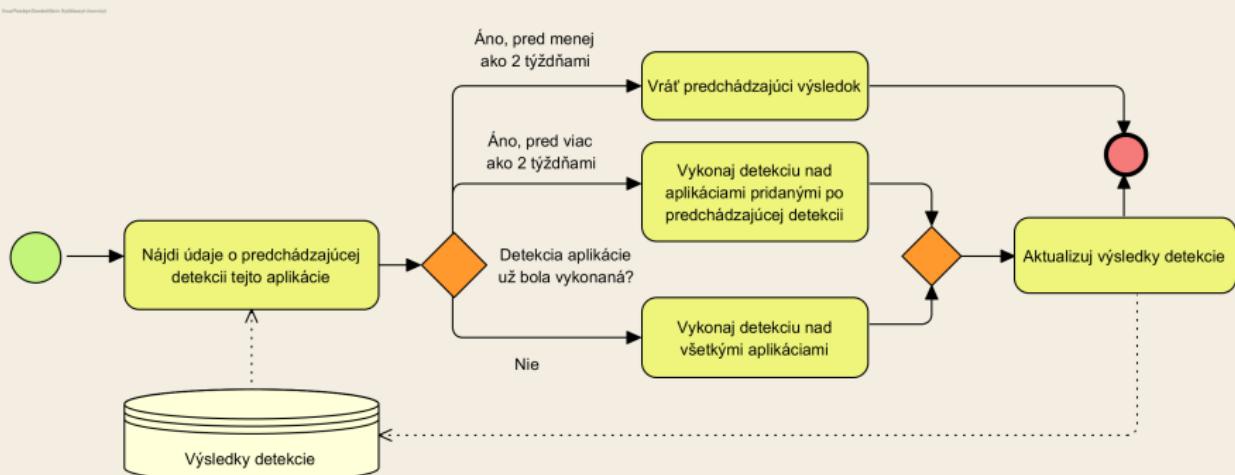
# Detekcia prebalených aplikácií

## Predpoklady

- Porovnanie hashov obrázkov
  - Rýchlosť
  - Možnosť extrakcie mobilným klientom
  - Malá pravdepodobnosť modifikácie (0.073) [1]
    - » *Evaluation of Resource-Based App Repackaging Detection in Android*
- Originálnych aplikácií je viac ako prebalených
- Nastavenie parametrov detektie na základe predchádzajúcich výskumov [2]
  - *FSquaDRA: Fast Detection of Repackaged Applications*

# Detekcia prebalených aplikácií

## Optimalizácia



# Nasadenie systému

## Mobilná aplikácia

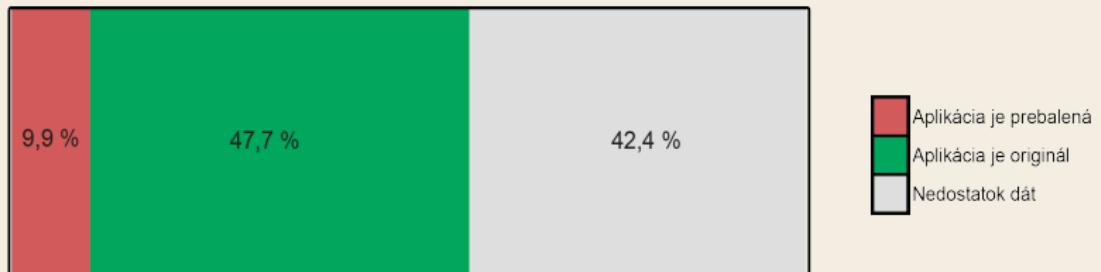
- 41 000 inštalácií
- 12 000 aktuálne aktívnych inštalácií
- 4,6 ★ (225 hodnotení)



# Nasadenie systému

## *Detekcia prebalených aplikácií*

- Databáza
  - 1 milión záznamov
  - 285 000 rôznych aplikácií
  - 16 000 zariadení
- Detekcia
  - 7 500 spustených detekcií



# Bibliografia

## Analýza inštalačných APK súborov pre OS Android

- [1] GADYATSKAYA, Olga et al. Evaluation of Resource-Based App Repackaging Detection in Android. In: Secure IT Systems: 21st Nordic Conference, NordSec 2016, Oulu, Finland, November 2-4, 2016. ISBN 978-3-319-47560-8.
- [2] ZHAUNIAROVICH, Yury et al. FSquaDRA: Fast Detection of Repackaged Applications. In: Data and Applications Security and Privacy XXVIII: 28th Annual IFIP WG 11.3 Working Conference, DBSec 2014, Vienna, Austria, July 14-16, 2014. ISBN 978-3-662-43936-4.