Analýza zraniteľností smartfónov na platforme Android

JÁN PARASKA

DOC. RNDR. JOZEF JIRÁSEK, PHD.

ÚINF

Ciele

- Analýza známych útokov na implementácie systému Android
- Implementácia nástroja na identifikáciu nebezpečnej/zraniteľnej aplikácie

Postup za uplynulý semester

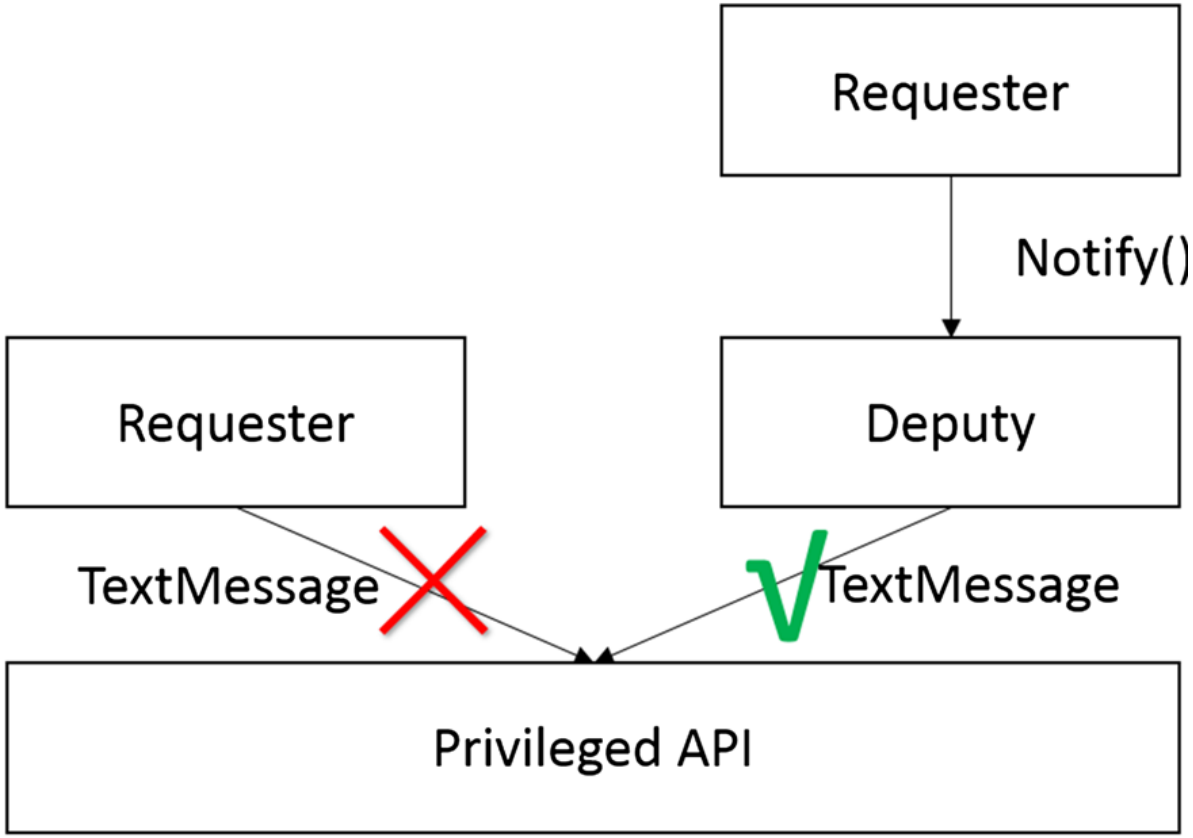
- Statická analýza
  - Eskalácia oprávnení - „Confused deputy“ útok
  - Motivácia
    - S narastajúcim počtom developerov sa zvyšuje počet „zle“ naprogramovaných aplikácií
      - Sep 2017 – cca 3 300 000 aplikácií na Google Play
    - Aplikácie obsahujúce bezpečnostné medzery podkopávajú bezpečnosť a súkromie
    - Ošetrenie špecifickej zraniteľnosti zameranej na neoprávnené získanie oprávnení (privilege escalation)
  - Systemical detection of Confused deputy attack - Jianliang Wu, Tingting Cui, Tao Ban, Shanqing Guo, Lizhen Cui

Confused deputy attack

- Komponenty aplikácie:
  - Activities – poskytujú používateľské rozhranie
  - Services – bežiace na pozadí, napr. sťahovanie
  - Content providers – nástroj na ukladanie a zdieľanie dát
  - Broadcast receiver-y – počúvajú na *Intenty* odosielané rôznymi komponentmi a aplikáciami
    - Pri obdržaní špecifického Intentu spustia úlohu na pozadí a výsledok môžu poslať iniciátorovi.
- Exportované komponenty
  - Spustiteľné inými aplikáciami
    - android:exported= "true„
    - intent-filter

Confused deputy attack - scenár

- Žiadateľ nemá oprávnenie na odoslanie SMS
  - Interný katalóg - zoznam komponentov schopných prijať *Intent*
  - Exportované komponenty
- Pošle *Intent* tejto aktivite
- Vyvolaná aplikácia „legálne“ urobí špinavú prácu



Analýza zraniteľnej aplikácie

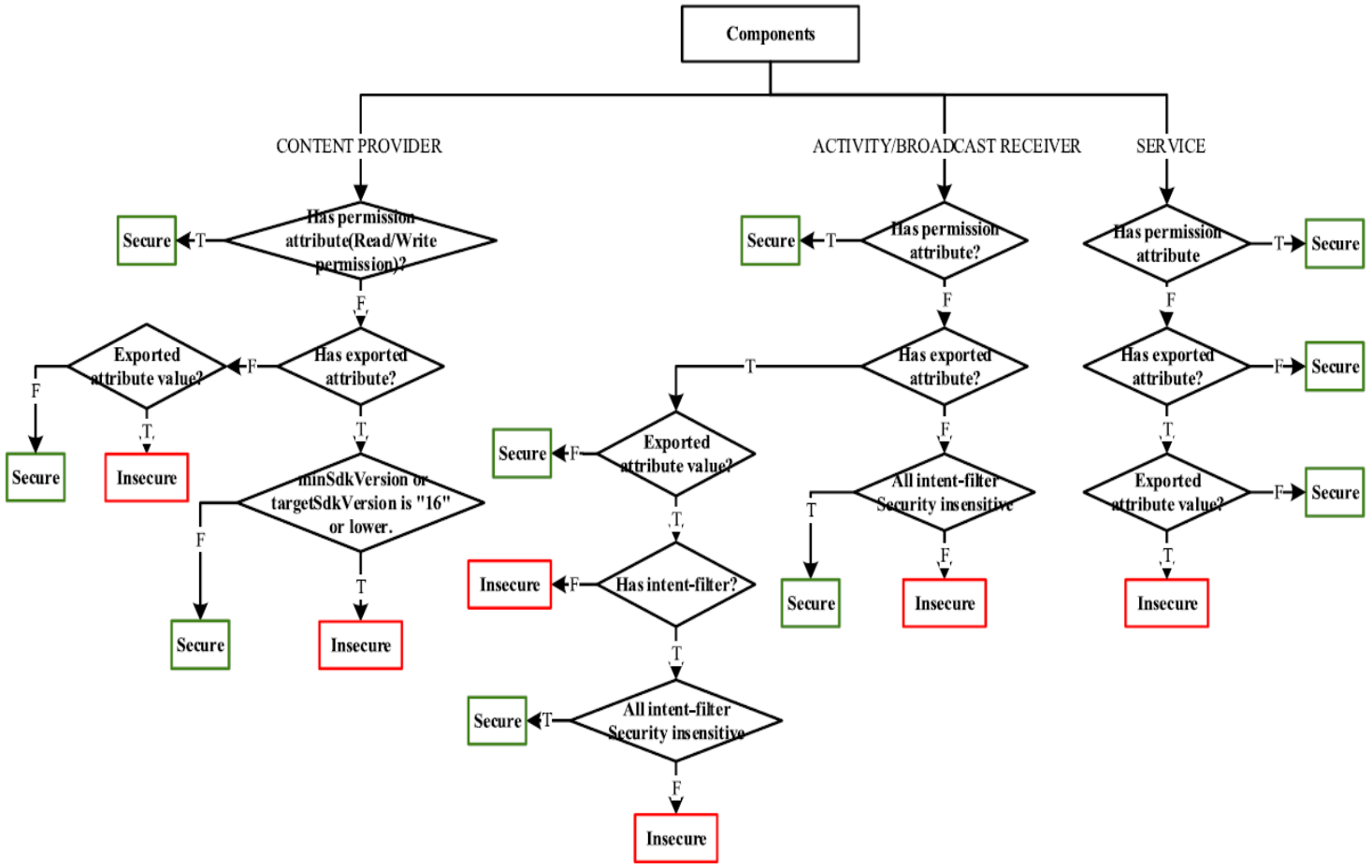
- Objavenie potenciálne zraniteľných komponentov
  - Extrahovanie komponentov z manifestu
  - Analýza nastavených atribútov
- Analýza potenciálne zraniteľných komponentov
  - Vytvorenie CFG
    - Komponentový CFG
    - Medzi-komponentový CFG

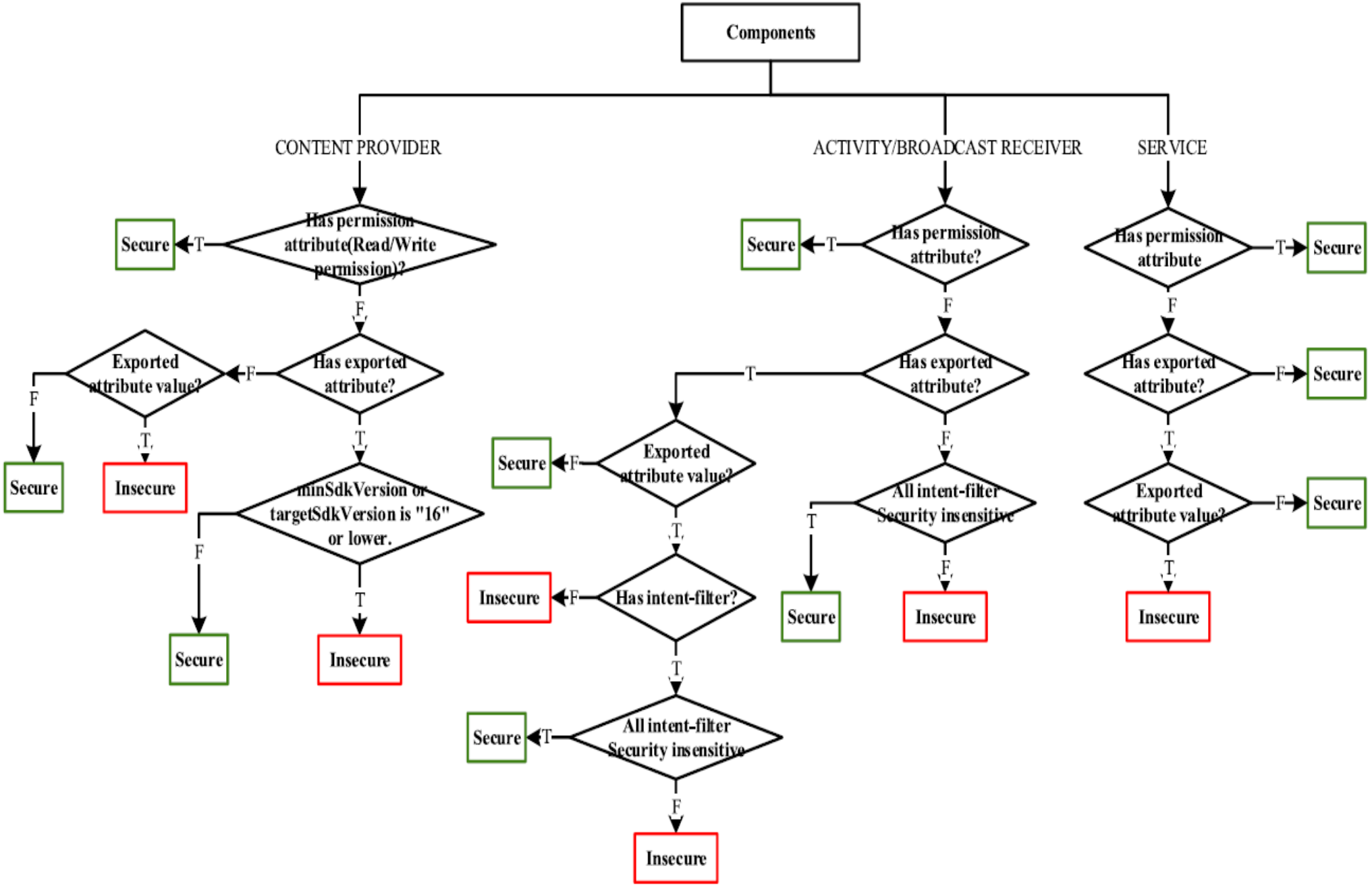
Objavenie potenciálne zraniteľných komponentov

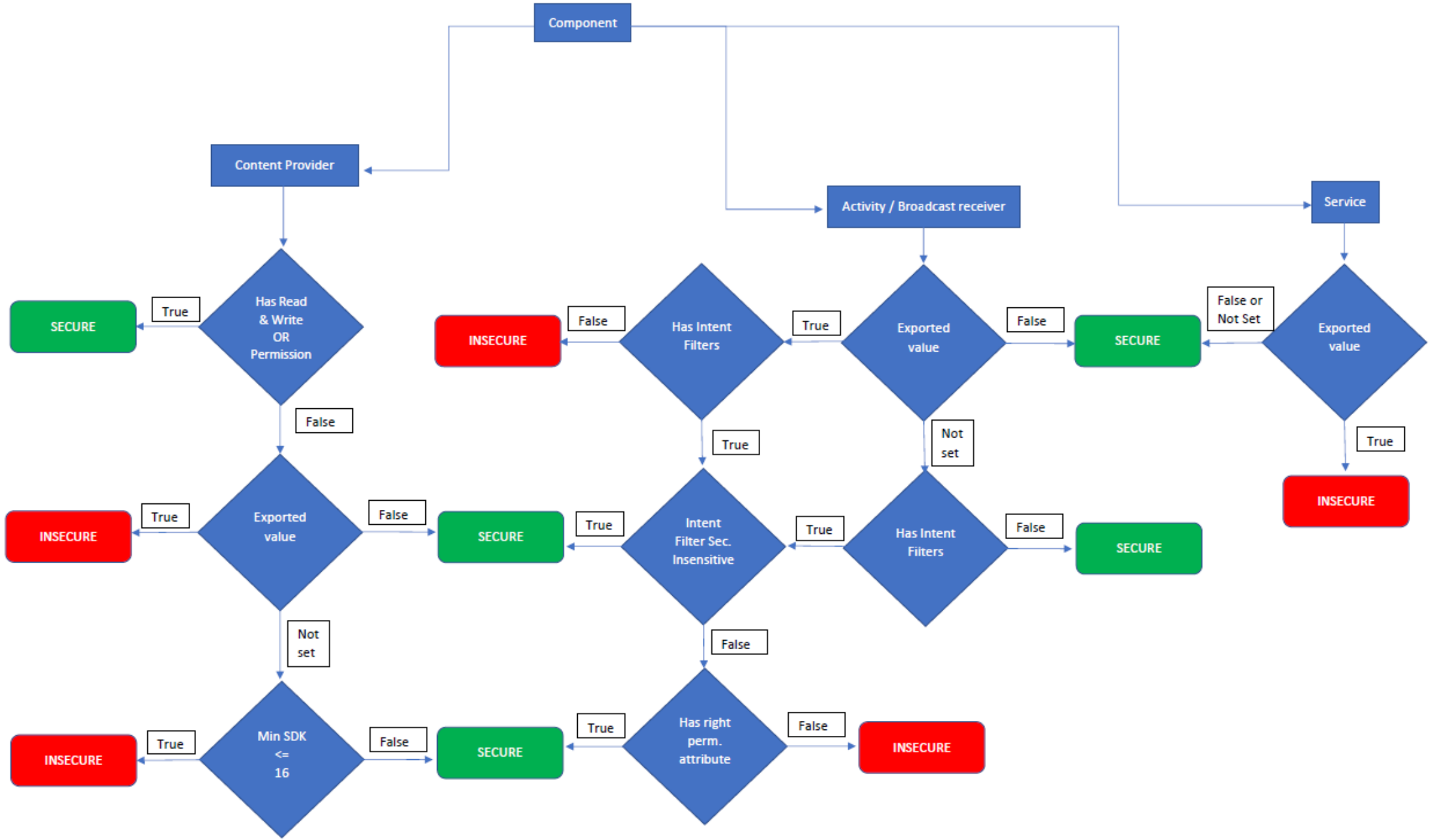
```
<activity
        android:name=".Listsms"
        android:label="@string/app_name"
        android:exported="false" >
</activity>

<activity
        android:name=".ActSendSms"
        android:label="@string/app_name" >
        <intent-filter>
                <action android:name="android.intent.action.VIEW" />
                <action android:name="android.intent.action.SENDTO" />
        </intent-filter>
</activity>

<activity
        android:name=".MainActicity"
        android:label="@string/app_name" >
        exported="true"
</activity>
```




Components
CONTENT PROVIDER
ACTIVITY/BROADCAST RECEIVER
SERVICE
Has permission attribute(Read/Write permission)?
Secure
T
F
Has exported attribute?
Exported attribute value?
Secure
Insecure
minSdkVersion or targetSdkVersion is "16" or lower.
Secure
Insecure
Has permission attribute?
Secure
Has exported attribute?
Exported attribute value?
Secure
Has intent-filter?
Insecure
All intent-filter Security insensitive
Secure
All intent-filter Security insensitive
Secure
Insecure
Has permission attribute
Secure
Has exported attribute?
Secure
Exported attribute value?
Secure
Insecure


Component
Content Provider
Activity / Broadcast receiver
Service
Has Read & Write OR Permission
True
SECURE
False
Exported value
True
INSECURE
False
SECURE
Min SDK <= 16
True
INSECURE
False
SECURE
Not set
Intent Filter Sec. Insensitive
True
SECURE
False
Has right perm. attribute
True
SECURE
False
INSECURE
Has Intent Filters
True
INSECURE
False
SECURE
Not set
Exported value
True
INSECURE
False
SECURE
Has Intent Filters
True
SECURE
False
Exported value
True
INSECURE
False or Not Set
SECURE

Analýza zraniteľnej aplikácie

- Objavenie potenciálne zraniteľných komponentov
  - Extrahovanie komponentov z manifestu
  - Analýza nastavených atribútov
- Analýza potenciálne zraniteľných komponentov
  - Vytvorenie CFG
    - Komponentový CFG
    - Medzi-komponentový CFG

Analýza zraniteľnej aplikácie

- Objavenie potenciálne zraniteľných komponentov
  - Extrahovanie komponentov z manifestu
  - Analýza nastavených atribútov
- Analýza potenciálne zraniteľných komponentov
  - Vytvorenie CFG
    - Komponentový CFG
    - Medzi-komponentový CFG

Starts another Activity	Starts another Service	Starts another Receiver
startActivity	bindService	sendBroadcast
startActivityForResult	startService	sendOrderedBroadcast
startNextMatchingActivity	stopService	sendStickyBroadcast
startActivityIfNeeded		sendStickyOrderedBroadcast
startActivityFromChild		
startActivityFromFragment		

Čo teraz?

- Dostupné informácie:
  - Identifikované potenciálne zraniteľné komponenty
  - CFG aplikácie
- Identifikácia bezpečných komponentov
  - Neobsahujú volania nebezpečných funkcií
  - Obsahujú volania nebezpečných funkcií ale kontrolujú potrebné povolenia
    - Context.checkCallingPermission()
    - Context.checkPermission()
- Identifikácia nebezpečných komponentov
- Obsahujú volania nebezpečných funkcií a existuje k nim cesta (v CFG) z verejných komponentov

Sensitive function categories	Function number	Descriptions
Telephony identifiers	23	IMEI, IMSI, MCC, MNC, LAC, CID, etc.
Account information	19	account name, account password, etc.
GPS coordination	4	current GPS Geo location
Web browser information	11	browser history
WIFI connection information	14	WiFi credentials, MAC address, etc.
Audio video flow	2	call recording, video capture, etc.
Telephony services abuse	3	premium SMS sending, phone call composition...
Arbitrary code execution	7	native code...

Uplynulý semester – čo je hotové?

- Statická analýza
  - Eskalácia oprávnení - „Confused deputy“ útok
  - Objavenie potenciálne zraniteľných komponentov
    - Extrakcia Manifestu z apk súboru – projekt apk-manifest-extractor
    - Implementácia analýzy komponentov aplikácie(java)
  - Analýza potenciálne zraniteľných komponentov
    - Konštrukcia CFG – knižnice soot(-inflow, -android), súčasť nástroja FlowDroid
    - Implementácia analýzy potenciálne zraniteľných komponentov(java)

Uplynulý semester – čo nie je hotové?

- Statická analýza
  - Eskalácia oprávnení - „Confused deputy“ útok
  - Objavenie potenciálne zraniteľných komponentov
    - Definovanie nebezpečných akcií intentu
  - Analýza potenciálne zraniteľných komponentov
    - Definovanie nebezpečných fukcií
  - Analýza väčšej vzorky aplikácií

Ďakujem za pozornosť