Exploiting missing permission in Android

Martin Gazdík, Juraj Varga

30.09.2013, EUROPEN 2013

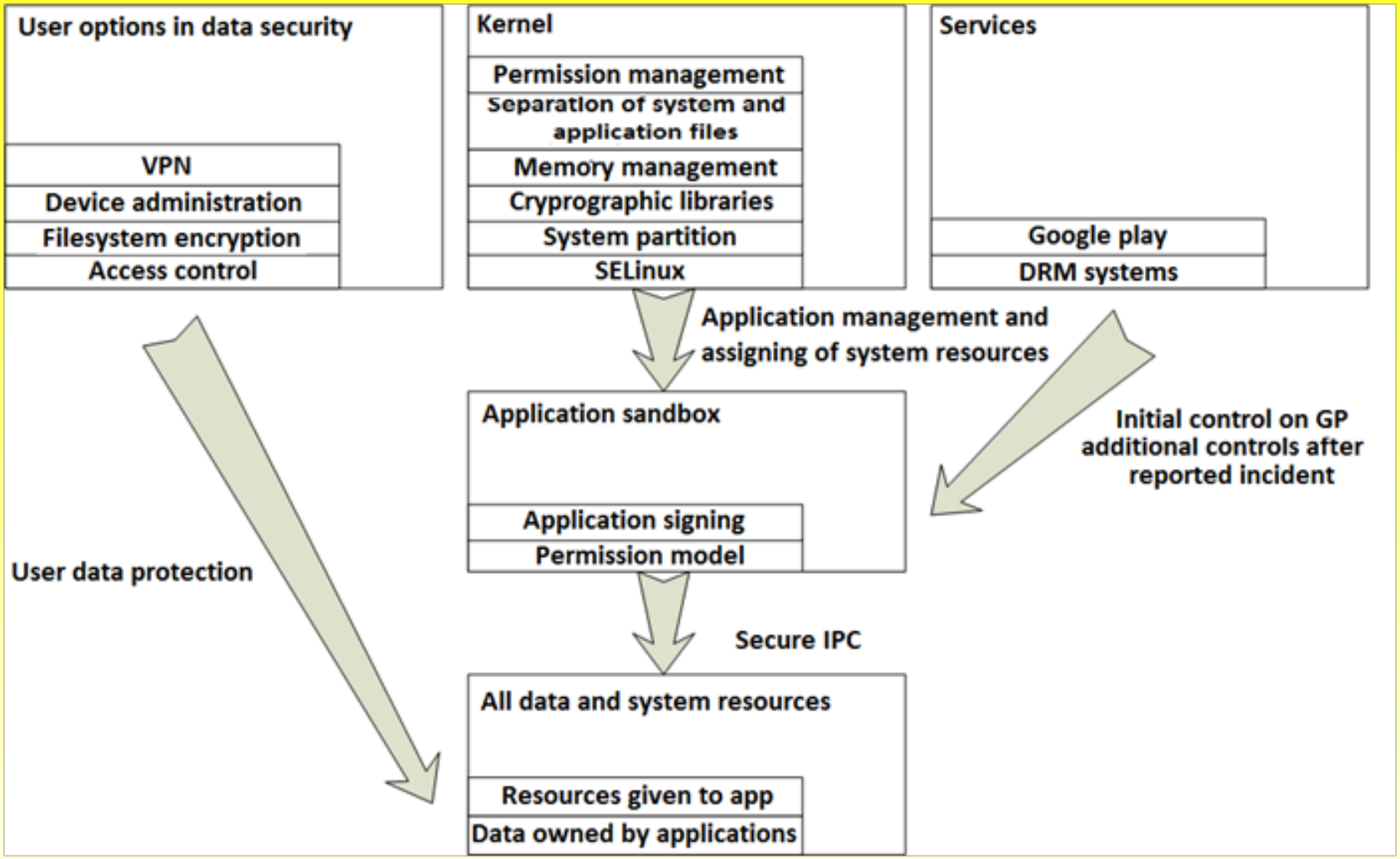
Outline

- OS Android - krátke info.
- Android permission model.
- Plán útoku - navrhnuté aplikácie.
- Experimenty.
- Výsledky a protiopatrenia.
- Záver.

OS Android

- Najrozšírenejší mobilný OS - počet používateľov a zariadení.
- Upravená Linuxová architektúra.
- Otvorená platforma - dobrý cieľ rôznych infekcií.
- Obsahuje viacero bezpečnostných mechanizmov.

Bezpečnostná architektúra OS Android

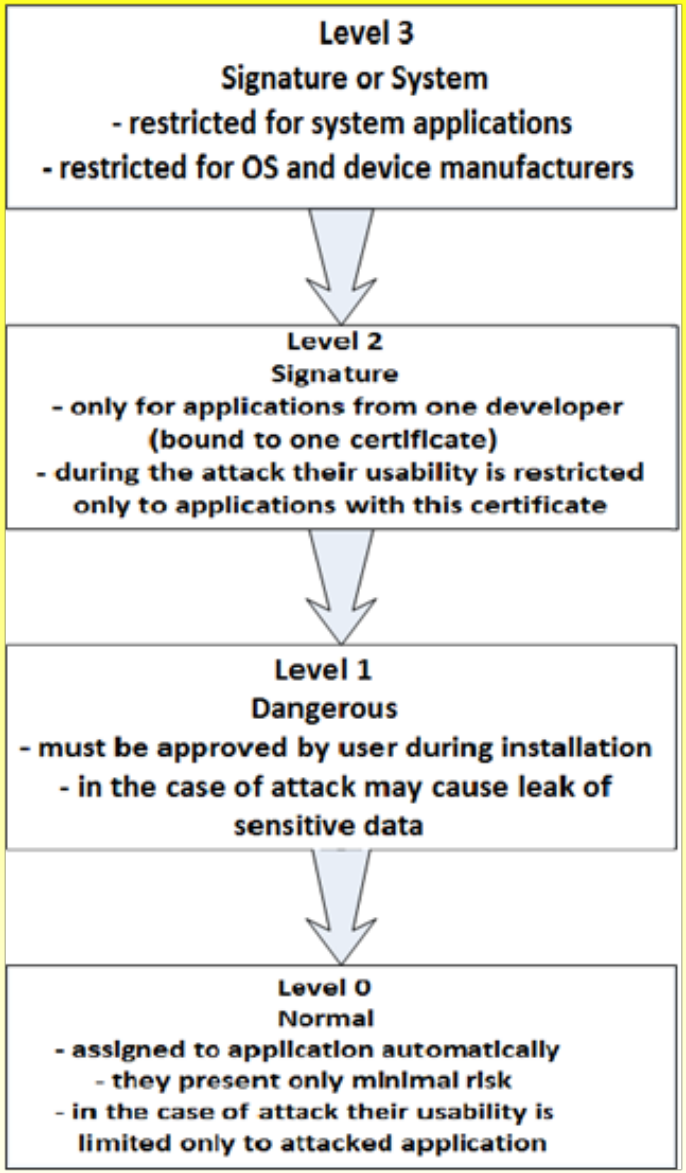


Android permission model

- Základ bezpečnosti Androidu.
- Špecifický pre platformu.
- Súvisí s aplikačným sandboxom -> limituje prístup k systémovým zdrojom.
- Zneužitie resp. chyby v pridelení môžu viesť k rôznym útokom.
- Povolenia (permissions) sú špecifikované v AndroidManifest.xml.

Android permission model 2

- Normal.
- Dangerous.
- Signature.
- Signature-or-system.
- Time-of-use.
- Install-time.



Vývoj permission modelu

- Upravuje sa pri vývoji nových verzií OS.
- Reprezentované tzv. API levels.
- Prvý API level (3) - 103, v súčasnosti (18) vyše 160.
- Väčšinou sa pridávali kvôli novým HW možnostiam zariadení.
- Chýba im však väčšia granularita, napr. CAMERA.
- Pre bežného používateľa sú príliš komplikované na porozumenie.

Plán útoku - Čo sa stane ak povolenie neexistuje?

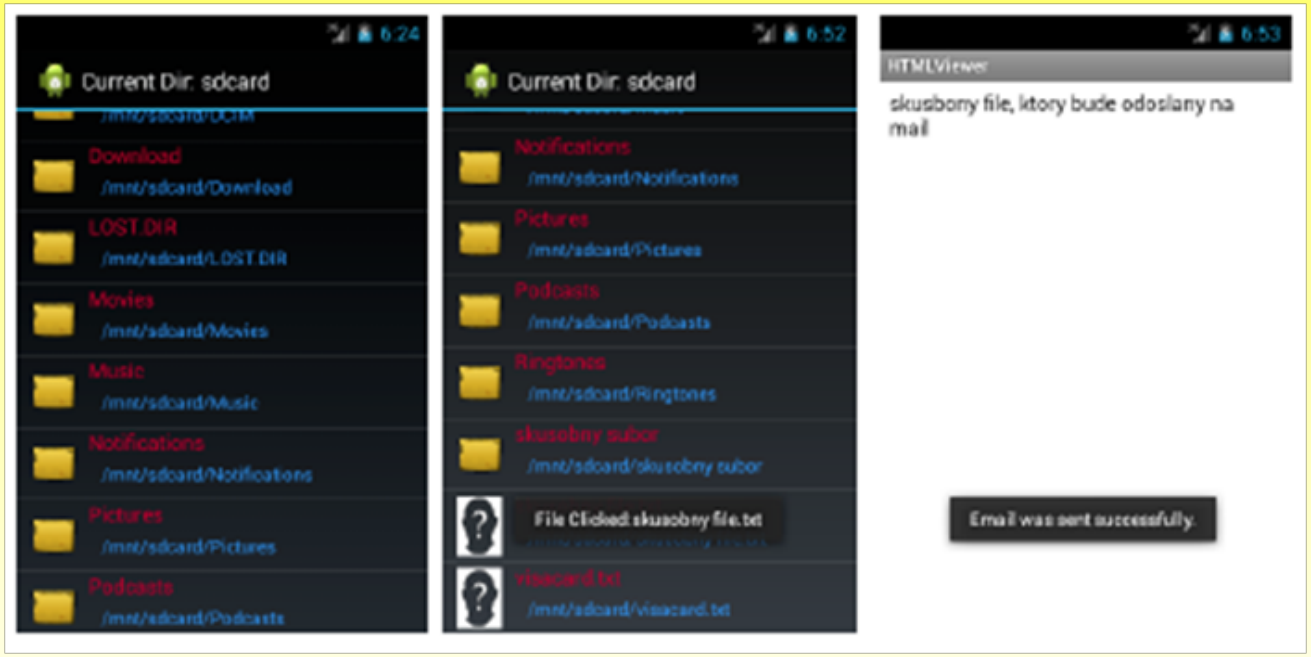
- Majme jednoduchú appku s databázou - napr. messenger.
- Malá - uložená v internej pamäti - nedostupná.
- Väčšia - uložená na pamäťovej karte - dostupná.
- Na prístup k súborom na pamäťovej karte netreba žiadne povolenie!!!
- Jasne v rozpore s politikou aplikačnej separácie. . .
- Appky demonštrujúce túto zraniteľnosť.

Customizovaný e-mailový klient

- Najjednoduchší spôsob prenosu ukradnutých dát.
- Java Mail Library.
- Plne manažovateľný.
- Pripojí sa na ľubovoľný SMTP server.
- Obmedzený len veľkosťou prílohy.

File manager

- Poskytuje legitímnu funkcionalitu.
- Po kliknutí na súbor ho na pozadí odošle.
- Vyžaduje INTERNET povolenie.
- Môže byť vyžadované na update reklamných bannerov.

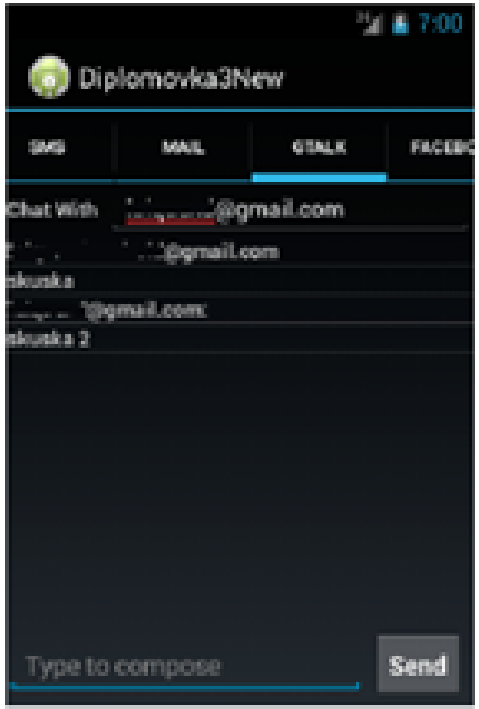


Komunikátor

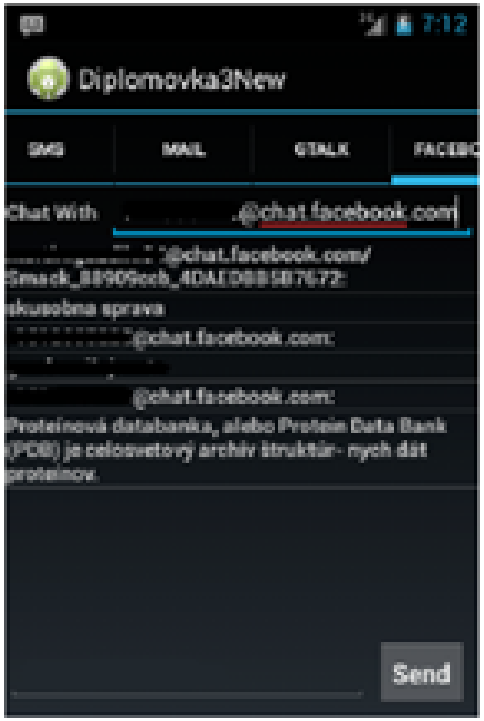
- Poskytuje legitímnu funkcionalitu.
- E-mail, SMS, G-Talk, FaceBook, Jabber.
- Vyžaduje povolenia na prístup k Internetu, manipuláciu s SMS správami čítanie zoznamu kontaktov.
- Správy sa ukladajú do databázy.
- Po dosiahnutí limitu na správy -> súbory sú odoslané útočníkovi.

Komunikátor 2

(a) SMS



(b) G-Talk



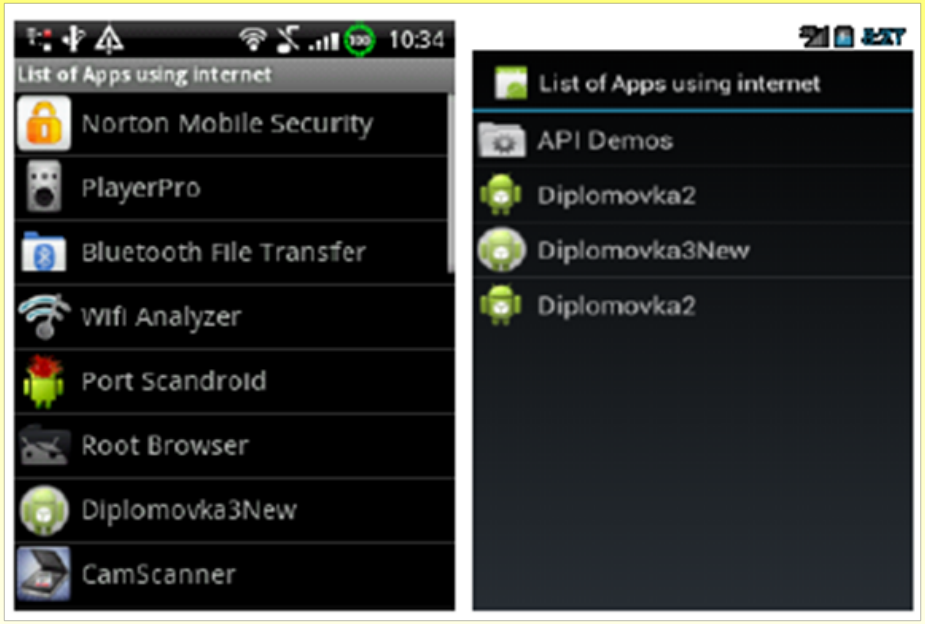
(c) FaceBook

Testy a výsledky

- Testované 7 free antivírovými appkami.
- Eset, AVG, avast!, McAfee, TrendMicro, Norton, Lookout.
- Nainštalované na zariadenie, nechané chvíľu v kľude, vykonávanie záškodníckej činnosti.
- Quick scan a deep scan - CyanogenMod.
- Ani jedna z našich appiek nebola zachytená.

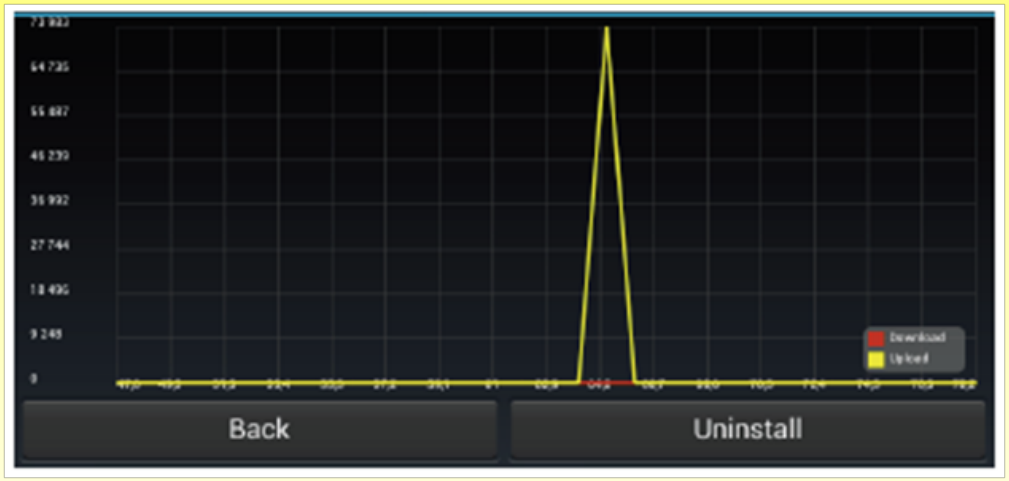
Protiopatrenia

- Ďalšia appka, bez potreby povolení.
- Skenuje aplikácie vyžadujúce INTERNET povolenie.
- Monitoruje dátový tok vybraných appiek.
- Upozorní používateľa, že niečo nekalé sa deje.
- Nechá používateľa rozhodnúť.



Protiopatrenia 2

- Veľmi jednoduchá metóda detekcie.
- Niektoré aplikácie by nemali vôbec uploadovať dáta.
- Napr. file manager - treba rýchlo odinštalovať.
- Iné zasa na správne fungovanie uploadovať dáta musia.
- Napr. komunikátor - je to na používateľovi.



Záver & Plány do budúcnosti

- Chýbajúce povolenie by malo byť pridané v novej verzii OS. . .
- Chýbajúce povolenie môže kompromitovať používateľské dáta.
- Veľmi jednoduchý útok, ale môže spôsobiť veľa škody.
- Veľmi jednoduchá, a miestami aj veľmi účinná metóda detekcie.
- Plná automatizácia - učiaci proces.
- Nechávať rozhodnúť používateľa nie je vždy dobrý nápad :-)
- Môže byť zahrnutá do aktuálnych antivírových appiek.

Ďakujem za pozornosť!