Androidov sigurnosni model

Attack of the POSIX mutants

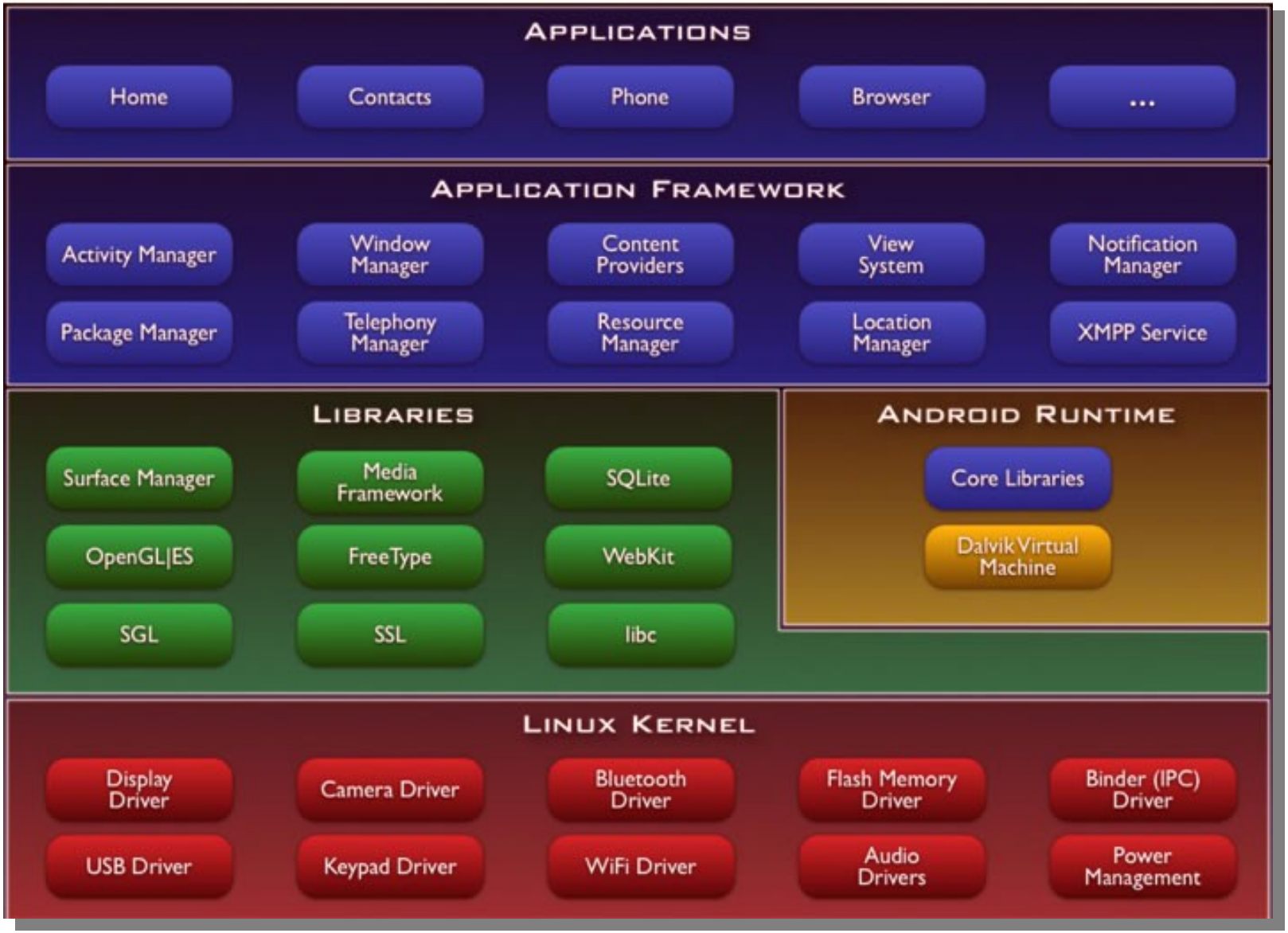
Radoslav Dejanović

CuC sys.trek 2014.

Androidov sigurnosni model

Naša sigurnost događa se ovdje... →

... i ovdje →



Androidov sigurnosni model

- POSIX-ish
    - oslanjanje na tradicionalne Unix mehanizme kao temelj sigurnosti
- virtualizacija
- sandboxing
- "moderni" mehanizmi zaštite naslonjeni na tradicionalne

Androidov sigurnosni model

Različitosti u odnosu na druge Unixoide:

- UID je ID i korisnika i aplikacije (AID – Android UID)

- svaka aplikacija ima svoj AID, svoj sandbox i svoje dozvole

- iznimke? shared UID! (jer sandbox sandboxu ne vjeruje)

- veća količina AID-a (100000 naspram "tradicionalnih" 65536 UID-a)

- izolirani AID (99000-99999) za procese koji trebaju najmanja prava

- init/Zygote kombinacija

- prvi korisnik je poseban, ali nema prave root privilegije

- korisnički UID se "lijepi" na AID aplikacije (nn+mmmmmmm)

- "patch disconnect" kad proizvođač uređaja "štopa" sigurnosne zakrpe

Androidov sigurnosni model

Različitosti u odnosu na druge Unixoide:

- GID je doživio tek manje izmjene, transformiran u "Android Permissions": /etc/permissions/platform.xml

- AndroidManifest.xml (obavezan uz svaku aplikaciju):
    - naziv aplikacije
    - opis komponenti
    - dozvole potrebne za rad
    - dozvole potrebne za komunikaciju sa drugim procesima
    - minimalni API
    - potrebne biblioteke
    - sigurnosne postavke na nivou aplikacije

- Aplikacije mogu zahtjevati vlastite dozvole – GID doesn't apply

- sandboxing je neizostavan

- sistemske aplikacije idu u /system/app, a korisničke u /data/app direktorij

- platform key za sistemske aplikacije (developer key za ostale)

Androidov sigurnosni model

Neugodne činjenice:

- multiuser okruženje (zasad) ovisi o xml datoteci koja "sakrije" aplikaciju od korisnika

- neke stvari nije moguće sakriti od korisnika (WiFi, primjerice)

- zle aplikacije u pozadini mogu pratiti aktivnost korisnika i nije ih moguće zaustaviti ako ih je pokrenuo drugi korisniki

- "podkorisnici" (ID >=10) mogu bez znanja vlasnika (ID = 00) instalirati update postojećih aplikacija (rogue market), koristiti NFC, Bluetooth...

- moguće je zaboraviti postaviti platform key prilikom razvoja ROM-a

- native code ranjivosti (overflow, corruption, escalation...)

- različiti uređaji imaju različite verzije OS-a, sa različitim sigurnosnim problemima

- development: moving target

Androidov sigurnosni model

Zaključak

- kreativno korištenje UID/GID funkcionalnosti

- niži nivo sigurnosti koristi iskušane Unix metode

- viši nivo sigurnosti omogućuje finu granulaciju dozvola

- sam OS i biblioteke osjetljivi su na klasične sigurnosne probleme

- multiuser model je vrlo primitivan i nedostatan za poslovna okruženja

- iznimno je važno eliminirati "patch disconnect"

Androidov sigurnosni model

Malo opširnije...

http://sistemac.carnet.hr/node/1450