Vargar og vélmenni

Öryggi og Android snjallsímar

Kjartan T. Hjörvar – CERT-ÍS

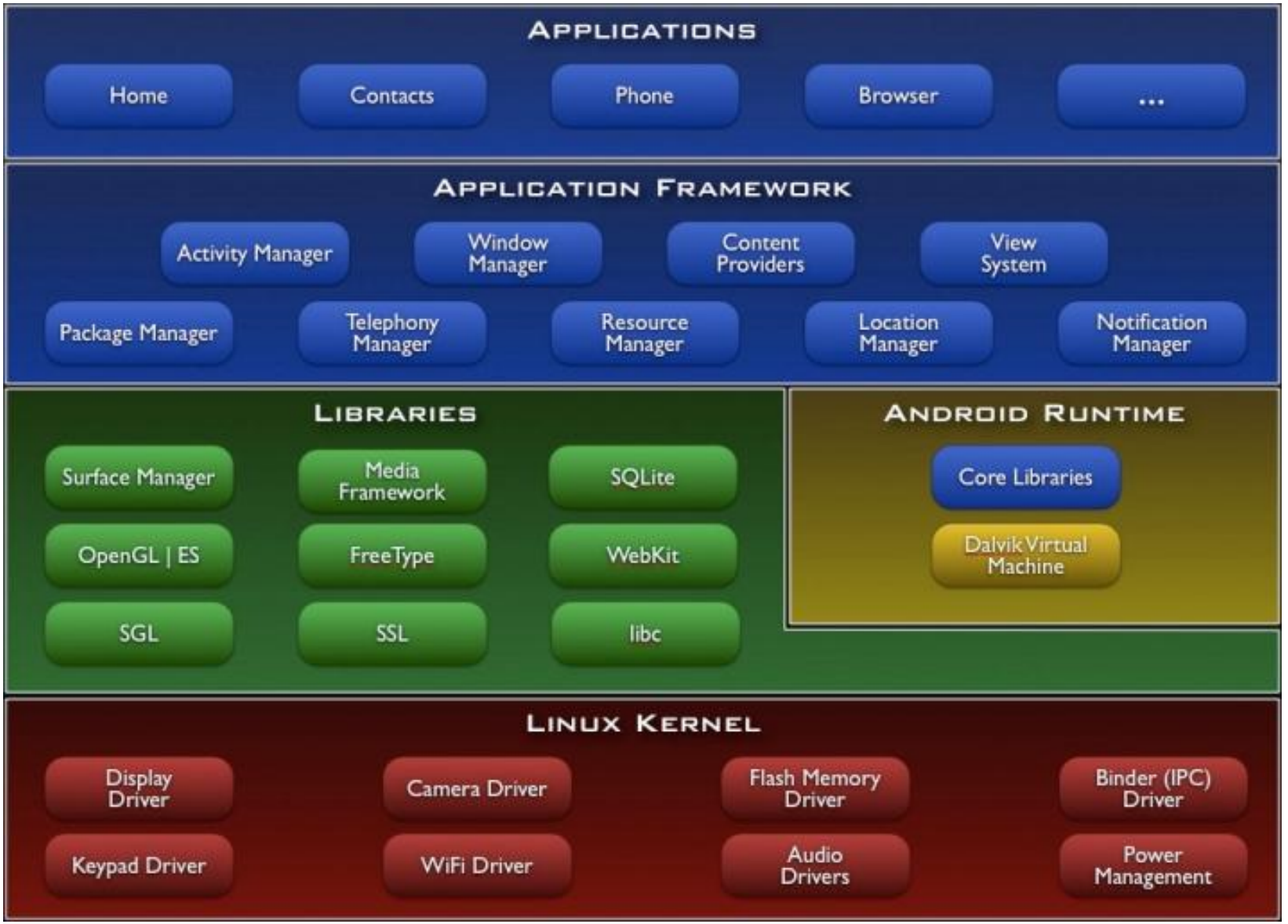
Yfirlit

- Android grunnkerfið
- Forrit á Android
- Veikleikar
- Aðrir árásarfletir
- Úrræði fyrir kerfisstjóra

Dæmigert Android tæki

- 1,5 GHz tvíkjarna örgjörvi, 1GB innra minni, 10-50+ Mb/s nettenging
- IP tengingar gegnum farsímanet og WiFi
  - Lítur út gagnvart neti eins og borðvél eða netþjónn
- Bluetooth, USB, minniskort, myndavél!
- Keyrir Android stýrikerfið...

Uppbygging Android



Heimild: Google

Lífsferli Android

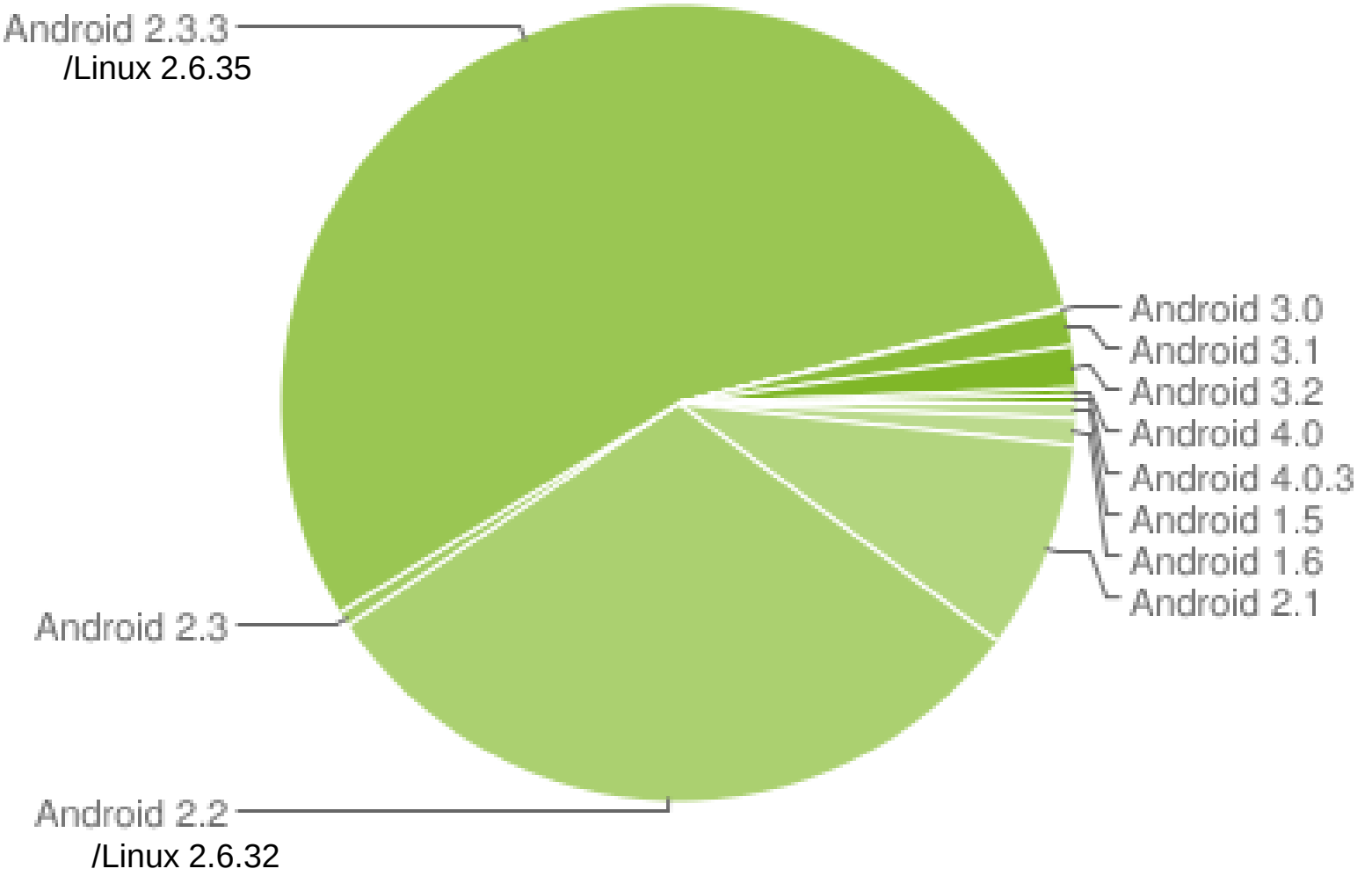
- Google
  - Býr til grunnkerfið
  - Útbýr lagfæringar
- Framleiðendur síma
  - Aðlaga Android að sínum tækjum
  - Undir eftirliti frá Google til að bera Android merkið
  - Geta sett inn forrit sem ekki er hægt að fjarlægja
  - Aðlaga lagfæringar, prófa og senda út

Ábyrgð á Android frh.

- Fjarskiptafyrirtæki
  - Geta fengið sérútgáfur af símum frá framleiðendum
  - Sér forrit, umhverfi, markaðir
  - Þurfa einnig að aðlaga, prófa og senda út lagfæringar
- Hugbúnaðarfyrirtæki
  - Skrifa forrit og dreifa m.a. gegnum markaði
  - Uppfærslur í gegnum markaði

Útgáfur í notkun

Android Market: 20.12.2011 - 3.1.2012



Heimild: Google

Uppsetning forrita

- Markaðir – t.d. Android Market frá Google
- Réttindi birt og staðfesting fengin
- Bein uppsetning forrits
  - Ekki sjálfgefið að það sé leyft
  - Sótt t.d. af vefsíðu
  - Vefslóðin getur komið með QR kóða

Google.com

Umhverfi forrita

- Keyra í sandkassa
  - Aðgreining frá öðrum forritum
  - Aðgangur að eigin geymslusvæði
  - Aðgangur að minniskorti, sameiginlegt milli forrita
- Hafa ákveðin réttindi
  - Discretionary Access Control
  - Lýsa yfir hvað þau vilja gera, notandi samþykkir
  - Geta nýtt virkni annarra forrita og þannig réttindi þeirra

Árásarfletir Trójuhesta

- Forrit sem gera meira en þau segja

- Geta nýtt réttindi annarra forrita
  - Gætu notað vafra til að hafa samband yfir netið
- Geta lesið gögn af minniskorti
- Mögulegt að brjótast út úr sandkassanum
  - Gagnastuldur
  - Fullur aðgangur

Veikleikar

Auðkenni	Tegund	Hvað	Alvarleiki
CVE-2008-7298	Upplýsingabreytingar, truflun á þjónustu	Android browser	5,8
CVE-2010-4804	Upplýsingaleki	Android browser	4,3
CVE-2010-1807	Upplýsingaleki, breytingar, truflun á þjónustu	WebKit	9,3
CVE-2011-0419	Truflun á þjónustu	Android	4,3
CVE-2011-0680	Upplýsingaleki	Android - mms	5
CVE-2011-1149	Upplýsingaleki, breytingar, truflun á þjónustu	Android - ashmem	7,2
CVE-2011-1717	Upplýsingaleki	Skype	2,1
CVE-2011-1823	Fullur aðgangur	Android - vold	7,2

Sterkari varnir - SEAndroid

- Kemur frá Þjóðaröryggisstofnun Bandaríkjanna (NSA)
- Byggir á SELinux, önnur nálgun á öryggi
  - Miðlæg stýring í stað dreifðrar (MAC vs. DAC)
  - Bætir aðgangsstýringar að gögnum
  - Setur réttindi á allt, líka socket
  - Getur líka stýrt réttindum UID=0
- Hefði takmarkað tjón af völdum flestra veikleika sem upp hafa komið

Aðrir árásarfletir

- Phishing – svikamyllur
  - Reyna að komast yfir lykilorð og auðkenni
- Beinar netárásir
- “Maður í miðjunni” árásir
  - Hlerun samskipta
  - Raunhæfast yfir WiFi
  - Notandi getur ekki fjarlægt rótarskilríki
- SMS óværur

Tæki tapast eða er stolið

- Er til afrit af gögnum?
- Er staðsetningarforrit virkt?
- Er tækið læst?
- Gögn dulkóðuð?
- Hvað er hægt að lesa af símanum?
  - Skjöl
  - Tölvupóstar
  - Myndir
  - Lykilorð
  - Dulkóðunarlyklar
  - Símtalaskrá
  - SMS
  - Staðsetningar

Kerfisreglur

- Device Administration API (2.2)
  - Leyfir ýmsar takmarkanir á lykilorðum, t.d.
    - Lengd
    - Flækjustig (3.0)
    - Endingartíma (3.0)
  - Dulkóðun á gögnum (3.0)
    - Aðeins á geymslusvæði forrits, ekki SD kort
  - Stjórn á myndavél (4.0)
  - Endurstilling tækis í upphafsstillingu
    - Eyðir alla jafna ekki gögnum af SD korti

Tvískipting tækja

- Skipting tækja í tvö aðskilin svæði
  - Fyrirtækjasvæði, læst, dulkóðað og stjórnað af kerfisstjóra
  - Persónulegt svæði undir stjórn notanda

- “Split personality”, “dual personality”, “virtualization”
  - Nú þegar til slík forrit
  - VMware vinnur að því að koma *Horizon Mobile* inn í Android kjarnann

Yfirlit

- Android grunnkerfið
- Forrit á Android
- Veikleikar
- Aðrir árásarfletir
- Úrræði fyrir kerfisstjóra

Hafið í huga

- Að viðskipti yfir netið séu með öruggum hætti
- Lán á símtæki getur haft afleiðingar í för með sér
- Auðvelt er að hlera almenn þráðlaus staðarnet
- Vafra skynsamlega
- Ekki geyma viðkvæmar upplýsingar á aukaminniskorti
- Nota örugg samskipti eins og hægt er
- Mikilvægast: Læsa símanum með lykilorði

Takk fyrir