WiFi drošība un Lielo datu analītika – Ieguvumi un ietekme uz privātumu un drošību.

Brīvība pret Drošību

Mums patīk mobilitāte un brīvība

- Modernās tehnoloģijas – mobilās ierīces, 3G/4G/LTE un Wi-Fi, virtualizācija un mākoņpakalpojumi ir uz visiem laikiem izmainījuši mūsu ikdienu un darba rutīnu.
- Mūsdienās visi izmanto mobilās iekārtas un kādu no daudzajiem mākoņpakalpojumiem vai servisiem:

WiFi ir kļuvis par universālu datu nesēju

e-Lasītāji

Viedtelefoni

Tabletes

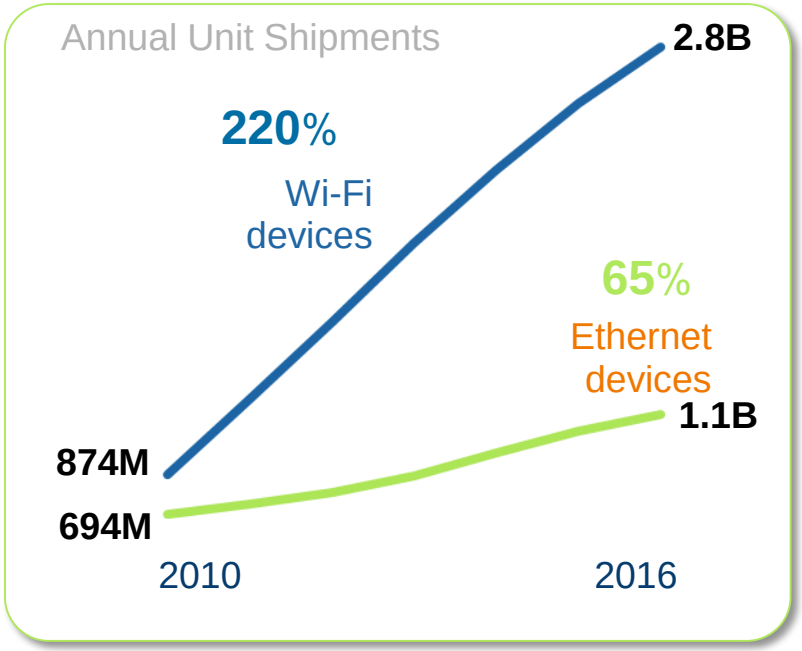
Medicīnas aprīkojums

Portatīvie datori

PoS termināli

Vides pārvaldības risinājumi

Projektori



Source: iSuppli 2012

Izplatītākie mīti par WiFi

- Wi-Fi tīkli ir nedroši
- Wi-Fi tīkli ir primārie hakeru uzbrukumu mērķi
- Slēpiet un sargājiet savus SSID!
- Wi-Fi nedrīkst būt piekļuve korparatīvajiem datiem

1. apgalvojums:
WiFi tīkli ir nedroši

- Šis apgalvojums ir cēlies no WiFi tehnoloģijas pirmsākumiem un pateicoties 2 ļoti izplatītiem cēloņiem:
- Atšķirībā no LAN tīkla, Wi-Fi nevar tikt ierobežots konkrētā teritorijā un tādējādi rodas lielāks pārklājums nekā nepieciešams.

Patiesībā, modernie Wi-Fi tīkli izmanto stipro AES kriptēšanu un dati (pat tie, kuri ir fiziski pieejami saņemšanai) ir kriptēti, kas patiesībā Wi-Fi padara drošāku pat par LAN.

- Wi-Fi tehnoloģijas iesākumā izmantoja WEP kriptēšanu, kas bija ar kļūdām un tas tik tiešām apdraudēja datu drošību. 2004. gadā WEP standartu aizstāja ar WPA un WPA2 (stabils drošības standarts) ar AES kriptēšanu.

Diemžēl, pateicoties, WEP standarta nedrošībai, WiFi tehnoloģiju sāka uzskatīt par ievainojamu un nedrošu.

2. apgalvojums:
WiFi konfigurācijas riski

- Vēl joprojām, liels vairums IT auditoru savos dokumentos iekļauj punktus par WiFI, kas atbilst 2000. gada tehnoloģijas līmenim:

Default Password - change the default administrator password. Use your browser to access the address provided in the manual. Use the control panel to make the change.
Password Strength - create a long and strong password using a combination of upper and lower case characters, numbers, and symbols.
Service Set Identifier (SSID) - change the SSID name to something unique. Disable broadcasting of the SSID.
Universal Plug and Play (UPnP) - UPnP provides automatic discovery of other Plug n Play devices on the network. Where possible, disable Wide Area Network (WAN) management and UPnP connectivity.
Encryption - Create a strong encryption key using WPA2 AES. Create a long and strong Pre-Shared Key (PSK) that has at least 40 random characters, numbers, and symbols.
Firewall - enable the Stateful Packet Inspection (SPI) firewall on the device.

Avots: *http://www.altiusit.com/files/blog/Top10WirelessNetworkRisks.htm*

Šāda veida apgalvojumi faktiski ignorē mūsdienu WiFi tehnoloģiju un tos varētu attiecināt vairumā tikai uz SOHO (small office / home office) tehnoloģiju, kura arī vairs neeksistē.

3. viedoklis:
WiFi tīkli ir hakeru primārais uzbrukumu mērķis

- Patiesībā fakti liecina par pretējo: neviens no lielākajiem kiberuzbrukumiem pēdējos gados nav bijis saistīts ar WiFi izmantošanu.
- Tas, protams, nenozīmē, ka bezvadu tīkli ir neinteresanti priekš hakeriem – ir iespējams to izmantot kā līdzekli, lai pasargātu hakeru identitāti un saņemt anonīmu piekļuvi, lai īstenotu kādu uzbrukumu.
- WiFi tīklā var ielauzties (parasti kombinācijā ar kļūmēm programmatūrā un IT administratoru uzstādījumos), taču ieguvumi ir krietni mazvērtīgāki, jo vērtīgā informācija parasti tiek glabāta ļoti aizsargātā korporatīvajā serverī, nevis uz lietotāja datora.
- Joprojājām nav zināms neviens zināms paņēmiens kā uzlauzt pareizi nokonfigurētu WPA2 WiFi tīklu.

P.S. Neviens nav pasārgāts, ja lietotāju login dati (lietotājvārds, uzvārds) tiek kompromatizēti.

4. viedoklis:
WiFi nedrīkst būt piekļuve korporatīvajiem datiem

- Patiesībā tas mūsdienas nemaz nav vairāk iespējams, jo lielākā daļa no biznesā lietotājām iekārtam ir ar WiFi savienojumu
- Tas nenozīmē, ka nevajag rūpēties par datu aizsardzību – taču datu aizsardzība ir kļuvusi krietni sarežģītāka.
- Lai vai kā, visi lielākie kiberuzbrukumi tika izdarīti caur vadu tīklu un vairākos no gadījumiem palīdzēja kāds no iekšienes (ļaunprogrammatūra uz datora, kurš pieslēdzās lokālajam tīklam vai fiziska persona, kura asistēja no iekšienes). Tieši tāpēc WiFi ir jābūt aizsargātam tāpat kā citām tīkla sastāvdaļām.
- Vecā tipa pakešu filtrēšanas ugunsmūri vairs nespēj aizsargāt jūsu datortīklu, līdzīgi kā policija vairs nestrādā ar metodēm, kas bija efektīgas pirms 10 gadiem…

Kopš 2000. gada WiFi ir radikāli mainījies!

Mobilās ierīces ir kļuvušas par ļaundaru galveno prioritāti, jo tās ļoti biezi nav pietiekami labi aizsargātas un satur ļoti daudz sensitīvas informācijas, kura var dot piekļuvi citām sistēmām – korporatīvajam tīklam, finanšu sistēmām, banku kontiem un citām.

Cilvēki ļoti bieži izmanto vienu un to pašu paroli, līdz ar to ir ļoti vienkārši uzlauzt dažādas lietotnes un sistēmas

Lietotāju ievaddati tiek saglabāti dažādās vietās. Lielākā daļa no mobilajām aplikācijām iegūtos datus saglabā dažādos «mākoņos». Tādējādi hakeriem šie «mākoņi» ar lielu datu masu ir ļoti pievilcīgi. (Viens no lielākajiem uzbrukumiem: eBay uzlaušana – 140 000 000 lietotāju konti tika uzlauzti).

Daži no lielākajiem kiberuzbrukumiem

Kā jau iepriekš paskatījām, tad lielākie uzbrukumi nav saistīti ar WiFi un tā izmantošanu, lai uzlauztu tīklu. Tā vietā uzbrukumi bija mērķēti uz lielo kompāniju datu noliktavām.

- eBay hack, 2014. gads: 140 000 000 konti
- Heartland Payment Systems, 2008-2009: 130 miljoni ierakstu
- Target Stores, 2013. gads: 110 miljoni ierakstu
- Sony online entertainment services, 2011. gads: 102 miljoni ierakstu
- National Archive Administration, 2008. gads: 76 miljoni ierakstu
- Anthem, 2015. gads: 80 miljoni ierakstu
- Epsilon, 2011. gads: 60 million to 250 miljoni ierakstu
- Home Depot, 2014. gads: 56 miljoni maksājumu karšu
- Evernote, 2013. gads: More than 50 miljoni ierakstu
- Living Social, 2013. gads: Vairāk nekā 50 miljoni ierakstu
- TJX Companies Inc., 2006-2007: Vismaz 46 miljoni ierakstu
- Sony Pictures Entertainment, 2014. gads: Visa kompānijas informācija

Mākoņpakalpojumi un WiFi

Pastāv vairāki ieguvumi, ko sniedz WiFi integrācija ar «mākoņiem»:

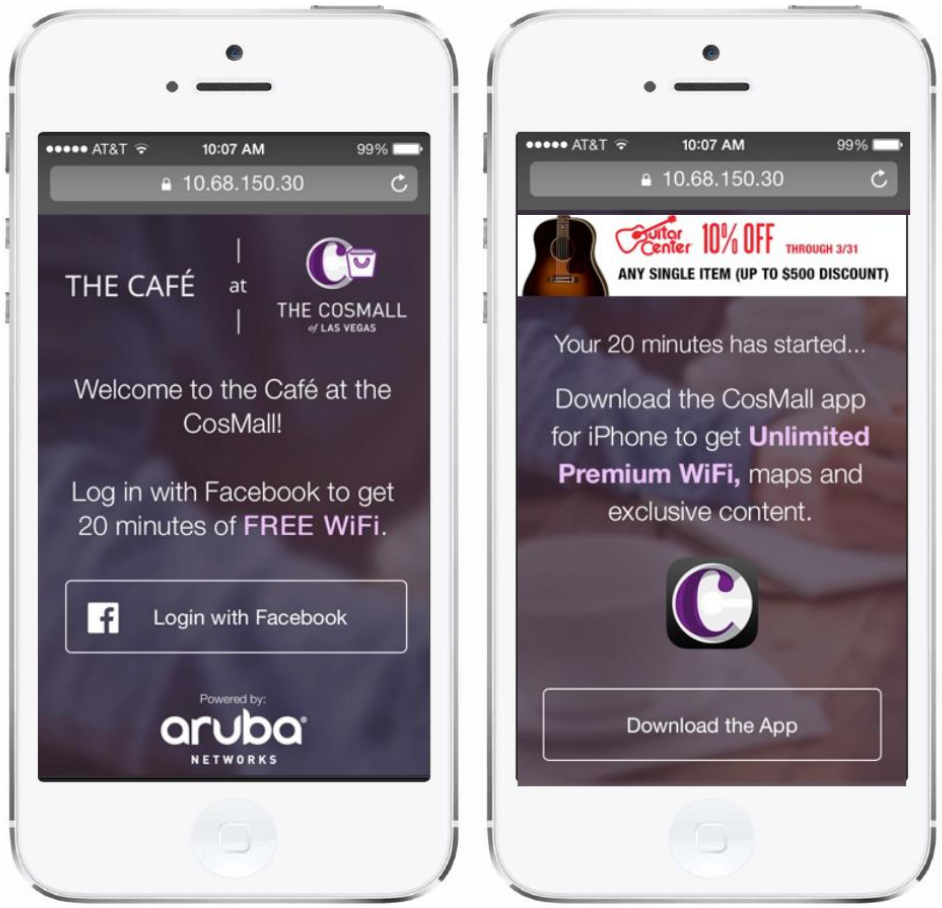
- Mākoņpakalpojumu pieejamība izmantojot WiFi
- Mobilo iekārtu servisi, kuri asistē, izmantojot Wi-Fi
- Risinājumi, kuri balstīti uz atrašanās vietas un klātbūtnes noteikšanu ar WiFi palīdzību
- Risinājumi, kuri balstās uz WiFi piekļuvi un datiem par tā izmantošanu
- WiFi risinājumi, kuri tiek pārvaldīti izmantojot WiFi

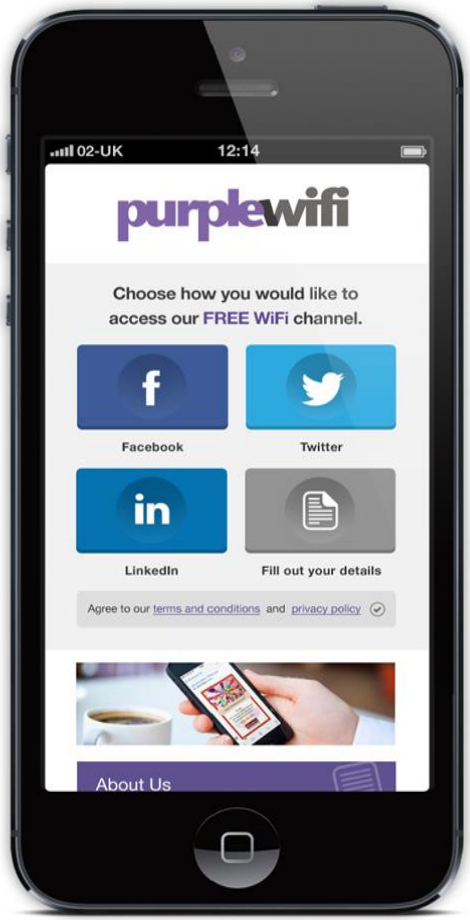
Visos augstākminētajos gadījumos un kombinācijās, apvienojot mākoņpakalpojumus ar WiFi tehnoloģiju, mēs iegūstam jaunas un satriecošas iespējas un funkcijas.

Interaktīvie asistenti

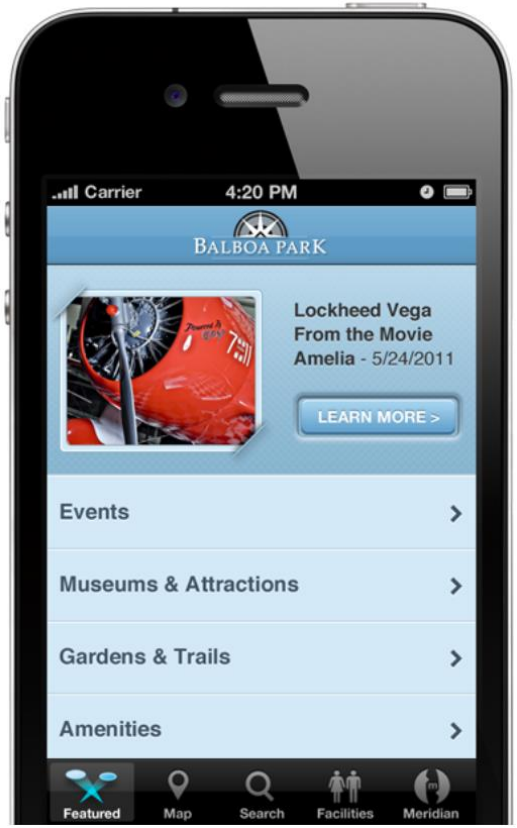
Šīs aplikācijas iegūst dažādus personīgos datus un mūsu ievadīto un meklēto informāciju un sniedz bagātīgas atbildes un prognozes par meklēto. Tās varbūt nav tieši saistītas ar WiFi, taču ļoti daudz izmanto Interneta piekļuvi un ar to saistīto informāciju.

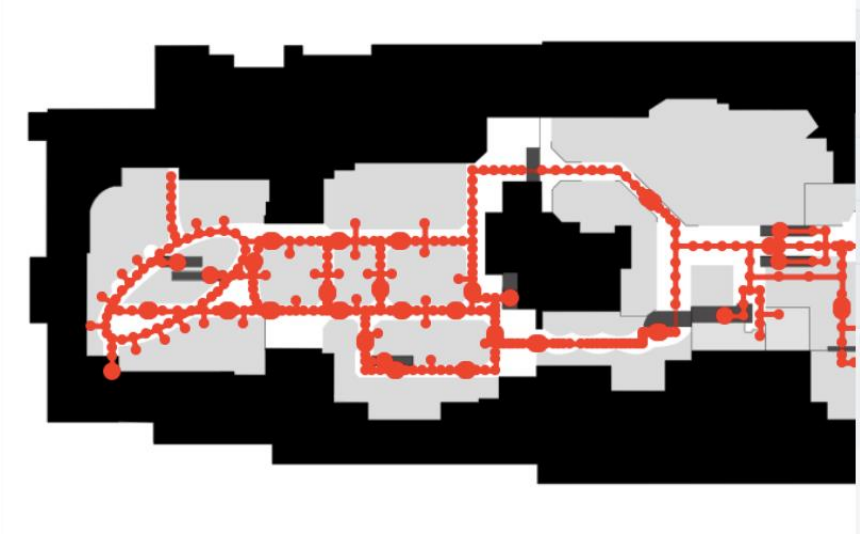
WiFi integrācija
Piekļuve ar mārketinga rīkiem





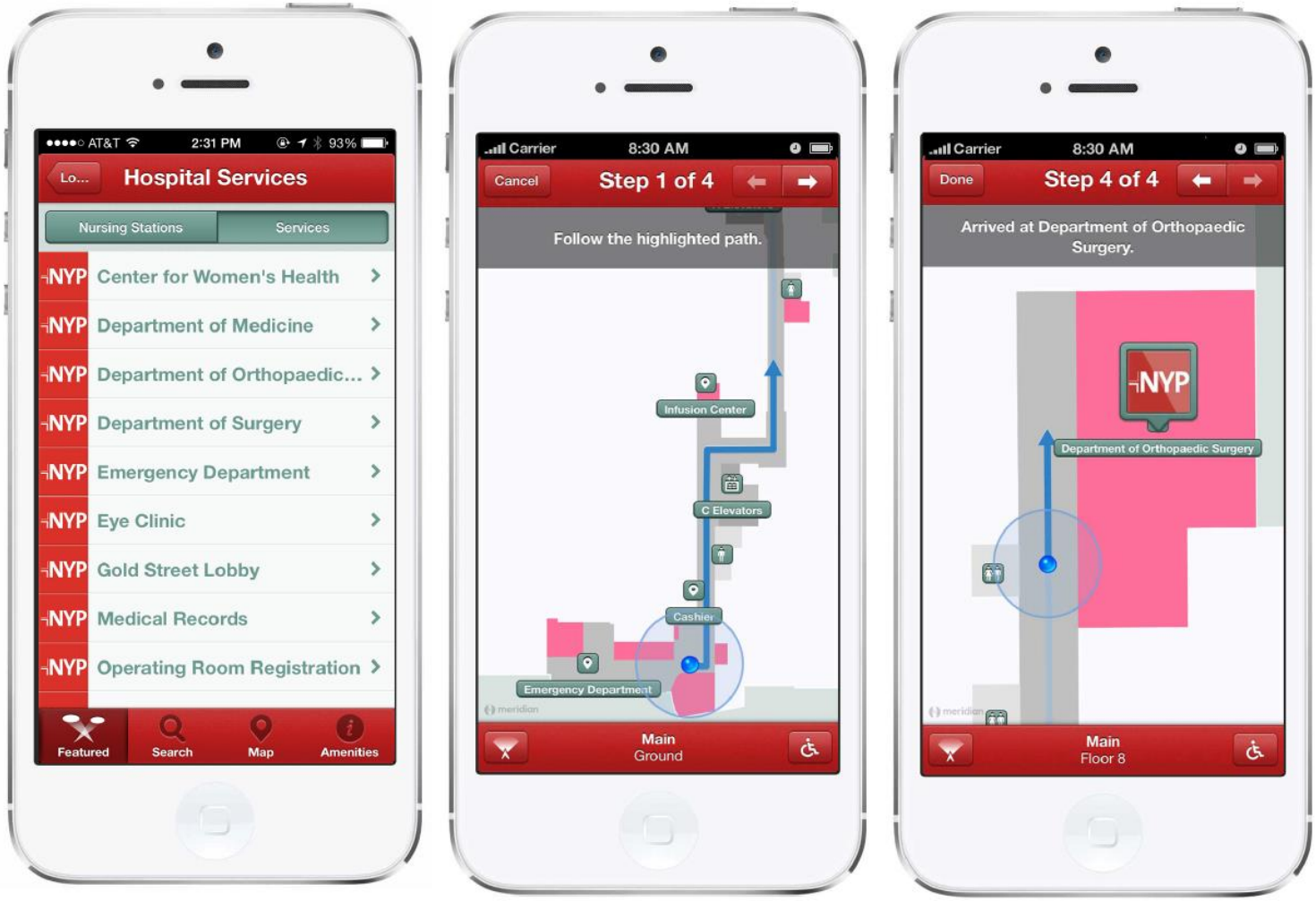
Aplikācijas ar WiFi lokācijas servisu atblastu



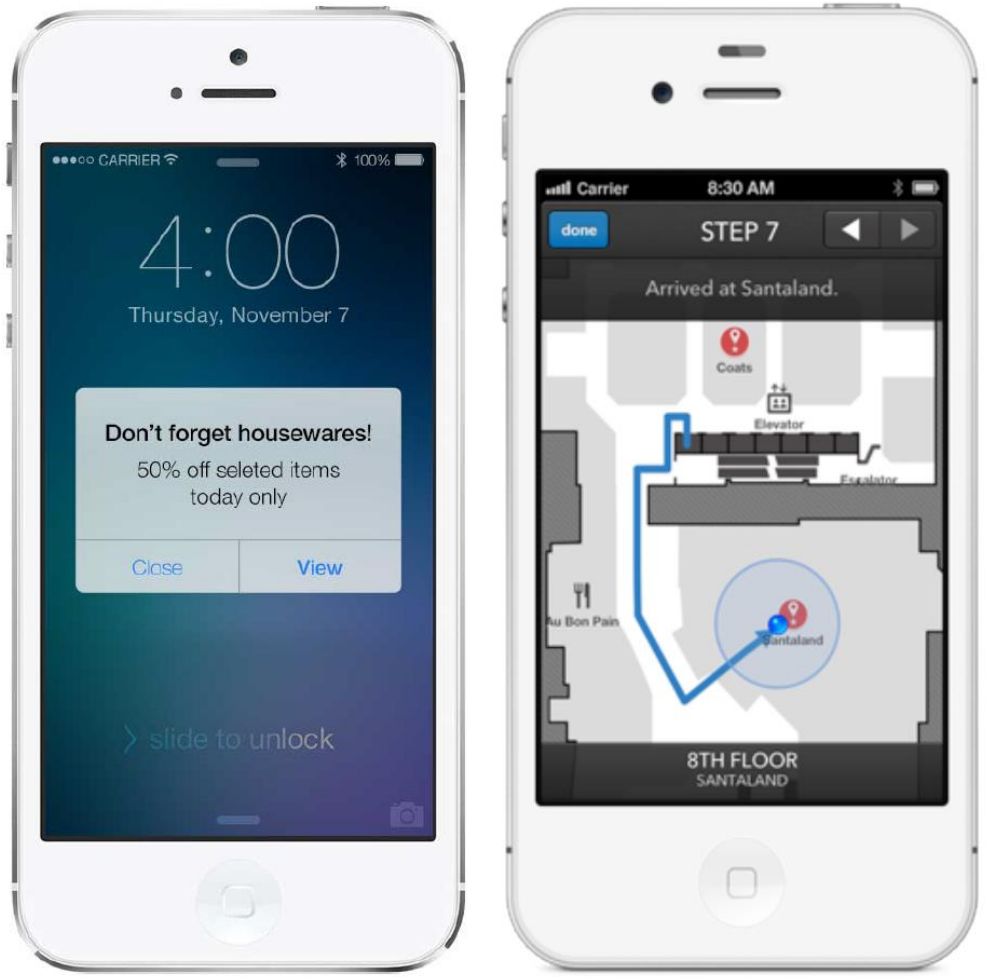


Viedtelefonu aplikācijas izmanto WiFi, lai noteiktu atrašanās vietu un sniegtu atbilstošo informāciju.

WiFi kā iekštelpu navigācija



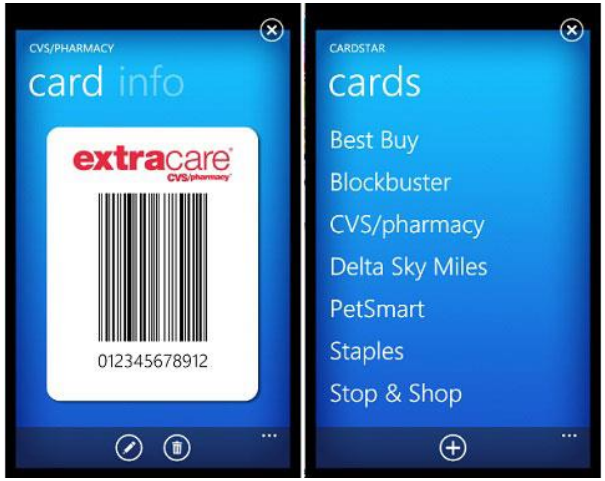
Aplikācijas, kuras nosaka lokāciju izmantojot Beacon tehnoloģiju



Lojalitātes programmas, kuponi un mārketings

Maksājumu aplikācijas un mobilie maki

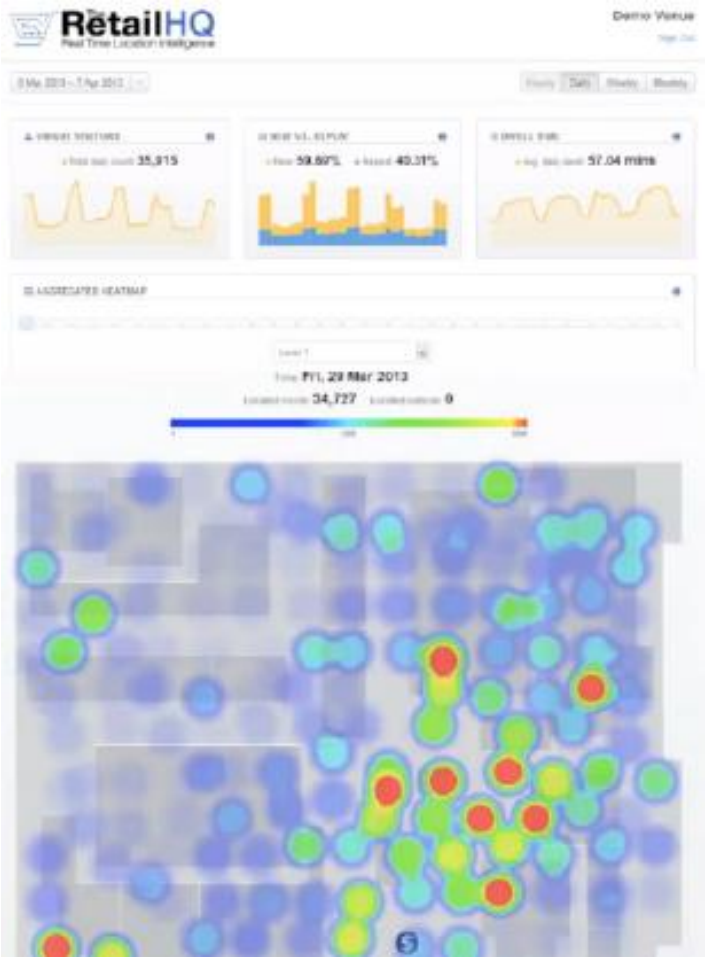
Tā ir dzīva nauda!



Banku aplikācijas, drošas piekļuves - (kalkulatoru) aplikācijas

Aplikācijas satur ļoti vērtīgu informāciju un datus, kā arī piekļuves kodus!

WiFi atrašanās vietu pakalpojumi un analītika

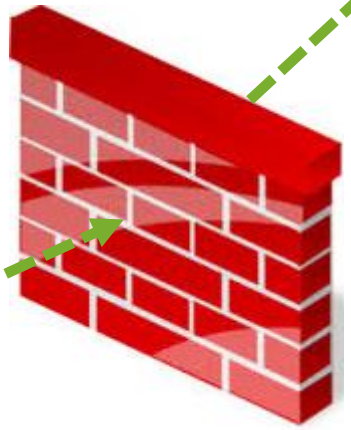


Vēsturiskā uzņemuma tīkla struktūra

2 veidu iekārtas, visi dati - lokāli

Uzņēmuma LAN (visi dati datucentrā vai uz PC)

Dati



Internet

Mobils lietotājs (visi dati datucentrā un vai uz laptopa)

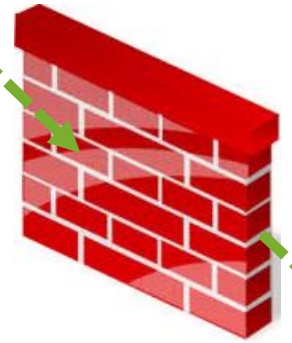
Musdienīgs uzņēmuma tīkls

4 iekārtu veidi, dati – virtualizēti, un veidojās BIG Data

Dati: daudzos mākoņos + savāktie dati

Enterprise LAN (dati virtualizēti)

Pakalpojumu savāktie dati



OS un APP savālktie dati

Internets

3G/4G/Wi-Fi SP

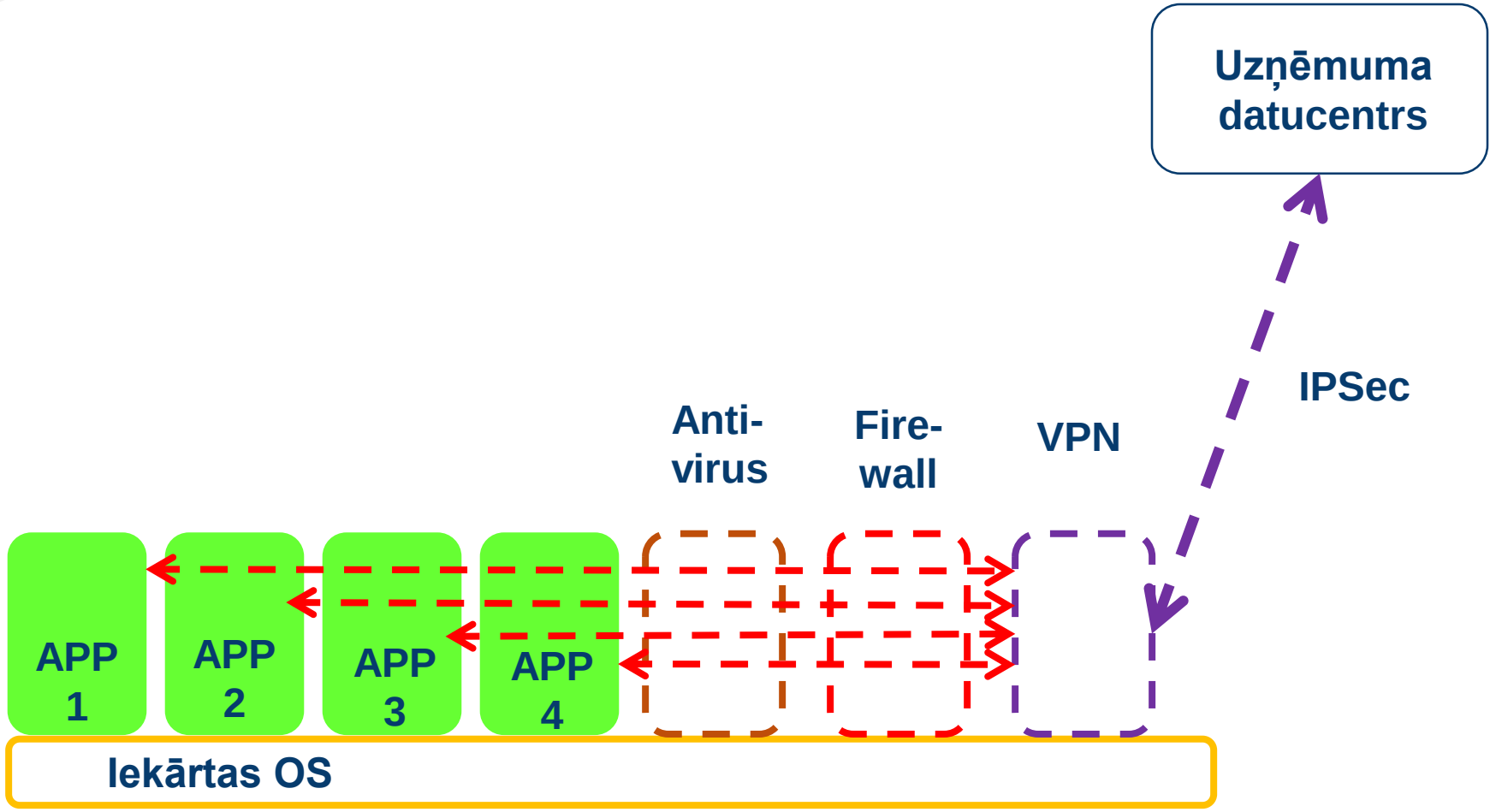
Operatoru savāktie dati

Search, WWW, E-shops, Mail, Social networks

Pakalpojumu savāktie dati

Mobilais lietotājs (dati datucentrā, mākoņos un uz laptopa)

DATU DROŠĪBA UZ IĒKĀRTAM AGRĀK



DATI. KĀDI?

Mobilās iekārtas bieži satur:

- Piekļuves datus IT systēmām
- Kontaktus, e-pastus, SMS, zvanu sarakstus
- Kreditkaršu datus / banku piekļuves kodus
- Prīvātos video / audio failus un dokumentus

Pakalpojumu sniedzēji un mākoņu operatori vāc datus:

- Atrašanās vietas vēsturi
- Web browsinga vēsturi un ieradumus
- Komunikāciju ar citām personām
- Tranzaksijas
- Navigācijas un un auto-vadīšanas vēsturi un ieradumus
- Citi dati pēc viņu izvēles

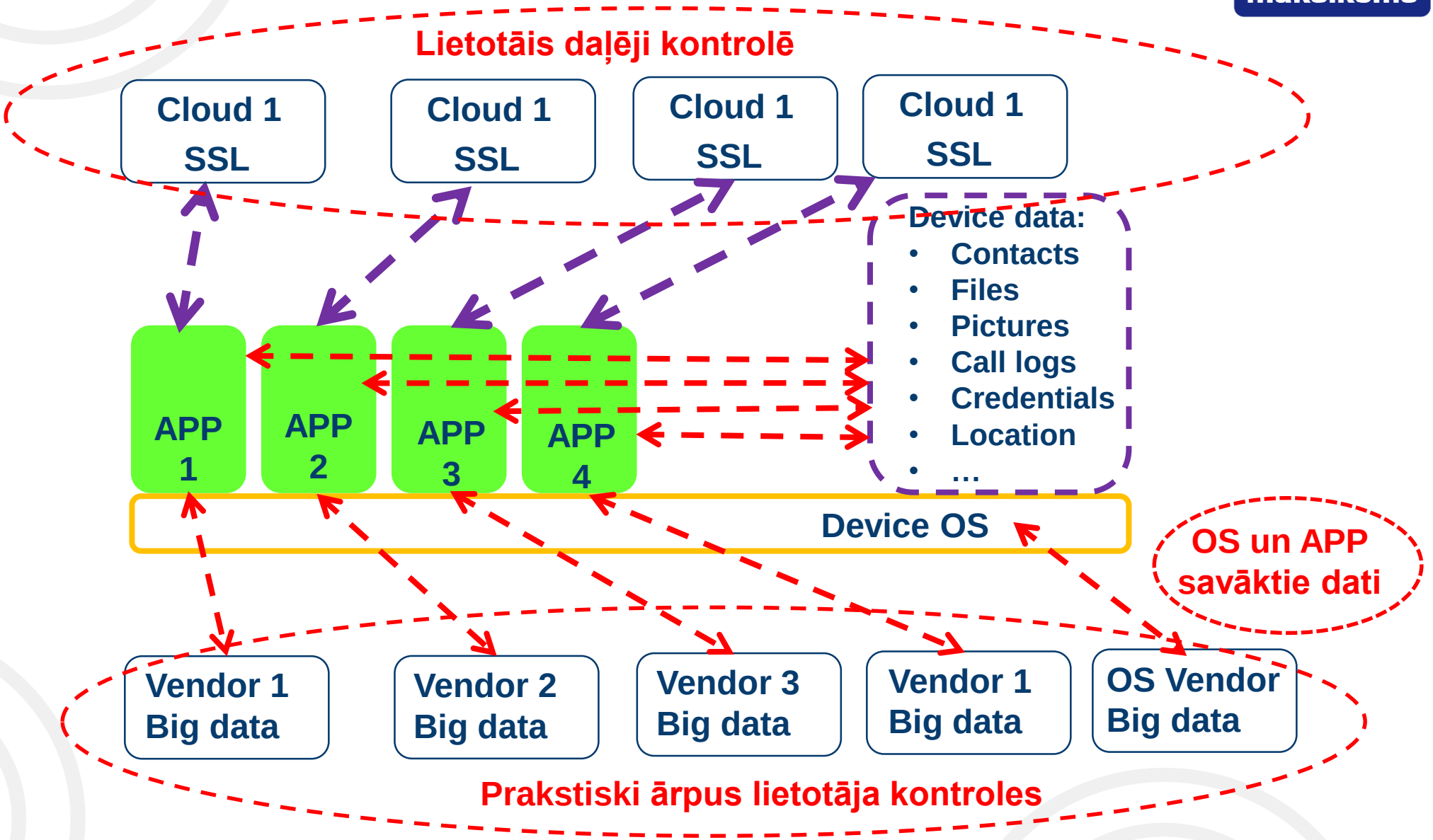
Daudz vairāk ir secināts, kombinējot datus no dažādiem avotiem…

Kur ir mūsu dati?

- Pateicoties sociālajiem tīkliem, mākoņu pakalpojumiem un datu glabāšanai, mūsu dati ir atrodami vairākās vietās;
- Mēs nevaram kontrolēt kādus datus savāc un saglabā pakalpojumu sniedzēji;
- Dati galābājās dažādas datubāzes ar dažādiem īpašniekiem un mērķiem, no kuriem neviens neuztraucas par mūsu privātumu;
- Pateicoties pieaugošajai mobilitātei, nosargāt privātos datus ir kļuvis gandrīz vai neiespējami;

Hakeru uzbrukumi mērķi arī ir mainījušies un tie tagad bieži izvēlas lielus mākoņpakalpojumu sniedzējus ar lielu apjomu privātajiem datiem.

IEKĀRTU DROŠĪBA ŠODIEN



Kurš vēlas Jūsu datus?

Patiesībā - gandrīz vai visi, jo datiem mūsdienās ir liela vērtība:

- Viens no lielākajiem datu vācējiem ir Google, jo tikai pateicoties iegūto datu tidzniecībai, mēs varam par «brīvu» lejupielādāt aplikācijas un lietot pakalpojumus. Šobrīd līdzīgu ceļu iet Microsoft, kuri ar Windows 10 palīdzību iegūs vēl vairāk datus;
- Drošības dienesti nepārtraukti vāc datus par visiem un visur
- Lielāki un mazāki uzņēmumi pērk un izmanto datus mārketingā;
- Dati tiek izmantoti, lai darbinātu servisus (asistentus);
- Dati tiek iegūti, lai uzlabotu servisu kvalitāti (viens no visizplatītākajiem iemesliem, lai pamatot datu vākšanu);
- Kibernoziedznieki mēģina iegūt šos datus pa tiešo vai uzlaužot lielās datu noliktavas.

Jācīnās par brīvību

Pastāv iespējas ierobežot datu iegūšanu, taču **mēs nevaram no tā tik vienkārši izvairīties**.

Visu, ko esam koplietojuši, **mēs nevarēsim tik vienkārši atgriezt un izdzēst.**

Aizliedzot datu savākšanu varētu apstāties servisi, kas balstās uz LIELO DATU ieguvi. Katram pašam ir jāizdara izvēle, ko un kad koplietot (ja tāda iespēja pastāv)!

Kādi jautājumi?

Droši uzdodam:
Eižens Putniņš
SIA MAKSIKOMS CEO
eizens@maxicom.lv
+371 29459183