

Smarttelefonens säkerhet inom operativsystemets mjukvaruuppdateringar

Kandidatavhandling
Ben Eriksson
XX.XX.2021
Åbo Akademi
Datateknik

Innehållsförteckning

| | |
|--|-----------|
| 1. Introduktion | 2 |
| 2. Bakgrund | 3 |
| 2.1 Smarttelefonen | 3 |
| 2.2 Operativsystem | 4 |
| 3. Smarttelefonsäkerhet | 5 |
| 3.1 Informationsäkerhet | 5 |
| 3.2 Statistik | 6 |
| 4. Säkerhet inom operativsystem | 8 |
| 4.1 Säkerhetsproblem | 8 |
| 4.2 Operativsystem och uppdateringar | 9 |
| 4.3 Android och iOS | 10 |
| 4.4 Android | 11 |
| 4.5 iOS | 14 |
| 4.5.2 Jailbreak | 16 |
| 5. Analys och diskussion | 17 |
| 6. Sammanfattning | 17 |
| Referenser | 19 |

1. Introduktion

Världen utvecklas inom IT-sektorn där fler och fler apparater är kopplade till internet. Smarttelefons användningen har ökat ända sedan den kom till marknaden och har ökat t.o.m. de senaste åren drastiskt [1]. Detta leder till att cyberbrottsligheten har riktat sig mer och mer på smarttelefons användare eftersom mycket konfidentiell data både personlig och inom företag rör sig runt i användares smarttelefoner. Det betyder att tillverkare måste säkerställa användarens data samt skydda deras identitet i en värld där cyberattacker och virus blir allt allmänare. Enligt F-Secure är lösningen för att lyckas motarbeta cyberbrottslighet fordras användning av ett brett utbud på säkerhetslösningar, inte enskilda produkter [2]. När cybersäkerhetens betydelse har ökat och kommer att öka i framtiden betyder det att efterfrågan på konstanta säkerhetslösningar kommer att finnas. Här måste tillverkarna kunna ge användarna en hög uppdateringsfrekvens och hålla hög kvalitet på dessa uppdateringar för att hålla deras operativsystem säkra och aktuella till deras enheter.

Jag kommer i detta kandidatarbete att behandla teman som säkerhet, smarttelefoner, operativsystem och mjukvaruuppdateringar. Jag kommer att gå djupare in på hur frekvent olika operativsystem uppdateras för att förbättra smarttelefonens säkerhet beroende på vilken tillverkaren är. De operativsystem jag kommer analysera är Android och iOS. Dessa ger en heltäckande bild över de populäraste operativsystem för smarttelefoner. Eftersom många tillverkare använder sig av Android kommer jag att analysera flera än ett företag som använder sig av Android som operativsystem eftersom tillverkarna har egna policyn med uppdateringar. Operativsystemet iOS används endast av Apple Inc. och kommer att jämföra dessa olika tillverkare med avseende på hur deras policy skiljer sig från varandra och deras styrkor och svagheter.

Jag har som mål att framhäva betydelsen på hur ett operativsystem med uppdaterad mjukvara bibehåller säkerheten lämpligare för smarttelefoner än en

smarttelefon vars operativsystem ej längre erbjuds de senaste säkerhetsuppdateringarna. Dessutom att uppmärksamma konsumenten betydelsen om hur länge tillverkaren av enheten i allmänhet medför mjukvaru-uppdateringar. Detta stöder individen med hur frekvent det lönar sig att köpa en ny smarttelefon och medför inte en onödig säkerhetsrisk. Något övrigt denna avhandling kan stöda är för företag som har arbetstelefoner för anställda. Denna information har också stor nytta för företag var säkerheten kan ha mer betydelse men också ett enkelt sätt att sänka kostnaderna för företaget med att inte lika frekvent ha behov av nya smarttelefoner. Om en person inte är medveten om att deras enhet inte är försedd eller kommer att ges de senaste uppdateringarna är risken större för att råka ut för en cyberattack. Därför är det viktigt att uppmärksamma smarttelefons användare om detta problem.

2. Bakgrund

2.1 Smarttelefonen

En smarttelefon är en mobiltelefon som kan utföra mer liknande prestandakrävande funktioner än en dator klarar av. Det är vanligt att enheten har ett pekskärmgränssnitt, kan kopplas till internet och operativsystemet kan ladda ner och köra applikationer. Smarttelefonen har existerat i över ett decennium och användarantalet har ökat för varje år. Detta leder till att företag utvecklar nya funktioner till att använda smarttelefonen för. Med en möjlighet på miljontals olika applikationer att ladda ner, ges mängder av möjligheter för användaren att använda sin smarttelefon [3]. Med användarnas ökade möjlighet till användning av smarttelefonen leder detta till att allt mer och mer data och framförallt personlig data existerar på dessa enheter. Med dessa påföljder har smarttelefonen revolutionerat samhället med att smarttelefons användare har "hela sitt liv" i dessa apparater som kan ha stora påföljder. Här är det viktigt att användaren är medveten om riskerna och är aktuell insatt i egna enheten. Hur säker är enheten och hur länge kommer det att erbjudas mjukvaruuppdateringar av tillverkaren. Något som användare kan påverka är från vilket företag de väljer att införskaffa sin enhet ifrån. Det som spelar stor roll för

användarens smarttelefons säkerhet är hur länge det erbjuds mjukvaruuppdateringar med tanke på först och främst vilket företag det gäller, men dessutom vilket operativsystem företaget använder sig av.

2.2 Operativsystem

För att en enhets hårdvara skall fungera tillsammans med de installerade tillämpningsprogrammen eller applikations programvaran krävs ett operativsystem. Ett operativsystem består av en samling program som förenklar användandet av enheten. Operativsystemet är alltså som en mellanhand till användaren och enhetens hårdvara. Operativsystemets huvudsakliga syfte är att systemet skall vara enkelt att använda, använda hårdvaran effektivt, kunna köra användarprogrammen och understödja felsökning [4].

Operativsystemet tillhandahåller tämligen enhetliga gränssnitt vilket ger en bred möjlighet till olika apparater som datorn eller smarttelefonen kan interagera med t.ex. andra trådlösa nätverks komponenter. Detta har blivit en populär konkurrenskraft inom IT sektorn var olika företag kan skapa enheter som kan bara kopplas till deras egna "ekosystem" eller bara erbjuda en viss mån av funktionerna om inte enheterna är av samma företag eller beroende på vilket operativsystem företaget använder sig av. De moderna operativsystemen är försedda med grafiskt användargränssnitt vilket säkerställer en enkel användning för användaren. Dessa moderna operativsystem stöder ett flertal mediaformat som audio, video, bild, kamera, pekskärm, GPS mm [4].

För mobila operativsystem har vi en annan bakgrund till säkerhetsproblem än de som uppstod för stationära och bärbara datorernas operativsystem, samt server-operativsystemen. Processen för dessa system var när ett problem hittades gav man ut en programfix eller använde sig av tredjeparts applikation som skyddade systemet. Detta gjordes istället för att omskriva operativsystemets kärnkod och erbjuda dessa lösningar genom operativsystemet. Med ett sådant tillvägagångssätt sparar man resurser. Stor andel för många av dessa systems kärnkod skapades innan

internet var en vardaglig tillgång för alla vilket det mobila operativsystemet inte var, tvärtom. Därför ger det en viss befogethet för användaren att kräva förbättrad säkerhet från en smarttelefons operativsystem eftersom det har en bättre grund än system som utvecklats i ett tidigare skede.

3. Smarttelefonsäkerhet

3.1 Informationssäkerhet

Ett stigande fenomen som uppkommit med smarttelefonen är att användaren kan ta med dessa mindre enheter inom deras vardag på ett behändigt sätt. En stationär eller bärbar dator följer inte med konstant under liknande omständigheter som en smarttelefon. Detta leder till att allt mer och mer data existerar på smarttelefonerna som inte förekom tidigare när telefonerna inte var kopplade till internet. Med en större möjlighet till användning leder det till att användaren är mer öppen för att använda smarttelefonen för flera ärenden. En ökad användnings profil inte bara för användarens eget bruk utan smarttelefoner används också ur ett företagsperspektiv. Detta kan leda till att alltmer känslig eller säkerhetsstämplad data lagras i dessa enheter vilket gör smarttelefonerna mer eftertraktansvärda för cyberattacker [5].

Smarttelefonens datahantering bildar ett problem tillsammans med applikationerna som i dagens läge erbjuds för olika tjänster. Dessa tjänster löser ofta problem eller behov för användaren vilket i sin tur lagrar data av användaren. Denna datamängd stiger i en mängd olika kategorier vilket en stor del av dessa kan vara väldigt känsliga för användaren t.ex. bilder, kreditkort, filer, GPS-lagring mm. men här skall vi inte heller glömma data som kan vara företagsrelaterad [4].

Det existerar många andra hot för smarttelefons användare och inte bara den data de själva väljer att lagra i deras enheter utan yttre hot som malware och trådlösa förbindelser Wi-Fi och Bluetooth som kan utnyttjas på en mängd olika sätt [6].

Eftersom data har blivit mer åtråvärt på marknaden har det ökat applikationer som i bakgrunden samlar in data av användarna utan användarens godkännande. Här har EU vidtagit åtgärder och intagit en dataskyddsförordning (GDPR) för att skydda användarnas personuppgifter [7]. Mer hotande tillvägagångssätt kan man även utföra med malware allt från att banda in samtal, förneka tillgång till enheten eller data i utbyte mot kapital (ransomware) [8].

Möjligheterna till smarttelefonens användbarhet utvidgas mer och mer vilket gör att säkerheten inte alltid hinner med i utvecklingen. Detta dilemma tillsammans att de olika operativsystemen har deras egna styrkor och svagheter, blir det återigen ett krav på hur mjukvaran måste framställas efter beroendet på vilket operativsystem det gäller. Vad för nackdelar eller buggar kan förekomma med operativsystemets version som enheten använder sig av och när det även existerar olika versioner av operativsystemen, komplicerar detta utvecklingen för tillverkarna ytterligare.

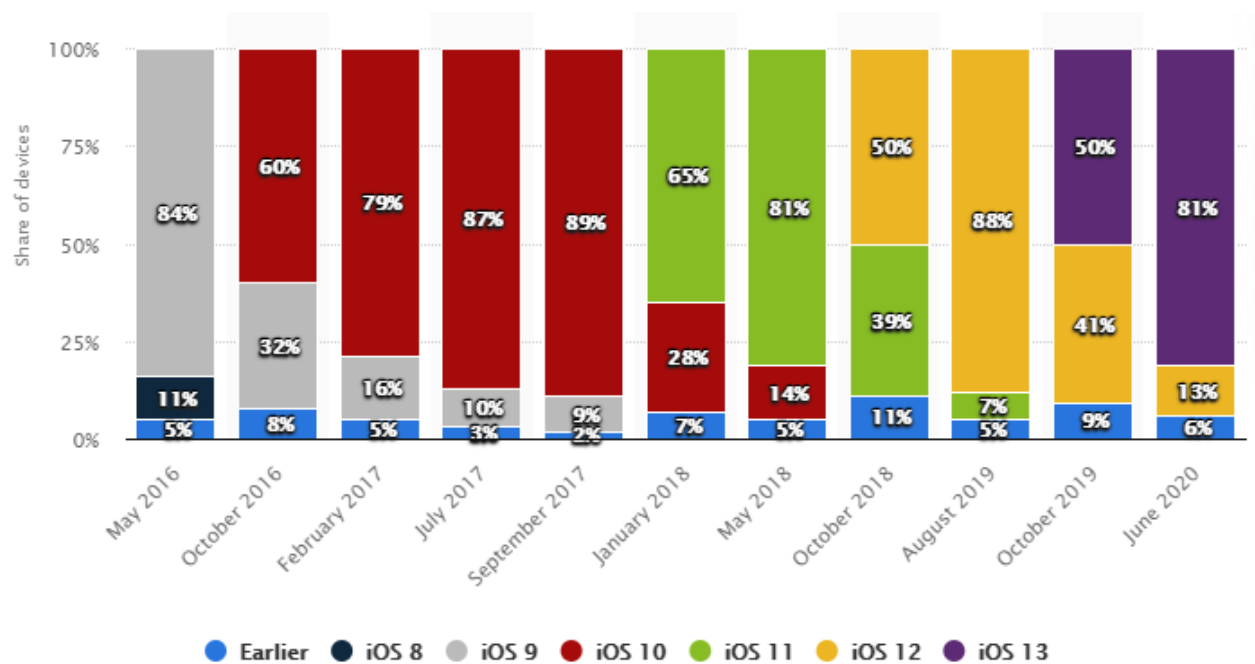
3.2 Statistik

Med en mer betydande smarttelefons användning är det inte en tillfällighet att hackers måltavla börjar skifta intensivare från datorer till smarttelefoner. Tyvärr hänger mycket på användarens kunskaper och hur aktuellt hen följer med sin egen enhet över dess säkerhetstillstånd. Dessutom kan inte säkerhetsuppdateringar skydda en från alla hot som existerar men det lägger avsevärt mindre risk för användaren att enheten fortfarande får uppdateringar. Här gäller det för tillverkaren att vara transparent med hur länge de erbjuder uppdateringar vilket förvarnar användaren när det börjar bli dags att byta till en ny enhet.

I en undersökning utförd av "Which?" kom man underfund med att över en miljard Android enheter är i riskzonen för attacker. Dessa enheter är sårbara för att de är försedda med äldre versioner av mjukvara. När de undersökte Googles egna data över Android enheterna använde över 40% av användarna operativsystem som ej längre får säkerhetsuppdateringar [9]. En stor orsak att detta sker specifikt för

Android enheter är pga. deras ekosystem. Till Skillnad från Apple som kommer ut med 1-2 nya smarttelefoner varje år och som kommer från samma tillverkare har flera hundratals olika smarttelefoner med Android kommit till marknaden från flera olika tillverkare. Detta utgör ett stort problem när det kommer ut en ny version av Android eftersom varje tillverkare måste välja vilka modifieringar de vill använda sig av från uppdateringen för deras egna enheter. Då kan det uppstå problem om tillverkarna antingen inte hänger med i uppdateringarna eller helt enkelt inte tycker det är värt att ge ut nya uppdateringar för deras äldre enheter.

Med tanke på smarttelefonsmarknaden var majoriteten har föredragit Androids operativsystem beror en stor del på att flera smarttelefonföretag använder sig av detta operativsystem. Android har ca. 70% av smarttelefonsmarknaden medans iOS har haft en andel på ca. 20% de senaste åren [10]. Androids antal av applikationer och dess öppna källkods baserade mjukvara är bland de största orsakerna till att android är så populärt. I jämförelse mot Apple var de använder sig av deras egna operativsystem (iOS) med sluten källkod för applikationer och inte erbjuder samma mängd applikationer tillsammans med det höga priset för deras smarttelefoner gör att de inte kan etablera sig ännu starkare i marknaden. Men något vi tydligt kan se i figur 1 vad Apples iOS lyckats med i jämförelse till Android användare är deras höga andel av användare som använder sig av de senaste versionerna av operativsystemet. Denna tydliga skillnaden av marknaden mellan Android och iOS tillsammans med hur stor andel av enheterna är uppdaterade till de senaste operativsystemsversionerna ger oss goda synpunkter av varför det sker mera attacker mot Android än iOS[11].



Figur 1: Apples procentandel av iPhones med vilken OS version.

4. Säkerhet inom operativsystem

4.1 Säkerhetsproblem

Ett stort problem som förekommer för smarttelefoner sker ofta med att tillverkare ger ut mjukvaruuppdateringar tillsammans med säkerhetsuppdateringarna. Detta kan leda till att flera enheter blir utan uppdateringar över en längre tidsperiod eller helt enkelt faller ut från gruppen som får mjukvaruuppdateringar vilket leder till att det blir en sekvens av att också säkerhetsuppdateringar avslutas för den enheten. I vilket fall som helst är båda av dessa fall ett stort säkerhetsproblem för ägarna till enheter som detta sker för. Det är inte alltid möjligt att förse äldre smarttelefoner med de nyaste uppdateringarna t.ex. p.ga. föråldrad hårdvara [12]. Skulle vara avsevärt mindre press på tillverkarna för smarttelefoner att istället för att satsa på flera olika smarttelefons modeller varje år istället lägga fokus på färre modeller. För att göra det enklare och kostsammare för dem i framtiden med att ge ut säkerhetsuppdateringar till färre

modeller och de håller sig relevanta att användas under en längre tidsperiod utan att användaren utsätts för högre säkerhetsrisk.

Som tidigare nämnts är det mycket ansvar för användaren. Dessa enheter har med hjälp av efterfrågan också ökat i pris. Detta kan göra livet svårare för den möjliga kunden på många olika sätt. Det blir ekonomiskt tyngre att köpa en smarttelefon lika frekvent som tidigare vilket kan leda till att hens enhet blir föråldrad. Det blir en svårt ämne för företag att lösa med tanke på "bring your own device" (BYOD) eller om företaget skall förse dess arbetare med smarttelefoner. Svårt kontrollerat alternativ vilket än företaget väljer. Med BYOD aspekten kan man inte tvinga ens arbetare att de alltid måste ha en smarttelefon som är "aktuell" och dessutom skall dessa enheter vara uppdaterade för att vara en mindre säkerhetsrisk. Om företaget förser arbetarna med enheter blir det svårt att kontrollera att dessa enheter för det första används till företagsmässiga ändamål. Att man t.ex. ej laddar ner applikationer som kan samla in data som är företagsstämplat. Detta kan också totalt förlora sin poäng om företagets arbetare väljer att använda deras gamla enhet till arbetet och utnyttjar istället företaget för att uppgradera deras privata enhet. Då blir slutresultatet att man fortfarande använder en föråldrad enhet till arbetet [13].

4.2 Operativsystem och uppdateringar

Smarttelefonen kan få bättre prestanda och nya funktionaliteter med mjukvaruuppdateringar. Men det viktigaste med mjukvaruuppdateringar till operativsystemet är att den inte skall bli föråldrad med tanke på säkerheten för smarttelefonen. En smarttelefon som inte har fått nya mjukvaruuppdateringar på de senaste åren skyddar ej mot alla de nyaste skadeprogram eller de säkerhetsbrister som kan hittas i operativsystemen. Så fort som mjukvaruleverantörer hittar på lösningar att fixa exploaterbara hål i deras programvara, har hackare börjat försöka hitta nya säkerhetsbrister. Det är en oändligt cirkel som mjukvaruföretag fångas upp med cyber kriminaliteten för att skydda sina användare. I dagens läge existerar

företag som har anställt personer att försöka hitta dessa exploaterbara hål för att sedan komma på säkerhetslösningar var säkerheten är bristfällig.

4.3 Android och iOS

Jag har valt att undersöka dessa operativsystem pga. deras popularitet men också med tanke på att det finns flera tillverkare som använder sig av Android, vilket skiljer sig från iOS som bara används av Apples egna tillverkade smarttelefoner. Båda operativsystemen har sina styrkor och svagheter och skiljer sig en hel del när vi tittar på säkerhetsproblemen som kan uppstå. Här gäller det att användarna måste tänka på vad som är viktigt för en själv och vilken enhet är bäst för ens egna användning.

Det finns många styrkor med att företag ansvarar och utvecklar själva operativsystemet från början till slut ens apparater skall använda. Apple är ett företag som har en mycket stark position inom smarttelefons sektorn och är mycket omtyckta med tanke på deras användarvänliga operativsystem. Något som ytterligare stödjer Apples popularitet med tanke på att de kunnat utveckla ett operativsystem som de kan använda för deras andra elektroniska apparater som har en liknande användargränssnitt t.ex. smart plattor, smart klockor, stationära datorer mm. Dessa apparater bildar ett uppskattat "ekosystem" tillsammans vilket tilltalar kunder att använda flera av Apples enheter eftersom de kan synkronisera med t.ex. inställningar, applikationer, bilder, anteckningar [14].

Android däremot är ett lite mera komplext operativsystem med tanke på att det utvecklas genom open source och ägs kommersiellt av Google [15]. Android används av flera olika företag med deras egna justeringar och personlig touch som är anpassade för just deras smarttelefoner. Detta öppnar många dörrar för positiva användarmöjligheter men ställer stora krav på företagen med tanke på framförallt säkerhetsuppdateringar. Det blir svårt för företagen att uppnå en hög standard med nya mjukvaru funktioner och att samtidigt hålla säkerhetskraven höga. Vilket enkelt kan leda till att äldre smarttelefons enheter blir utelämnade från

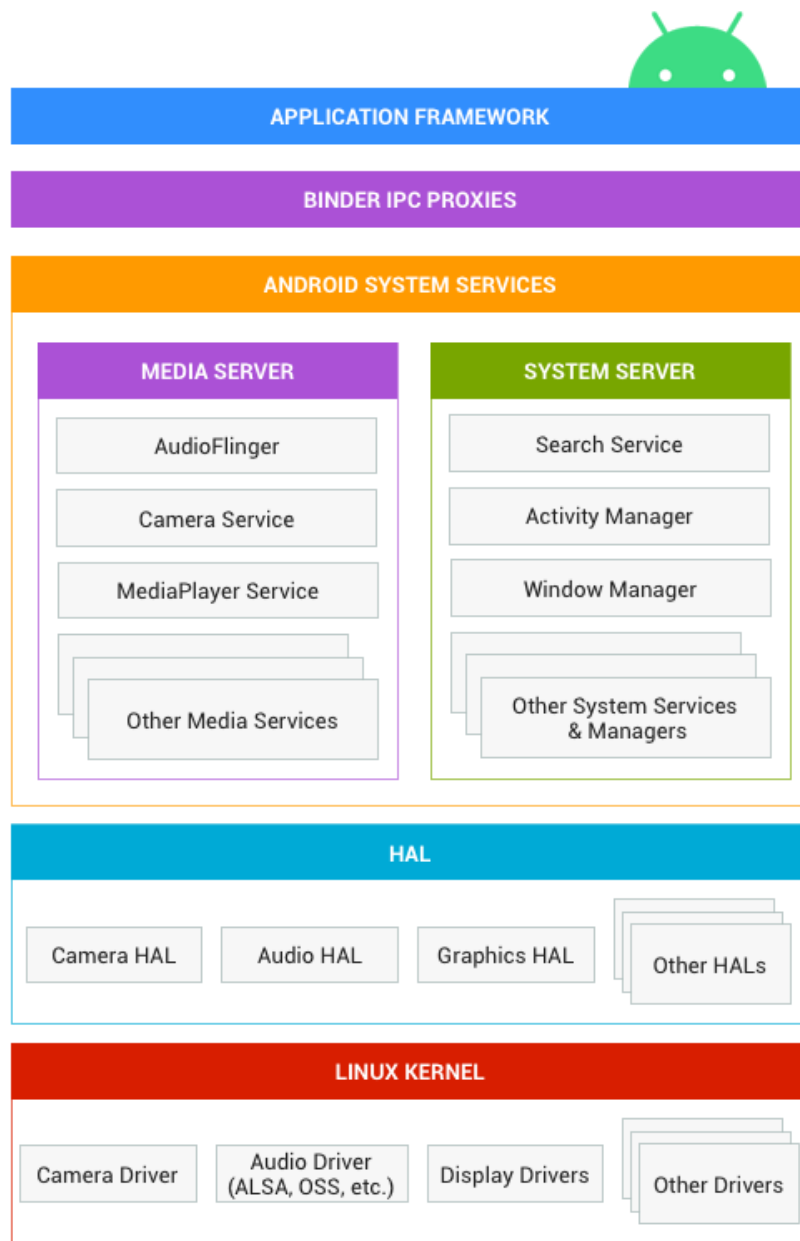
mjukvaruuppdateringar. Något som kan ske p.g.a. olika orsaker men en avsevärd stor faktor är kostnader att uppehålla äldre enheter som inte hämtar in inkomst till företaget lika mycket som nya enheter [16]. Jag kommer att undersöka djupare Googles egna Pixel smarttelefoner och OnePlus smarttelefoner som lanserats genom åren och använder sig av Android för att ge oss en bättre överblick skillnader mellan iOS och Android.

4.4 Android

Android använder sig av en modifierad version av Linux Kernel tillsammans med andra öppna mjukvaror. Det utvecklades först av Android Inc. men blev uppköpta av Google 2005 [17]. Efter det har Google tillsammans med andra företag sammanslutit sig till Open Handset Alliance vilket är ett samarbete för att kunna erbjuda konsumenterna en accelererad innovativitet med lägre pris och för en bättre användningsupplevelse[18]. De släppte första versionen av Android OS år 2007. Androids källkod Android Open Source Project (AOSP) går under Apache licensen som Apache Software Foundation (ASF) distribuerar programvara som baserar sig på öppen källkod. Android har programmerats i största del med Java, C och C++ [19]. Med detta tillvägagångssätt är det inte bara Google eller de andra organisationer som är med i Open Handset Alliance kunnande man kan utnyttja för att utveckla Android.

Googles beslut att göra källkoden tillgänglig för alla ger möjligheter för tredjepartsutvecklare att fritt insätta tillägg utan behöva göra dem tillgängliga för deras öppna mjukvarucommunity, bara de följer licensvillkoren. Trots att Android är ett operativsystem som erbjuder fri och öppen källkod (FOSS) ges en stor del av smarttelefonerna med ytterligare förinstallerad mjukvara där den mest noterbara är Google Mobile Services (GMS). Här ingår Googles ekosystem med t.ex. applikationer som Google Chrome, Youtube, Gmail, Google Maps och Google Play, av vilka den sistnämnda är Googles digitala applikations distributör [20].

Uppbyggnad (fattas)



Figur X: Androids operativsystems uppbyggnad

1. Google Pixel (fattas)

allmänt kort

styrkor/svagheter med deras uppdaterings historia/policy

(skillnader/jämförelser i analys)



Figur X: Googles lansering av Google Pixel 4a & 5 30.9.2020

2. OnePlus (fattas)

allmänt kort

styrkor/svagheter med deras uppdaterings historia/policy

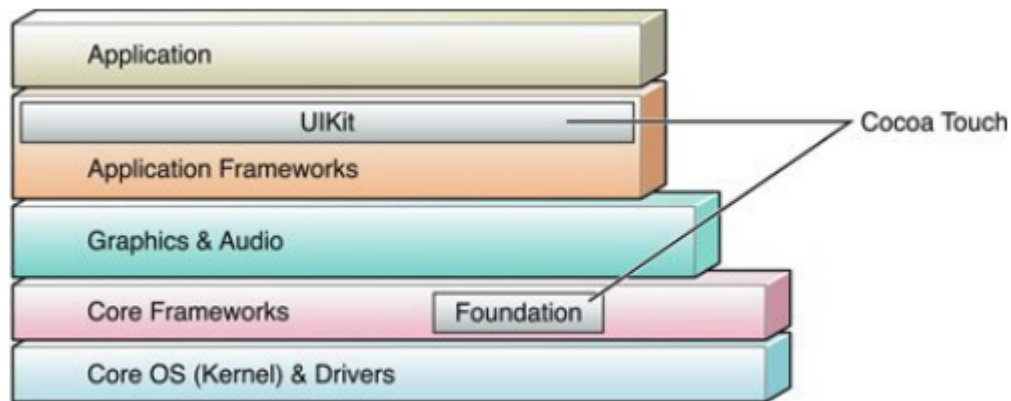
(skillnader/jämförelser i analys)

4.5 iOS

Apples egna operativsystem iOS som används för deras smarttelefoner är utvecklat för att endast deras egna tillverkade enheter skall använda detta operativsystem. Lika som Android släppte Apple ut första versionen av iOS 2007. Det är det andra mest nedladdade mobila operativsystemet efter Android [4]. Till skillnad från Android är iOS ett företagsspecifikt programvara där bara endast en bråkdel är öppen källkod under Apple Public Source License (APSL) under ASF licensen [21]. Kerneln iOS använder sig av är XNU kerneln av Darwin operativsystemet. Darwin är utvecklat av Apple härledd från tidigare operativsystem och andra fria mjukvaru projekt. Darwin utformar grunden av komponenter som iOS är baserad av och även åt andra av Apples enheters operativsystem t.ex. macOS, watchOS, iPadOS. De programmeringsspråk Apple använt sig av för att utveckla iOS är C, C++, deras egna utvecklade programmeringsspråk Objective-C och Swift. Apple utvecklade Swift för att ersätta Objective-C som saknade modernare funktioner [4][22].

Uppbyggnad (fattas)

<https://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=6637558>



Figur X: Cocoa Touch gränssnitt i Apples iOS uppbyggnad

Med tanke på andra telefontillverkare det finns på marknaden har Apple en av de bästa om inte det bästa tillvägagångssättet när det gäller mjukvaruuppdateringar för deras smarttelefoner (iPhones). Den kortaste perioden som Apple har erbjudit mjukvaruuppdateringar var 36 månader för deras första iPhone. Om vi tittar på några senare modeller som Apple har tillverkat har månaderna av support rört sig runt 50-60 månader av mjukvaruuppdateringar. En policy att erbjuda i så många månader uppdateringar gör att de sticker ut av mängden eftersom ingen kan jämföra sig av en så här lång period av uppdateringar. Detta betyder inte att iOS är säkrare i alla aspekter än andra tillverkare eller Android men det ger visserligen en mindre risk med att använda en ouppdaterad enhet som ej kommer att få nya uppdateringar till operativsystemet. När Apple har gett ut en ny version av deras operativsystem (iOS) utger de ej säkerhetsuppdateringar till äldre iOS versioner såvida det inte är en extremt stor sårbarhet av äldre versionen som hittas i ett senare skede. Den enkla lösningen är att man måste uppgradera ens enhet till de senare versionerna för att få alla säkerhets korrigeringar till sin enhet. Apple nämner på deras hemsida över detta, "En av de viktigaste säkerhetsåtgärderna är att se till att Apple-mjukvaran är uppdaterad". Apple har även en sådan policy om ett hot existerar, granskar de först att risken är hanterad innan de bekräftar att ett säkerhetsproblem förekom, "Apple

skyddar sina kunder genom att aldrig avslöja, diskutera eller bekräfta säkerhetsproblem innan en fullständig utredning har genomförts och alla nödvändiga program korrigeringar eller utgåvor är tillgängliga”.



Figur X: Hur länge Apple erbjuder uppdateringar till äldre iPhone modeller

4.5.2 Jailbreak

Jailbreak är ett fenomen som har uppkommit med Apples produkter som gör det möjligt för användarna att avskaffa vissa restriktioner men ändå använda deras produkter. Genom att förändra iPhonens mjukvara för att sedan kringgå begränsningar som Apple infört. Vad det innebär med denna process är att man har

möjlighet att installera och använda tredjeparts program som inte har blivit godkända av Apple. Varför dessa inte har blivit godkända kan det finnas många olika förklaringar till men eftersom Apple inte accepterar varenda applikation till deras App Store vilket är tillsammans med iTunes de enda plattformarna var man skall enligt Apple ladda ner applikationerna till sin iPhone. Detta är en stor anledning till varför jailbreaking existerar. Men Apple har dessutom valt att ha en del extra säkerhetsåtgärder vilket leder till att det är svårare att köra skadlig programvara i deras iOS. Alla applikationer som är godkända av Apple utlovar ett minimum av kvalite och säkerhet vilket gör att en användare som väljer att hålla sig borta från jailbreaking kan känna sig säkrare eftersom en stor säkerhetsrisk för en iPhone är när den har blivit jailbreakad. Men detta har även sina nackdelar med att normala procedurer begränsas vilket leder till att användarupplevelsen blir sämre. Detta är en stor skillnad mellan iOS och Androids operativsystemen var man har mycket mera frihet och möjligheter att kunna ladda ner mjukvara och använda sig av olika plug-ins. Detta ses som en orsak varför personer väljer att använda sig av jailbreak möjligheten för att kunna använda Apples produkter på ett mer justerbart sätt som passar just den användarens behov.

5. Analys och diskussion

- jämförelse mellan Android tillverkare och sen dom jämförelse mellan iOS
- för företag kanske dyrare telefoner som erbjuder längre uppdateringar än att måsta mera frekvent uppdatera ens enheter
- vilka egenskaper/olikheter
- styrkor/svageter

6. Sammanfattning

- (sammanfattning) runt 0.5 sida
- mer transparent med användaren, tydligare hur länge man får uppdateringar, vad lönar sig att göra efter det och lösningar för användaren när uppdateringarna slutar komma
 - lagar/staten krav på tillverkare på dessa problem
 - tyvärr mycket hänger upp till användaren/human element
 - färre enheter-->mera fokus på uppdateringar och att förbättra dem

-Operativsystemet kan vara till stor hjälp men kan inte skydda mot alla attacker, användaren måste själv vara aktiv och utbilda/lära sig hur de bäst kan använda deras smarttelefoner men ändå tänka på säkerheten

Referenser

(Läggs in efter att jag fått texten färdigt, sparat dom i mina bokmärken)

[1]

<https://www.statista.com/statistics/330695/number-of-smartphone-users-worldwide/>

[2] "Market and strategy | F-Secure for investors." [Online]. Available:

https://www.f-secure.com/en/web/investors_global/management/strategy-and-vision.

[Accessed: 14-Jan-2019]

[3] <https://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=6980261>

[4] <https://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=7980403>

[5]

<https://online.maryville.edu/blog/the-rise-of-mobile-attacks-and-what-that-means-for-you/>

[6] <https://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=5875929>

[7] <https://gdpr.eu/tag/gdpr/>

[8] <https://www.kaspersky.com/resource-center/definitions/what-is-ransomware>

[9] <https://www.bbc.com/news/technology-51751950>

[10]

<https://www.statista.com/statistics/272698/global-market-share-held-by-mobile-operating-systems-since-2009/>

[11]

<https://www.statista.com/statistics/565270/apple-devices-ios-version-share-worldwide/>

[12]

<https://www.howtogeek.com/129273/why-your-android-phone-isnt-getting-operating-system-updates-and-what-you-can-do-about-it/>

[13]

<https://digitalguardian.com/blog/ultimate-guide-byod-security-overcoming-challenges-creating-effective-policies-and-mitigating>

- [14] <https://www.businessinsider.com/apple-iphone-macbook-ecosystem-so-good-i-dont-want-iphone-2019-12?r=US&IR=T>
- [15] <https://source.android.com/>
- [16] <https://www.androidcentral.com/why-you-ll-never-have-latest-version-android>
- [17] <https://www.androidauthority.com/google-android-acquisition-884194/#:~:text=Why%20Google%20buying%20Android%20was.companies%20in%20all%20of%202005.&text=Some%20of%20Google's%20other%20acquisitions%20have%20not%20bee n%20as%20successful%2C%20however.>
- [18] http://www.openhandsetalliance.com/oha_faq.html
- [19] https://www.openhub.net/p/android/analyses/latest/languages_summary
- [20] <https://www.android.com/gms/>
- [21] <https://opensource.apple.com/apsl/>
- [22] <https://developer.apple.com/library/archive/documentation/Darwin/Conceptual/KernelProgramming/Architecture/Architecture.html>

Figurer:

Figur X

<https://www.statista.com/statistics/565270/apple-devices-ios-version-share-worldwide/>

Figur x (androids mjukvaru plattform) <https://developer.android.com/guide/platform>

Figur x (androids uppbyggnad) <https://source.android.com/devices/architecture>

Figur X (google pixel launch)

https://www.youtube.com/watch?v=q2HSJHOMDyk&ab_channel=MadebyGoogle

Figur X (iPhone modeller uppdateringar)

<https://www.statista.com/chart/5824/ios-iphone-compatibility/>

Figur X (iOS cocoa touch)

<https://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=7980403>