Johan Paramanathan
Tanusan Rajmohan

15.05.16

iOS Sikkerhetshull

Figur 1 (Hentet fra Softpedia)

Innhold: I denne oppgaven tar vi for oss den generelle oppbygging av iOS og kommer inn på sikkerhetskomponentene ved operativsystemet. Deretter vil vi ta for oss diverse utførte angrep og løsninger, samt statistikk. Strukturen i oppgaven er satt opp slik at vi tar for oss de diverse sikkerhetskomponentene, med en hendelse eller angrep relatert til det respektive området. Når det gjelder jailbreaking har vi begge erfaring med dette, så noe av informasjonen er kontribuert derfra. Til slutt tar vi for oss hendelser som nylig har forekommet og drøfter om dagens situasjon, og hva som potensielt kan påvirke trusselbilde.

Innholdsfortegnelse

[x.] Eksempel overskrift

Alle overskriftene med [x] er en merknad til referansene.

[0] Introduksjon:

Sikkerhet er et omdiskutert tema i dagens IT-samfunn. Personvern og trygghet, står høyt oppe på listen over krav som blir stilt ovenfor de største aktørene. Ettersom antall angrep på mobile enheter vokser i rekord fart, står de største leverandørene ovenfor store utfordringer. Det blir stadig lagret sensitive data på telefonen, bilder har for eksempel blitt omdiskutert en del i media. Apple påstår at sikkerhet og personvern er fundamentalt. Det er dermed essensielt å diskutere om de forskjellige sikkerhetsaspektene ved iOS holder mål.

[1] Hva er iOS?

iOS er et mobilt operativsystem utviklet av Apple Inc, og ble for første gang lansert i 2007 sammen med den første iPhonen, hvor de bare kalte det for iOS X. I dag brukes fortsatt iOS hos de nyere produktene bare i en nyere form. Dagens programvare kalles for iOS 9.2.1 som støtter enheter helt ned til iPhone 4s. I dag er Apple blant de mest fremtredende og attraktive produsentene innenfor mobiltelefoni, datamaskiner, smart-klokker, bilteknologi og tv-teknologi. De har forskjellige operativsystemer til hver type enhet, iOS til mobile enheter, OS X til datamaskiner, tvOS for de nye Apple Tv-ene og watchOS for de nye smartklokkene. iOS plattformen brukes hovedsakelig for iPader, iPhoner og iPoder. Selv med så mange forskjellige systemer så klarer de fortsatt å gi ut hyppige oppdateringer. Det mobile OSet har i snitt 5 oppdateringer per år.

Figur 2 (Apple logo gjennom historien, hentet fra wikipedia)

Oppbygning av iOS

I 2007 annonserte Apple den første iPhonen som skulle kjøre på samme Unix kjerne som Mac OS X og skulle ha mulighet til å bruke de samme verktøyene som Mac. Under lanseringen ble operativsystemet kalt "iPhone OS" og den beholdt dette navnet helt til iOS 4 kom. I 2010 ble navnet på OSet endret til iOS for enkelhetsskyld og fordi det hørtes bedre ut.

Det første OSet som kom var helt nytt og spennende. Det er kanskje litt vanskelig å tenke seg at Apple slet i starten, men de var et stykke bak konkurrentene. I det første OSet så hadde Apple et par mangler som blant annet at den ikke støttet tredjepartsapper, man kunne ikke multitaske, klippe og lime og ikke sende MMS. Den var stort sett veldig lukket, så det var en liten sannsynlighet for at den ville bli hacket. Selv med disse manglene ble de uansett populære.Apple kom med følgende utsagn om manglene, "*Instead of competing on specs, Apple focused on getting the core experience right*"[1]. En av tingene Apple gjorde som ble en suksess var at de kom med en ny interaksjons metode, nemlig touch skjerm. Dette var noe som endret da tidens syn på interaksjon. En annen ting Apple gjorde var å skjule filsystemet, noe som gjorde at produktet ble mer

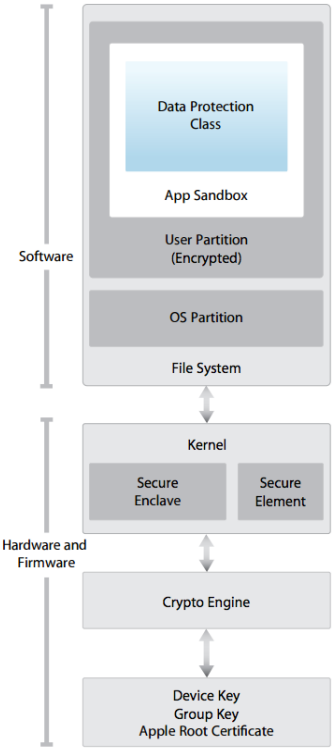
[1] *"iOS: A visual history",* Verge Staff

brukervennlig og lett. "*iOS 1.0 also introduced a new computing paradigm that broke from smartphone tradition: hiding the filesystem*[2] *from the user*."[3]

"*Apple would be continuously updating iOS with new verisons and new features*". Den første oppdateringen av systemet kom kun tre måneder etter at den første iPhonen kom ut på markedet. Oppdateringene som kom i starten hadde et par nye trekk og endringer som blant annet "iTunes Wi-Fi Music Store", "Re-arrange icons" funksjonen, "Multitouch keyboard" osv. De store endringene tok plass når det eventuelt kom et nytt produkt på markedet. For eksempel, mellom hoppet fra iPhoneOS(iOS) 1 til iPhoneOS(iOS) 2 så endret de firmware slik at det var mulig og ha tredjepartsapper. Det var da *The App Store* kom ut på iOS, noe som gjør det mulig å laste ned og utvilke apper til diverse enheter. Under de små endringene som for eksempel fra iOS 2.1 til 2.2 ble et par ting rettet opp, som blant annet at det var mulig å laste ned Podcasts og Google street view ble tilgjengelig.

[2] Sikkerhetskomponenter

Etter mye medieoppmerksomhet rundt sikkerheten rundt produktene sine, har Apple blitt mer fokusert på sine mobile plattformer. Senere versjoner av iOS (7,8,9), har brukeropplevelse blitt mindre prioriritet, hvor sikkerhet har blitt satt høyere på listen. I de seneste årene har det blitt gjort et stort antall angrep på en rekke iOS enheter. Dette medfører at utviklingen av et robust system automatisk kommer i søkelyset.



Figur 3 (OS-oppbygning)

Kortfattet består oppbygningen av en programvare og en maskinvare/firmware del. De fleste angrepene blir gjort på programvarenivå og er dermed "lettere" å rette på. Et av de viktigste hovedtrekkene ved programvare-sikkerheten, er *App Sandbox* som i teorien går ut på at brukeren ikke får tilgang til filbehandleren. Dette kan sammenlignes med en sandkasse, hvor apper kun har tilgang til sitt eget begrensede område. Videre i samspill med *App Sandbox* kommer et krypteringslag(eng: *encryption and data protetction*), som brukes for å sikre at uautoriserte personer ikke får dekryptere data. Dette laget blir konfigurert automatisk, slik at brukere ikke deaktiverer/aktiverer ved en feiltakelse. Hovedsaklig brukes sanboksteknologien, for å forhindre at system integriteten blir påvirket. Brukere skal i teorien ikke være i stand til å komme seg gjennom dette laget. Noen brukere har "trengt seg gjennom" krypteringslaget, og åpnet opp muligheten for å laste ned ikke-godkjente apper. Dette fenomenet er også kjent som *jailbreaking* eller å "roote" telefonen.

[2] "Hiding the filesystem" vil si at brukeren ikke kan endre, fjerne eller legge til filer uten verktøyene som Apple har skapt, slik som iTunes.
[3] *"iOS: A visual history",* Verge Staff

Maskinvare/firmware (eng: hardware) kan kun rettes opp hvis modellen fysisk oppgraderes. Angrep på maskinvare nivå forkommer sjeldnere, og er som nevnt vanskeligere å rette opp og utvikle. Noe av den viktigste maskinvare teknologien som har blitt utviklet i senere tid, er Touch ID og crypto engine. Touch ID er en biometrisk sikkerhetsfunksjon som går på gjenkjenning av fingeravtrykk. Touch ID gjør det vanskelig for hackere å trenge seg gjennom. Dette på grunn av de utallige kombinasjonene som finnes for å kopiere fingeravtrykk. De lange komplekse kodene blir lagret som fingeravtrykket, ikke som et fysisk bilde. Dermed slipper bruker å huske på denne koden. Passord beskyttelse har lenge vært en autorisering metode, på samtlige av iOS-enhetene. Det er dermed sagt at det ikke er umulig å hacke, f. eks har det blitt laget " IP box ", som kortfattet prøver alle mulige kombinasjoner fra 0000 til 9999.

Dette har blitt rettet opp i senere versjoner av iOS(9.x.x). Løsningen var å innføre en 10-forsøk sperre grense på programvaren. Siden dette også er et maskinvare angrep, måtte en eventuell oppgradering komme ved neste iPhone lansering. Derfor innførte Apple A7 prosessor, som funger som en TPM[4] chip. Med andre ord kan ikke uautorisert tredjeparts maskinvare bruke enheter med A7, eller nyere A-serie prosessorer. Det samme gjelder de nye laderne, som inneholder et sertifikat. Dette er spesialdesignet til å identifisere om laderen er skapt av et autorisert firma og ikke inneholder noe skadelig. Denne maskinvaren ble satt i gang også etter at A7 prosessorene kom som kom i september 2013.

[3] Nettverksikkerhet og iCloud

Nettverksikkerhet har med årene blitt et større trussel område for de største selskapene. DoS (Denial of Service) har i følge Forbes Magazine, økt med 57% fra i fjor. Nettverksikkerhet er derfor minst like omfattende som hardware/software sikkerhet. I følge mørketall rapporten fra 2014, er det essensielt med et godt nettverkssystem, foruten kan dette lede til økt antall angrep. Nettverksikkerhet har dermed med årene blitt et veldig aktuelt tema i hvert fall med tanke på iOS.

Figur 4 (Illustrasjon av cloud teknologien)

Kommunikasjonen som brukes i iOS' nettverksikkerhet er en kryptert ende-til-ende kommunikasjon (Eng: *Secure socket layer*) v3.0 i samspill med transport lags sikkerhet (eng: *Transport layer security*) v1.2. Det blir også brukt digitale sertifikater (DTLS), for å etablere en sikkerkobling mellom enheter og servere. Dette er standardiserte nettverksprotokoller, og blir brukt over hele verden. Selv om nettverks teknologien er standardisert, kan angrep forekomme, men vanskelighetsgraden blir økt betraktelig. DTLS fungerer som et identifiserings ledd mellom enhet og server. Den

[4] Trusted Platform Module = sikker krypteringsprosessor som kan lagre krypterte nøkler som beskytter informasjon

bruker public keys[5] og private keys[6], som er to mekanismer som gir en sikker ende-til-ende kommunikasjon, ved å kryptere og dekryptere dataen.

iCloud er en skytjeneste, som tilbyr brukeren å lagre data i en "sky", altså lagre data utenfor den fysiske enheten. Dataen kan være kontakter, bilder, dokumenter eller annen informasjon som er relevant for tredje-parts applikasjoner. iCloud håndterer alt innholdet ved å kryptere dataen med AES[7]-128. Nøklene blir sortert i en hierarkisk ordning, som blir lagret i *iCloud keychain*. Denne funksjonen tillater brukere å dele passord, over flere enheter som er eid av samme bruker. De krypterte bytesene blir lagret i tredjeparts applikasjoner som Windows Azure og Amazon S3. De resterende metadataene og nøklene blir lagret i iClouden, med andre ord, har Apple ikke direkte tilgang til brukerens passord. Hvis dataen som er lagret hos tredjeparts applikasjonene kommer på avveie eller blir misbrukt, er dataen kryptert med vilkårlig tall. Dette gjør det vanskelig for potensielle hackere å bruke informasjonen til noe som helst.

[4] iCloud - Hull i skyen?

Figur 5 (iCloud logo)

Tilbake i 2014 ble det gjort et stort angrepet på en rekke iOS enheter eid av kjendiser. Dette ble utført via iCloud, men var ikke et dirkete angrep på iCloud. Angrepet på enhetene ble gjort ved at hackerne fant et smutthull i Apples *Find My iPhone* teknologi. Dette smutthullet gikk ut på å bruke en metode som heter "brute-forcing"[8]. Grunnen til at dette var mulig var at iClouds innloggingsfase ikke hadde noen sikkerhet eller "fail-switch". Man hadde altså et uendelig antall forsøk på å taste inn passordet. Dette ga hackere muligheten til å aksessere kontoen, uten at brukeren ble informert. Det skal sies at det originale innbruddet på mobilen skal ha vært gjort via "chaining"[9] mellom de ulike kontoene. Når de fikk tilgang til brukerens konto klarte de å koble seg videre til neste mål/bruker via kontaktlisten til den brukeren de allerede hadde hacket.

Cloud-angrepet har blitt ansett som et simpelt angrep, men har gitt Apple utviklerne hodebry med tanke på å rette opp "smutthullet". "*This means that your data is protected from unauthorised access both while it is being transmitted to your devices and when it is stored in the cloud.*"[10] Dette ble skrevet av Apples administrerende direktør Tim Cook. En mulig løsning var å innføre "two-step-verification", som er en måte å dobbelt sjekke at det er riktig person. Enten ved å sende kode på melding som brukeren skulle taste inn som en ekstra bekreftelse. Dette valget har Apple gitt brukeren, så brukeren får velge om vedkommende vil ha "two-step-verification". Apple valgte å legge inn et nytt varslings

[5] Public key – En nøkkel tilgjenelig for alle sammen, f.eks et mobil nummer
[6] Private key – En nøkkel som må forbli konfedensiell, f.eks en pin-kode til simkort.
[7] Advanced Encryption Standard (AES) = en algoritme for å kryptere informasjon.
[8] Metode som sjekker om at alle nøkler er oppfylt etter kravet: $d_K(y_0) = x_0$
[9] Chaining - gå fra en "bruker" til en annen via den første "brukeren"
[10] "*Data security*", Apple.com

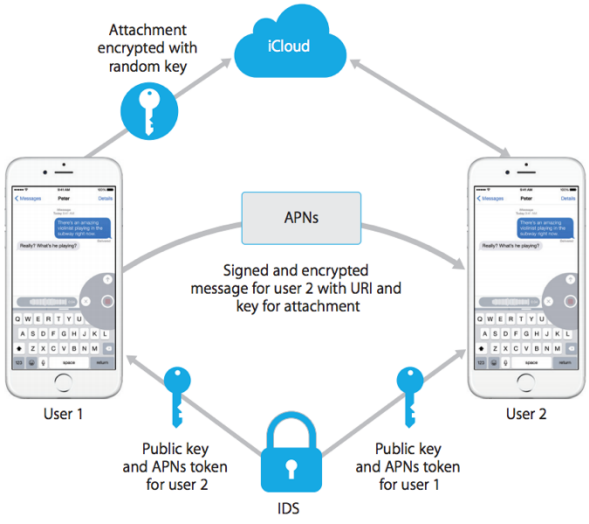
system, for å sikre brukerne. Dette gjorde at brukeren fikk varsel hver gang noen logger inn på en annen PC, enn den registrerte. Denne varslingen ble sendt til brukerens mail-adresse.

I denne perioden hadde Apple hendene fulle med kjendis-saken, som rammet flere hundre brukere. Like etter denne hendelsen, oppstod det enda et angrep på iCloud. Denne gangen var det et angrep på serverne i Kina som stod for tur. Dette angrepet var ikke som det forrige, hvor hackeren prøvde en brute-force metode. Motivasjonen til angriperne var ute brukernavn, passord og annen personlig informasjon til diverse enkelt brukere. "*We're aware of intermittent organised network attacks using insecure certificates to obtain user information, and we take this very seriously*,"[11] Apple la ut denne meldingen på supportsiden sin, hvor de også hadde nevnt at serverne deres ikke hadde blitt påvirket. Dette angrepet var et "indirekte angrep", hvor hackere hadde brukt et tredjeparts program for å prøve å lure brukeren. Denne typen angrep er også kjent som phishing. Apple forklarte også i en pressemelding at de med det seneste OSet ikke skulle ha blitt påvirket av dette angrepet. "*If users get an invalid certificate warning in their browser while visiting www.icloud.com , they should pay attention to the warning and not proceed*,"[11] . Apple gav beskjed snarest til brukerne skulle se hvor de logget inn, siden hackerne også hadde prøvd å få brukeren til å taste inn passordet på en nettside med falsk sertifikat. Dette angrepet hadde ingen sammenheng med det forrige angrepet.

Figur 6 (Hentet fra The Guardian)

[5] iMessage - Sikker kommunikasjon

iOS bruker sin egen meldingstjeneste kalt iMessage for sending av tekstmeldinger, bilder, kontakter og vedlegg. Tjenesten bruker push-varsler (eng: *push-notification*)[12] og en public og private key for å beskytte dataen som blir sendt (Se illustrasjon). Apple logger ikke dataen, og ingen andre enn brukerne kan kryptere og dekryptere hverandres meldinger. iMessage i likhet med nettverksikkerheten bruker også en sikker ende-til-ende kommunikasjon.



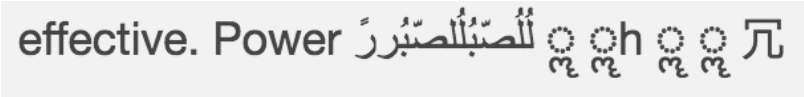
Figur 7 - Illustrasjon av hvordan kommunikasjonen mellom to brukere fungerer.

[11] "*Apple warns of new iCloud threat*", The Guardian

[12] Apple Push Notification Service - gjør at tredjepartsprogramutviklere sender notifications (varslinger) til programmer som er installert på Apple-enheter .

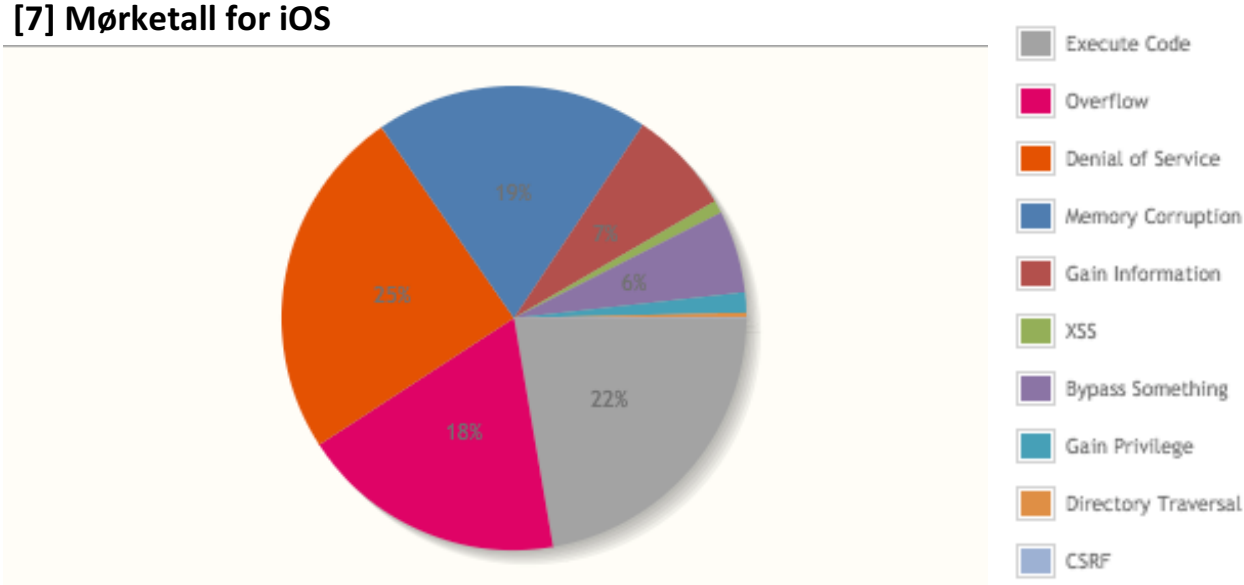
[6] Liten melding, store konsekvenser

I mai 2015 oppstod det et problem med meldingstjenesten til Apple, dette buggen ble hovedsakelig brukt for ikke-ondsinnede intensjoner. Noen hadde funnet en bug i systemet som fikk enheten til å krasje og starte på nytt, dersom man sendte en spesiell melding. Meldingen som forårsaker krasjet bestod av fire språk: engelsk, arabisk, marathi og kinesisk. Det blir antatt at buggen kanskje kunne være at systemet ikke taklet fremvisning av 4 forskjellige språk samtidig i varslingslinjen. Denne buggen skal tydeligvis ha funket på alle enheter som hadde et operativsystem under iOS 8.3, uansett om de var jailbreaket eller ikke. Det viste seg i tillegg at hvis en bruker eide en Apple watch som var tilkoblet den samme enheten, så ville smart-klokken også krasje og starte på nytt. Apple gikk rett på saken og kom med en melding så fort problemet ble oppdaget, "*We are aware of an iMessage issue caused by a specific series of unicode characters, and we will make a fix available in a software update*".[13] Det tok Apple omtrent 3 måneder å fikse denne buggen, hvor de gav ut en ny versjon av OSet (iOS 8.4).



Figur 8 (Bug-meldingen som ble sendt rundt, hentet fra Huffington Post)

[7] Mørketall for iOS

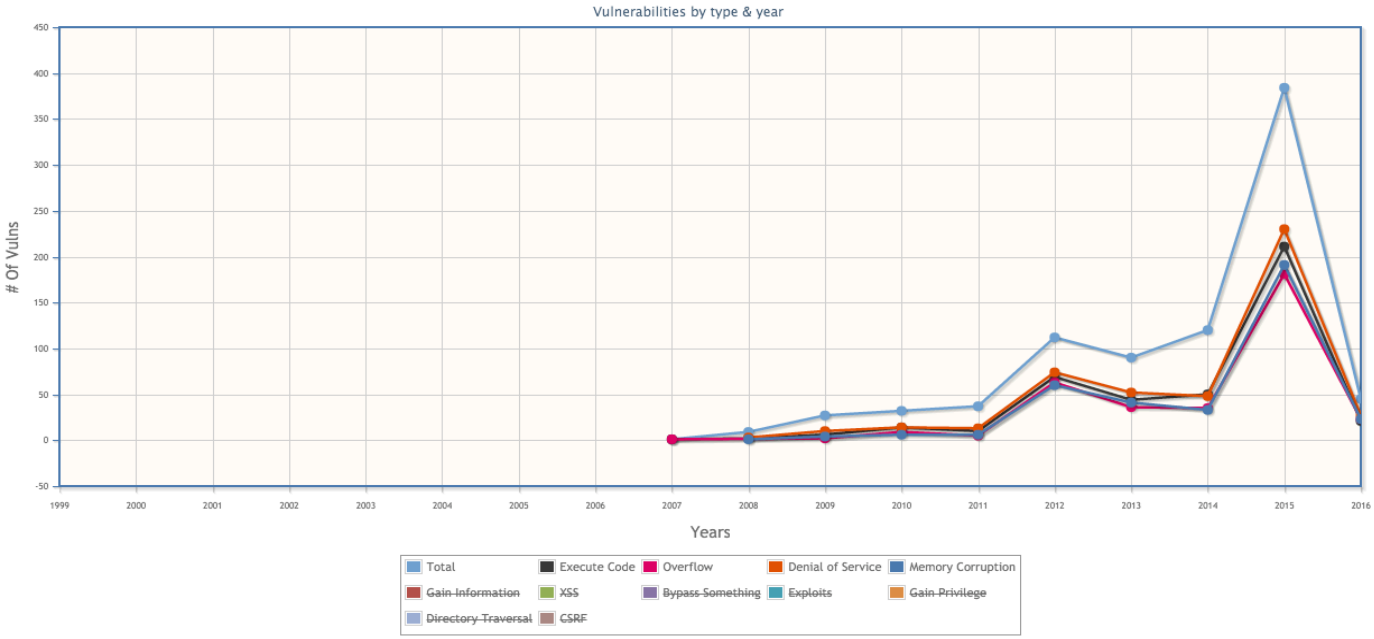


Figur 9 (Statistikk over brudd på iOS og hvilken type, hentet fra National Institue of Standards and Technology)

Grafen ovenfor viser tallene på de meste sårbare områdene ved iOS. Her ser man et jevnt fordelt sektordiagram, hvor det mest utsatte er område er DoS. Tjenestenekt angrep som det kalles, er at man forsøker å gjøre enheten eller nettverk ressursen utilgjengelig for brukeren. Denne typen angrep har også økt i Norge i følge mørketalls-undersøkelsen. Det er fire sårbarheter som man ser er dominante i følge grafen. De tre andre delene som forekommer er "*Execute code*", "*Overflow*" og "*Memory Corruption*". "*Execute code*" vil si at angriperen prøver å manipulere innputt for å forårsake at ufrivillige kommandoer kjøres på

[13] "*This Single Text Message Can Crash Your iPhone*", Ryan Grenoble, *The Huffington Post*

brukeren sin maskin. ”*Overflow”* eller ”*buffer overflow”* er en sårbarhet som forekommer ofte. Denne sårbarheten går ut på at angriperen utnytter programmet som venter på brukeren sin innputt. Det finnes to typer buffer angrep, enten ”*stack-based”* eller ”*Heap-based”*. Begge typene angrep baserer seg ved å belaste beholderne over bruker innputt eller minne satt av til programmer. ”*Stack-based overflow”* er den mest vanlige typen angrep blant disse to. Dette i seg selv er ikke farlig, men dette kan forårsake farer når dette kombineres med ondsinnet kode. ”*Memory Corruption”* er noe som oppstår i et dataprogram når innholdet i et minne område har blitt endret på, som årsak av en program feil. I grafen (se figur 10.) under ser man hvilke typer sårbarheter som har blitt utnyttet i iOSet gjennom årene.



Figur 10 (Statistikk over brudd på iOS og hvilken type, hentet fra National Institue of Standards and Technology)

Gjennom årene ser man en tydelig økning i antall angrep på iOS-enhetene. De totale angrepene fikk en stor økning særlig mellom 2014 og 2015, stigningen tredoblet seg kun på et år. Ser man på de spesifikke angrepene, ser man at antall angrep forekommer med varierte mellomrom. For eksempel så er DoS angrep veldig hyppig i 2012, men i 2013 så synker tallene igjen. Dette gjør utviklingen av sikkerhets komponenter ekstremt vanskelig i henhold til hvilke områder som bør prioriteres. En av hovedgrunnene til at angrepene har blitt tredoblet seg på alle områder, er at antall enheter har steget. Siden Apple er et relativt “nytt selskap” på det mobile markedet, er det forståelig med en pessimistisk angreps vekst i oppstartsårene, men i de seneste årene har veksten blitt større. I 2015 var antall angrep på det høyeste i forhold til de tidligere årene. Et angrep som har påvirket tallene er for eksempel *App store* angrepet.

[8] Infisert App Store?

Figur 11 (The App Store)

I September 2015 ble Apple sin applikasjons butikk angrepet. App store er en nettbasert butikk hvor man kan få tak i applikasjoner til enheten. Angrepet ble utført ved at hackere hadde klart å implementere farlig kode inn i appene. Millioner av brukere skal ha blitt utsatt av dette angrepet, ved enten data tap eller phishing. Angrepet startet i Kina, men utviklet seg sakte utover.
Hvordan dette angrepet ble utført var ved at hackerne hadde klart å lage en kode med onde intensjoner. De hadde klart å implementere koden i en versjon av kode editoren brukt for å lage appene, programmet kalt *Xcode*. Mange utviklere og store selskap hadde tydeligvis klart å bruke denne versjonen og dermed klart å lage apper som var infiserte. De mest utsatte var i Kina, fordi det var raskere å laste ned den modifiserte versjonen i Kina. Det koden utførte var å ta det unike nummeret på enheten, for så å hente annen informasjon om enheten samt brukeren. Malwaren gjorde det også mulig for skaperen å ta kontakt med enheten som hadde blitt infisert. Det vanlige var at hackeren sendte falske varsler, tok over nettleseren eller sende brukeren til skadelige nettsider.

Motivasjonen bak angrepet var hovedsakelig penger. Mange av telefonene er fortsatt knyttet til betalingsmetode, eller har informasjon tilknyttet til bank. Hackerne var ute etter å stjele denne informasjonen og ta pengene til brukerne de hadde angrepet. Derfor mistenkes det at hackerne var fra samme land som hendelsen oppstod. Dette problemet skal ha blitt rettet opp i, kort tid etter hendelsen. "*We've removed the apps from the App Store that we know have been created with this counterfeit software*,". "*We are working with the developers to make sure they're using the proper version of Xcode to rebuild their apps*"[14], sa Apples talskvinne Christine Monaghan i en epost til pressen. Det ble heller ikke utgitt noe ytterligere informasjon på hvordan brukerne kunne finne ut om de hadde blitt infisert. Apple nevnte også at de tar sikkerhet på alvor og at iOS var designet for å være pålitelig og sikkert, fra det øyeblikket man skrur enheten på. Apple ville ikke gi noen tall på hvor mange apper som hadde blitt utsatt, men i følge det kinesiske sikkerhetsfirmaet Qihoo360 skal omtrent 344[15] apper ha blitt påvirket.

Figur 12 (Hacking Apps)

[9] Jailbreaking - iOS' svake punkt?

Figur 13 (Cydia)

Siden starten av iOS har det som oftest vært smutthull (eng: *exploits*) i koden som er blitt produsert. Dette smutthullet har utviklere av jailbreak verktøy alltid klart å trenge seg gjennom, og lagt til sin egen kodebit til den originale koden. Denne koden gir deg tilgang til root-nivå, noe man ellers ikke har. Man kan tenke seg at jailbreaking

[14] Reuters, CNBC
[15] Qihoo360, Reuters, CNBC

er en prosess hvor man installerer et sett med "fikset kode" til kernel-nivået, noe som lar brukeren få tilgang til en "admin" bruker. Dette medfører tilgang til alle filene som man egentlig ikke ville hatt, noe som gir litt mer fleksibilitet til enheten. *Cydia* er en populær "uoffisiell" App store for enheter som har blitt jailbreaket. Det blir ansett som en terminal, for å kunne modifisere(eng: *tweake*) enheten. Skaperen av Cydia er Jay Freeman også kjent som Saurik i jailbreak miljøet. Ved hjelp av Cydia kan brukeren få et hav av alternativer til å tilpasse enheten.

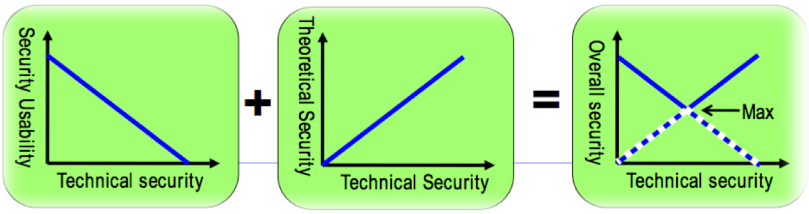
"Jailbreakere" har i de siste årene blitt et større og større samfunn. En av hovedgrunnene til at brukere velger å jailbreake er å bryte ut av de strenge retningslinjene til Apple. Dette i henhold til grensesnitt og generelt frihet til å modifisere. For å gi en liten analogi på hvorfor folk velger å jailbreake, kan man si at for Apple er OSet som en sandkasse. Man kan kun "leke" innenfor sandkassen, men hvis du vil leke utenfor så er jailbreaking det eneste valget du har. Man kan i teorien ikke ha et "perfekt grensesnitt" og høy sikkerhet på samme tid. Dermed får Apple et problem, andre aktører som f. eks Android ikke får. Friheten til å bryte ut og få lov til å bruke iOS til sitt "fulle potensiale", blir fristende for noen brukere.

Figur 14 (Pangu, en utvilker av jailbreak verktøy)

Et motargument for hvorfor man ikke bør jailbreake er at det også kan åpne enheten og utsette vedkommende for potensielle farer. Rot tilgang er en nødvendig del av jailbreakingen-prosessen, men dette kan også åpne "dørene" for farlig angrep. Slik som f. eks at hackeren får tilgang til hele enheten. Selv om det ikke har vært mange rapporterte hendelser på dette er det fortsatt en risiko. Andre ting en bør ta hensyn til ved jailbreaking er at appene eller funksjonene man installerer ikke samhandler med Apple sine retningslinjer. Noen brukere har klaget på at jailbreaking appene ikke "virker" som de vanlige appene. Disse appene kan bruke mer data, telefonen kan bli ustabil og batteritiden kan minke. Man kan også argumentere for å ikke jailbreake, ved å si at Apple utvikler grensesnittet i den retningen brukerne vil ha det. Slik som å endre bakgrunn, multitasking funksjonen eller bedre varslingssystem. Disse endringene hos Apple kan man også si at jailbreaking er årsaken til. Apple implementerte dette inn i systemet deres etter at jailbreaking hadde kommet med disse spesifikasjonene. Dette blir et slags paradoks, i forhold til om man trenger jailbreaking eller ikke. Dette leder i positiv retning, men negativt i seg selv.

Problemene Apple møter på med jailbreaking er massive. Alt fra gratis betalt-apper, til muligheten å hacke andre iOS enheter. Løsningen fra Apples side er at brukeren mister garantien på produktet. Dette har med årene vist seg å være en mindre effektiv metode. Man kan i dag si at Apple har et lite overtak ovenfor jailbreakerne, siden de bestemte seg for å tette smutthullene med hyppigere oppdateringer. Før pleide en jailbreak-oppdateringene å bli lansert rett etter at den nye versjonen av OSet var ute, noen ganger ble det til og med

lansert før. I dag bruker jailbreak utviklerne litt lenger tid. Det kan ta et par måneder etter at den nye jailbreak oppdateringen er ute. Den negative siden ved at Apple gir brukeren oftere oppdateringer er at OSet blir tregere for hver oppdatering. Hvilket som impliserer misfornøyde brukere. Den positive virkningen er at brukerne får et system som er tettet igjen for de seneste sikkerhetshullene, samt en ikke-jailbreakbar versjon.



Figur 15 Usabillity vs security (Figur fra forelesing 2)

[10] Apple vs. FBI, et farlig skille?

Et av de mest oppsiktsvekkende iOS relaterte sakene de siste årene er den såkalte Apple vs. FBI (*Federal Bureau of Investigation*). Denne saken gikk i hovedsak ut på at FBI prøvde å få Apple til å lage en "nøkkel" eller en slags "bakdør" for å kunne åpne en vilkårlig iPhone ,uten at det skulle bli noen komplikasjoner. Grunnen til at FBI ville ha denne tilgangen var at det nylig hadde vært et terrorangrep i USA. Terroristen med navn Syed Rizwan Farook og hans kone Tashfeen Malik hadde skutt 14 personer og skadd 21 andre i California. Grunnen til at FBI var ute etter mobilen til Syed, er fordi de mente han hadde en tilknytning til ISIS (*Islamic State of Iraq and Syria*). Syed eide en iPhone 5C, som er en enhet uten Touch ID funksjonen. Siden denne telefonen ikke hadde denne funksjonen ,var det ikke like lett for FBI å komme seg inn på iPhonen til Syed. OS versjonen denne telefonen hadde bruker en " auto-slett funksjon", som også brukes i den siste versjonen av OSet i dag. Denne "auto-slett funksjonen" vil med andre ord slette alt innhold på enheten automatisk, etter 10 pin kode forsøk.

Apple valgte og ikke lage en bakdør, fordi dette krenker sikkerheten og personvernet til brukerne deres. "*We have done everything that is both within our power and within the law to help, but now the U.S. government has asked us for something we simply do not have, and something we consider too dangerous to create.*", sa Tim Cook i Apple sitt *Customer Letter* som ble utgitt den 13. februar 2016.[16] Siden Apple ikke ville lage en bakødr de vet kunne skade mange, valgte FBI dermed å bruke et eksternt firma for å komme inn på iPhonen. Dette prosjektet kostet FBI totalt 1,3 millioner dollar, men ga ingen resultater. Det viste seg at det ikke var noen spor etter tilknyttinger mellom Sayed og ISIS. Denne hendelsen kunne enkelt ledet til en veldig kompleks situasjon, dersom Apple hadde valgt å skape en "bakdør". Dette kunne skapt et problem ved at flere sitter på en "nøkkel" til alle Apple enheter, som gjør at Apples utsagn om et sikkert system blir kontradiktorisk. Ville det vært etisk riktig å svekke OSet for å kunne få tilgang til enhver iPhone? Med andre ord svekke sikkerheten, for å gjøre verden "tryggere"?.

[16] "*A Message to Our Customers*", Tim Cook

Grunnen til at FBI saken har fått så mye medieoppmerksomhet er konsekvensene det kunne medført. Hvis forespørselen fra FBI hadde blitt innvilget, ville andre land krevd noe lignende. Dette motsier hele moralen ved personvern (*eng: privacy*).
Det å svekke personvernet til alle brukere, for å "fange" én delmengde kriminelle er paradoksalt. Edward Snowden, tidligere NSA (*National Security Agency*) har uttalt følgene om saken:

Figur 16 (Apple vs FBI)

" We've got this private product out there on the market, which is designed to protect the security of all customers, not some. This is a binary choice. Either all of us have security or non of us have security". [17]

Et annet problem som kunne oppstått, er økt antall angrep. Det å anta at IT verden kun består av gode intensjoner er idealistisk, men langt i fra realiteten. I følge mørketall rapporten er 44,8% alle virus spredninger gjort av brukeren. Et svekket system vil kun invitere hackere med onde intensjoner inn i system, og tilby en lettere hverdag. FBI har i realiteten sterke ressurser i henhold til saken. Det å dekryptere et passord på 10 karakterer (eng: digits), kan ta opp mot 250 år. Ved å lage en bakdør, med andre ord å svekke krypteringslaget (eng: encryption) på iOS, blir jobben "lettere" for FBI. Spørsmålet mange stiller seg er, hvorfor skal systemet som helhet bli svekket? Sannheten er at hele forslaget vil medføre flere konsekvenser, enn å være til hjelp. Apple sa at folk generelt i verden fortjener data beskyttelse, sikkerhet og at informasjonen deres er privat.

"***Sacrificing one for the other only puts people and countries at greater risk***."[18]
- Apple

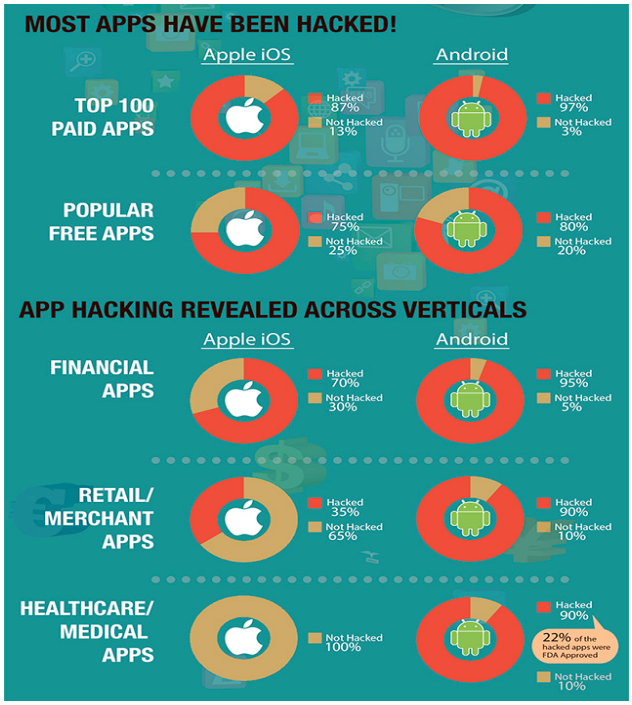
[11] Android vs. iOS - Frihet eller sikkerhet ?

Et av de største aktørene på den mobile plattformen er operativsystemet Android. Antall Android enheter på verdens basis er 82,8% (2 kvartal, *IDC*), dette går over flere selskaper blant annet Samsung, LG, Sony og Google. Til tross for en overlegen dominans på det mobile markedet, blir Apple sett på som et sikkerhets orientert produkt. En av årsakene til dette er antall ondsinnede applikasjoner på deres distribusjonsplattformen Android Market[19].
Tilnærmet lik hvem som helst, kan laste opp en applikasjon på Android. Dette i samspill med et mer sikkerhetsmessig "åpent" operativsystem impliserer sårbarhet. Med andre ord, bruker ikke Android et *sandbox*-system.

[17] "*Edward Snowden Interview on Apple vs. FBI, Privacy, the NSA, and More*", TheReason
[18] "*FBI says it has cracked terrorist's iPhone without Apple's help*", CNN Money
[19] Android market = noe alá App store.

Antall ondsinnede applikasjoner på iOS er nærmest neglisjerbart i forhold til Android. Dette impliserer ikke at iOS er ugjennomtrengelig, men opplagt mer robust. Det finnes flere grunner til dette, blant annet iOS *sandbox* og krypterings teknologien. I tillegg må utvikleren bli godkjent av Apple. Hvis utvikleren på et eller annet tidspunkt prøver å laste opp en infisert applikasjon, vil utvikleren bli kastet ut eller blokkert av Apple. Tredjeparts applikasjoner, kan heller ikke bli installert på de nyere iOS-enhetene, noe som kan gjøres på Android. Dette er et av grunnene til at Android opplever flere angrep enn Apple. På Android kan man laste ned applikasjoner, via f. eks nettleseren, noe som er umulig på én iOS-enhet. Tatt i betraktning at enheten ikke er jailbreaket.

Android er ansett som et mer utviklervennlig operativsystem, i henhold til utvikling av apper og brukergrensesnitt modifisering. Friheten gjør at brukerne fritt kan eksperimentere på måter iOS ikke kan. På den andre siden, blir Apple ansett som et mer sikkerhets orientert selskap. I lanseringen av iOS 9, ble sikkerhet et av hovedtemaene i presentasjonen av det nye OSet. I bunn og grunn koker diskusjonen ned til om man skal ha et ”open source” (nor: åpen kildekode) eller ”close source” (nor: lukket kildekode). Det finnes sterke argumenter på begge sider, men med et ”close source-system” blir antall angrep redusert betraktelig.



Figur 17 (Apple vs. Android angreps statistikk)

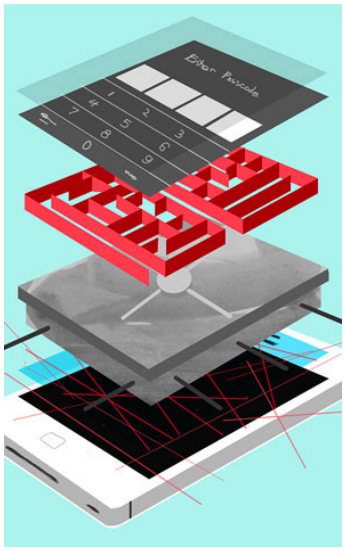
[12] Dagens situasjon

Hvorfor er det viktig med god mobil sikkerhet? Mobilen ble i hovedsak ansett å være en enhet for å ringe og sende tekstmeldinger. Siden den gang har mobilen utviklet seg til noe langt mer intrikat. For eksempel har tokens, bankkort og billetter fått et alternativ på de mobile plattformene. Apple har i de seneste årene satset på teknologi som erstatter fysiske verifikasjoner, blant annet ”*Apple pay*”[20], ”*wallet*”[21] etc. Med andre ord, jobber Apple mot en fremtid hvor teknologier integreres med hverandre, dette impliserer viktigheten ved god sikkerhet. Foruten kan sensitiv informasjon lett komme på avveie og konsekvensen kan bli større enn før.

Siden den første lanseringen av første iPhonen, har det blitt funnet en rekke alvorlige sikkerhetshull. En av hovedårsakene til at disse blir funnet i første omgang er brukerne. Hyppige tilbakemeldinger, samt mye medieoppmerksomhet rundt feilene, gir slutt produktet

[20] Apple pay = en måte å erstatte bankkort, bruker mobilen som et bankkort
[21] Apple wallet = en app som holder på informasjon om diverse kort (bank-, fly-, kredit-, kunde-, boardingkort osv.)

et relativt høyt sikkerhetsnivå. Dette går selvfølgelig på bekostning av selskapets rykte og omdømme. Gjennom årene har sikkerheten til iOS blitt sterkere, men i likhet har også hackere blitt smartere. Trusselbilde til iOS er vanskelig å forutsi, spesielt med tanke på variasjonen av angrepene. Mobil teknologien utvikler seg i rekordfart, dette er uten tvil et dilemma som kan forekomme i fremtiden for Apple ved utviklingen.



Figur 18 (illustrasjon av sikkerhets lagene til en iOS enhet)

Apples iOS bruker som nevnt et close-source system, men de lar utviklere få tilgang til beta-versjonene av de kommende OS oppdateringene. Dette gir beta-testerne tilgang til kildekoden, som igjen gjør det mulig å tilpasse applikasjoner til den nye versjonen. Dette blir brukt som en metode for å finne nye veier å jailbreake telefonen. Hvis Apple velger å fjerne denne mulighet for å minke sannsynligheten av jailbreaking, kan dette være slutten på jailbreaking. En av de store konsekvensene Apple kan få er den store mengden utviklere som vil slite.

Et annet viktig aspekt i sikkerhets debatten er personlig informasjon. iOS tilbyr en helse-app, som inneholder muligheten å lagre helse informasjon på enheten. For eksempel kan man lagre blodtype, eventuelle allergier etc. Hvis informasjonen kommer på avveie, kan dataen i verste implikasjon lede til fatale hendelser. Det er dermed essensielt å vurdere om iOS klarer å takle å holde på slik informasjon. Siden det meste av vår sensitive informasjon blir digitalisert eller nærmere bestemt kompatibelt på mobil. Må Apple vurdere om de har kapasitet til å opprettholde et høyt sikkerhetsnivå på samtlige av deres enheter. Per dags dato har det ikke blitt gjort angrep på helse applikasjoner (se figur 17), men dette må på ingen måte bli en selvfølge. Med tanke på variasjonen angrep som har blitt utført på iOS, er kanskje helse-appen det neste store målet. Diskusjonen koker ned til et punkt, nemlig hvor mye sensitiv informasjon man kan få lagret på enheten før det blir risikabelt.

Angreps strategiene som blir valgt for å få tak i sensitiv informasjon er hovedsakelig ikke dirkete angrep på iOS. Oppbygningen i seg selv reflekterer et robust system, men det er brukerne som er "det svake leddet". Sosial manipulering *(eng: social engnieering)* angrep, som heller bygger på menneskelige faktorer er vanskeligere for Apple å håndtere. De fleste av angrepene som har fått mye oppmerksomhet hos media, kommer under denne kategorien. Mindre sikkerhets mekanismer kan bli innført, men en viss mengde kontroll vil alltid ligge i brukerens hender. Et robust system vil alltid være utsatt når personen med nøkkelen kan bli lurt.

"The biggest threat to the security of a company is not a computer virus, an unpatched hole in a program, or a badly installed firewall. In fact the biggest threat could be you."[22]

– Kevin Mitnick

[22] Lecture 2, slide 38, "*Human Factors for Information Security*", Prof. Audun Jøsang

Konklusjon

Siden 2011 har antall solgte Apple enheter økt i rekord fart. Sensitiv informasjon blir stadig lagret, men vi kan ikke anslå at iOS er ugjennomtrengelig. Vi får stadig høre om sikkerhetshull og angrep. Utfordringene Apple har i fremtiden, er vanskelig å forutsi. De fleste store angrep som har fått medieoppmerksomhet har heller vært Sosial manipulering, fremfor sikkerhets-angrep på det fysiske systemet. iOS har innført en rekke midler, for å sikre at telefonen ikke blir brukt av uautoriserte personer, deriblant Touch ID, iCloud og FindMyIphone. Problematikken ligger i hvordan Apple skal håndtere angrep, som er rettet direkte mot brukerne. Det som åpenbart har vist resulterer er å bruke et ”close-source” system. Dette har minket antall angrep mot system betraktelig, hvertfall sammenlignet med en av hoved konkurrentene Android.

Om Apples iOS er det “beste” mobile operativsystem kan diskuteres, med fokus på sikkerhet. Det er utfordrende å drøfte med tanke på hvor komplekst iOS har blitt, i forhold til første lansering. En stor mengde ny teknologi har blitt introdusert, og faktum er at iOS er i ferd med å bli en slags ”nøkkel” for alle hverdagens aspekter. Det kritiske spørsmålet er hvor mye kan lagres på en liten enhet, før det blir for mye. Svaret kan kun fremtiden vise.

Med årene har Apple utviklet et robust system, hvert fall med tanke på historien til iOS. I dag så er sikkerhetsnivået bra i forhold til andre aktører, men det er ikke ugjennomtrengelig. Dette ble nylig bevist i FBI saken, hvor en iPhone nylig ble låst opp. Så holder iOS egentlig mål? I forhold til dagens teknologi, ja, men med et langsiktig syn er det vanskelig å vurdere. Sikkerhet er et relativt begrep, så å konstatere at iOS har god sikkerhet for alltid er umulig.

> ***“The only truly secure system is one that is powered off”***
> - Gene Spafford

Referanser:

[0] Tim Cook, ”Apple’s commitment to your privacy” , **Introduksjon**
<http://www.apple.com/privacy/ >
[Lesedato 03.05.16]

[1] Dieter Bohn, Aaron Souppouris, and Dan Seifert, Verge Staff , **Oppbyging av OS**
”iOS: A visual history”,
<http://www.theverge.com/2011/12/13/2612736/ios-history-iphone-ipad>
[Lesedato 04.04.16]

[2] Prof. Audun Jøsang, “*Lecture 06: - Computer security*” , **Sikkerhetskomponenter**
<http://www.uio.no/studier/emner/matnat/ifi/INF3510/v16/lectures/inf3510-2016-l06-compsec.pdf> [Hentet 14.04.16]

[2, 3, 5] Apple, iOS Security - White Paper, **Sikkerhetskomponenter, Nettverksikkerhet og iCloud og iMessage**
“*iOS Security iOS 9.0 or later*”
”<https://www.apple.com/business/docs/iOS_Security_Guide.pdf>
[Lesedato 03.04.16]

[3] iCloud Design Guide, Apple, figur 3, **Nettverksikkerhet og iCloud**
<https://developer.apple.com/library/ios/documentation/General/Conceptual/iCloudDesignGuide/Chapters/iCloudFundametals.html> [Lesedato 01.05.16]

[3] Dave Lewis, The Forbes, **Nettverksikkerhet og iCloud**
“*DDoS Attacks Continue To Rise*”,
<http://www.forbes.com/sites/davelewis/2015/01/29/ddos-attacks-continue-to-rise/#5e76c9624b7f> [Lesedato 23.03.16]

[3] Næringslivets Sikkerhetsråd, “*Mørketall 2014* “, **Nettverksikkerhet og iCloud**
<http://www.nsr-org.no/getfile.php/Dokumenter/NSR%20publikasjoner/M%C3%B8rketallsunders%C3%B8kelsen/M%C3%B8rketall_2014_WEB.pdf> [Lesedato 01.04.16]

[4] Prof. Audun Jøsang, “*Lecture 04: - Cryptography”* **iCloud - Hull i skyen**
<http://www.uio.no/studier/emner/matnat/ifi/INF3510/v16/lectures/inf3510-2016-l04-crypto.pdf> [Hentet 05.05.16]

[4] Tim Cook, ”Data security” **, iCloud - Hull i skyen**
<https://support.apple.com/en-us/HT202303> [05.05.16]

[4] Riley Walters, The Davis Institute for National Security and Foreign Policy at The **Heritage Foundation** , **iCloud** - **Hull i skyen**
"*Cyber Attacks on U.S. Companies in 2014*"
<http://thf_media.s3.amazonaws.com/2014/pdf/IB4289.pdf>
[Lesedato 07.04.16]

[4] Charles Arthur, The Guardian , **iCloud - Hull i skyen**
"*Naked celebrity hack: security experts focus on iCloud backup theory*"
<https://www.theguardian.com/technology/2014/sep/01/naked-celebrity-hack-icloud-backup-jennifer-lawrence> [Lesedato 27.04.16]

[4] Associated Press, The Guardian
"Apple warns of new iCloud threat"
<https://www.theguardian.com/technology/2014/oct/22/apple-warns-of-new-icloud-threat> [Lesedato 27.04.16]

[6] Ryan Grenoble, The Huffington Post, **Liten melding, store konsekvenser**
"This Single Text Message Can Crash Your iPhone"
<http://www.huffingtonpost.com/2015/05/27/text-message-crash-iphone-_n_7452324.html> [Lesedato 05.05.16]

[6] Apple, **Liten melding, store konsekvenser**
"Apple security updates"
<https://support.apple.com/en-us/HT201222> [Lesedato 05.05.16]

[7] Data from National Institue of Standards and Technology, figur 5 og 6, **Mørketall for iOS**
"*Apple Iphone OS : Vulnerability Statistics*"
<https://www.cvedetails.com/product/15556/Apple-Iphone-Os.html?vendor_id=49>
[Lesedato 26.04.16]

[8] Brian Posey, Techtarget, **Infisert app store**
"*How do buffer overflow attacks work?*"
<http://searchsecurity.techtarget.com/news/1048483/Buffer-overflow-attacks-How-do-they-work> [Lesedato 19.04.16]

[8] Reuters (With CNBC contributed content) , CNBC , **Infisert app store**
"*Apple's iOS App Store suffers first major attack*"
<http://www.cnbc.com/2015/09/20/apples-ios-app-store-suffers-first-major-attack.html> [Lesedato 07.04.16]

[8] Mark Ward, BBC **Infisert App Store**
"*Apple App Store attack - are you safe?*"
<http://www.bbc.com/news/technology-34312692> [Lesedato 07.04.16]

[10] Tim Cook, Apple, **Apple vs FBI**
"*A message to our customers*",FBI sak
<http://www.apple.com/customer-letter/> [Lesedato 01.05.16]

[10] Samuell Gibson, The Guardian, **Apple vs FBI**
"*Snowden: FBI's claim it can't unlock the San Bernardino iPhone is 'bullshit'*"
<https://www.theguardian.com/technology/2016/mar/09/edward-snowden-fbi-san-bernardino-iphone-bullshit-nsa-apple> [Lesedato 26.05.16]

[10] Common Cause Blueprint for a Great Democracy conference, TheReason, **Apple vs FBI**
"*Edward Snowden Interview on Apple vs. FBI, Privacy, the NSA, and More*",
<https://www.youtube.com/watch?v=o8pkUTav0mk> (fra 1:28 min)
[Lesedato 01.05.16]

[10] Evan Perez, Pamela Brown and Shimon Prokupecz, CNN, **Apple vs FBI**
"Sources: Data from San Bernardino phone has helped in probe"
<http://edition.cnn.com/2016/04/19/politics/san-bernadino-iphone-data/index.html> [Lesedato 01.05.16]

[10] Sam Thielman , The Guardian, **Apple vs FBI**
"*Apple v the FBI: what's the beef, how did we get here and what's at stake*?"
<https://www.theguardian.com/technology/2016/feb/20/apple-fbi-iphone-explainer-san-bernardino> [Lesedato 18.04.16]

[11] "*When Malware Goes Mobile*", Sophos LTD, **Android vs iOS - Frihet eller sikkerhet ?**
<https://www.sophos.com/en-us/security-news-trends/security-trends/malware-goes-mobile/why-ios-is-safer-than-android.aspx> [Lesedato 24.04.16]

[11] Ian Barker, Betanews, figur 13, **Android vs iOS - Frihet eller sikkerhet ?**
"87 percent of the top 100 paid iOS apps available as hacked versions"
<http://betanews.com/2014/11/17/87-percent-of-the-top-100-paid-ios-apps-available-as-hacked-versions/> [Lesedato 21.04.16]

[11] Ramon Llamas, Ryan Reith & Kathy Nagamine, IDC, **Android vs iOS - Frihet eller sikkerhet ?**
"Smartphone OS Market Share, 2015 Q2"
<http://www.idc.com/prodserv/smartphone-os-market-share.jsp>
[Lesedato 02.05.16]

[12] Prof. Audun Jøsang, "*Lecture 02: - Information Security Management - Human Factors for Information" Security*", **Dagens situasjon**
<http://www.uio.no/studier/emner/matnat/ifi/INF3510/v16/lectures/inf3510-2016-l02-isman-humfact.pdf> [hentet 01.05.16]

E-BOK:
[9] Forfattere: Charlie Miller & Dion Blazakis & Dino DaiZovi & Stefan Esser & Vincenzo Iozzo & Ralf-Philip Weinmann
(2012). iOS Hacker's Handbook [Lokalisert på Google]. **Jailbreak - iOS' svakepunkt?**
Kap: "*Jailbreaking*" (s.297) og "*Understanding the Jailbreak process*" (s.301)
Hentet fra:
<https://books.google.no/books?hl=no&lr=&id=1kDcjKcz9GwC&oi=fnd&pg=PR17&dq=Jailbreaking+iOS&ots=9LeEvBEg_q&sig=Z_8OHmKppN0QH1qfcGUCrD8lOHY&redir_esc=y#v=onepage&q=Jailbreaking%20iOS&f=false>