Универзитет у Крагујевцу
Факултет инжењерских наука

Семинарски рад из предмета
Заштита података (Теорија криптовања)

Тема:
Заштита података на Apple уређајима новије генерације

Студент:
Ива Којић 577/2016

Предметни професор:
Др Владимир Миловановић

Крагујевац 2020.

Садржај

Apple A11 Bionic чип

Apple A11 Bionic представља први тзв. SoC (System on a chip) интерно дизајниран GPU укључујући три језгра која имају исте перформансе као претходни PowerVR GT7600 коришћен у претходним моделима, али са 50% мањим коришћењем енергије. Овај чип такође представља први чип који у себи садржи NPU(Neural Processing Unit) који омогућава развитак бољих начина заштите података као што је Face ID.

Слика 1 Спољашњи изглед чипа

Дизајн чипа

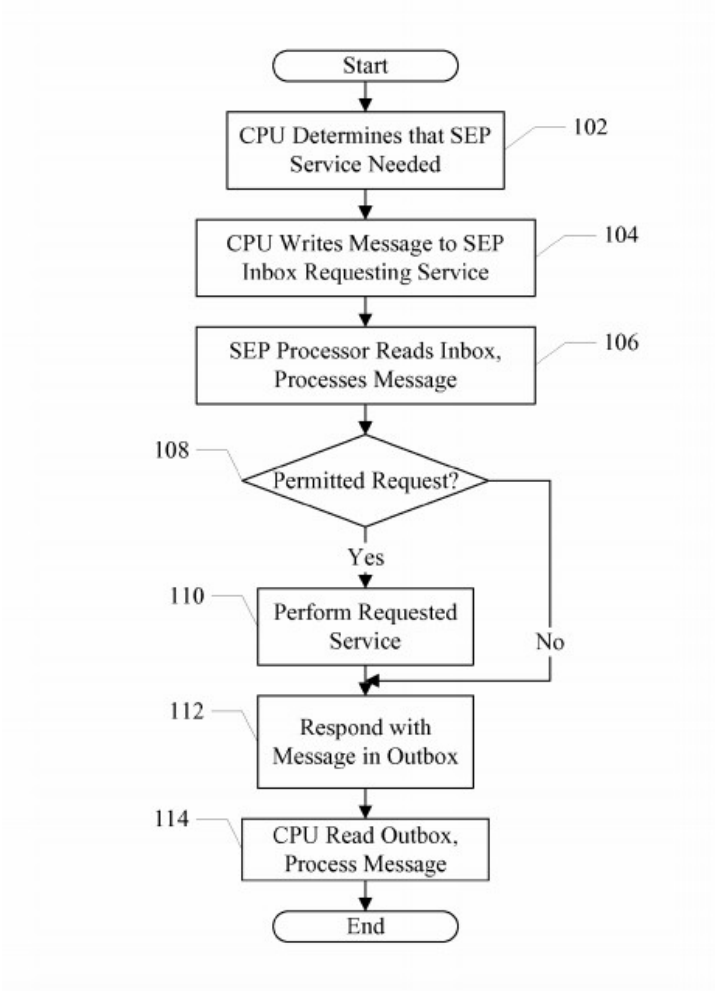
A11 чип је дизајниран од стране Apple Inc. Представља 64-битну ARMv8 архитектуру, са 6 језгара, од којих су два чипа виских перформанси до 2.39 GHz и четири енергетски-ефикасна језгра. Они се респективно наивају Монсун и Мистрал. Монсун језгра имају суперскаларну архитектуру „без реда'' са декодером ширине 7, док Мистрал језгра имају ширину 3, такође суперскалар и ‚без реда'', и базирани су на језгрима из претходника овог чипа тј. Apple A6. Bionic се највероватније односити на Neural Engine или The Neural Processing Unit (NPU), која представља уграђену хардвер за неуронску мрежу која умногоме олакшава сложене задатке везане за машинско учење. Ова компонента може обављати до 600 билиона операција у секунди, што представља велики корак у развоју Apple уређаја.

Овај чип у себи садржи 4.3 милиона транзистора, Монсун чипови су 25% су бржи од претхоника A10, а четири са високом ефикасношћу су чак 70% бржи од A10. Оно што заправо највише побољшава перфомансе овог чипа је друга генерација контролера који има 70% бољу ефикасност и може користити свих 6 језгара одједном.

Слика 2 Унитрашњи изглед чипа

Secure Enclave

Secure Enclave је хардверски заснован менаџер кључева који се користи за складиштење кључеве за шифровање, Touch ID и Face ID. Сигурна енклава ради на специфичном процесору назван Secure Enclave Processor (SEP), који је одвојен од CPU-а. Комуникација између CPU-а і SEP-а је строго контролисан на хардверском нивоу, спречавајући злонамерно узимање критичних информација од стране апликације. Secure Enclave користи Apple Pay за плаћања, као Touch ID или Face ID.SE је сигуран копроцесор је изолован од главног процесора да би пружио додатни ниво заштите. Secure Enclave је хардверска карактеристика одређених верзија iPhone, iPad, Mac, Apple TV, Apple Watch и HomePod. У телефонима се налази од 5C верзије. Кључни подаци су шифровани у систему Secure Enclave на чипу (SoC), који укључује генератор случајних бројева. Сигурна енклава такође одржава интегритет својих криптографских операција, чак и ако је кернел угрожен. Комуникација између Secure Enclave и процесора апликације строго се контролише тако што се комуникација врши само преко ,,поштанског сандучета'' које управља прекидима и баферима заједничке меморије.



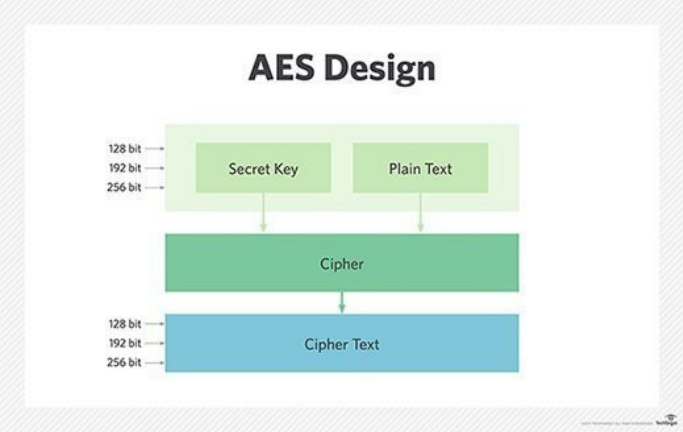
Слика 3 Дијаграм тока који илуструје реализацију једне поруке која пролази кроз пријемно/излазно сандуче

Сигурносна енклава има наменски Boot ROM сличан оном апликационом процесору. Тај Boot ROM иницијализује ефемерни кључ, који укључује UID уређаја и бројач против поновног покретања, током покретања уређаја. Кључ се користи за шифровање меморијског дела који користи сигурносна енклава. Услуге против поновног репродуковања неопходне су за опозив података у неким догађајима као што су промена лозинке, промена TouchID-а или FaceID-а, промена Apple Pay-а итд. Сигурна енклава је такође посвећена руковању обрадом података везаних за TouchID и FaceID. Ово осигурава да осетљиве биометријске информације остану у сигурносној енклави и да их не може прочитати ниједан други део уређаја, укључујући сам оперативни систем.

Шифровање и енкрипција података

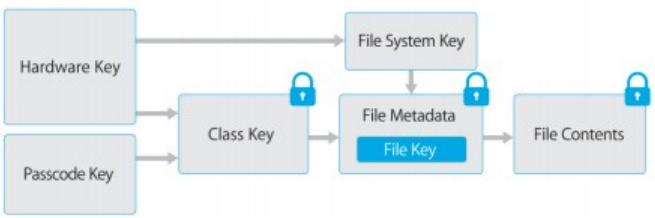
Шифровање и дешифровање података су ефикасни коришћењем наменског хардвера названог AEC-256.То представља криптомеханизам који се налази на магистрали између главне меморије и флеш меморије. Овај дизајн такође осигурава да се подаци увек шифрују пре него што се

упишу у меморију. UID и GID уређаја користе се као кључеви AEC-256. Они су створени током производње и читљиви су само AEC-у. Као резултат, само уређај који енкриптује податке може да их дешифрује, па чак и ако је меморија физички уклоњена и постављена на друге уређаје, они не могу да читају податке.



Слика 4 Дизајн AEC-256 криптомеханизма

Заштита података користи **хијерархију кључева** (која се назива и умотавање кључева) за шифровање датотека на уређају. Тачније, свака датотека је шифрована јединственим тајним кључем, *kf*. Кључеви датотека су шифровани од главног системског кључа, *ke*, и кључем класе, *kc*. Тек када је испуњен услов класе и системски кључ је доступан, кључеви датотека могу се дешифровати, а затим користити за дешифровање датотека. Кључеви класе су повезани са околностима у којима се уређај се налази. На пример, одбацује се класа *Complete Protection*, најсигурнија класа, одбацује кључ за дешифровање након што се уређај закључа, али класа *Protected Unless Open* омогућава континуирани приступ датотеци чак и након закључавања уређаја. Дозвољене класе су повезане са сваком датотеком и садржане су у метаподацима датотеке шифроване системским кључем. Слика 5 резимира хијерархију кључева.

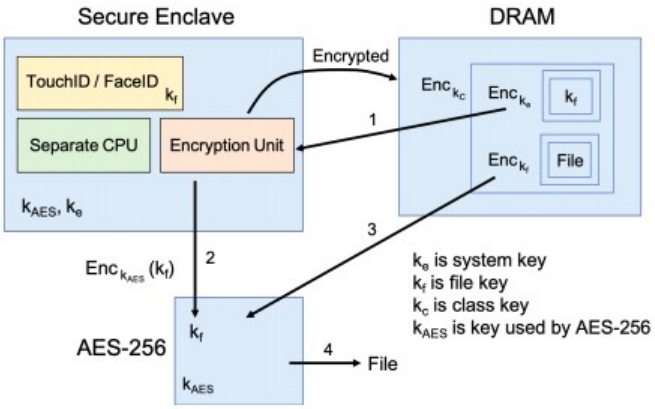


Слика 5 Хијерархија кључева

Дешифровање датотека се врши на следећи начин:.
Системски кључ (*ke*) чува се у сигурној енклави. На високом нивоу, подаци
поступак дешифровања је приказан у корацима од 1 до 4 на слици, под претпоставком да је кључ класе откључан.

Кораци 1 до 4 су следећи:
1. Сигурна енклава преузима и дешифрује *kf* користећи *ke* које има.
2. Сигурна енклава шифрира *kf* помоћу *kAES* и шаље га на *AES-256*.
3. Датотека шифрована помоћу *kf* се такође шаље на *AES-256*.
4. *AES-256* дешифрује *kf* из сигурносне енклаве користећи свој *kAES*. Затим користи *kf* за дешифровање датотеке.

У овом тренутку, неко би се могао запитати зашто систем не користи само један главни кључ, тј. системски кључ за шифровање свих датотека. Главни разлог је тај што ће, ако је један кључ датотеке угрожен, потенцијални хакер бити у стању да прочита само једну датотеку шифровану тим кључем, али не и било коју другу датотеку на уређају.
Поред тога, постојање хијерархије кључева такође поједностављује прецизно управљање кључевима и опозив кључа.

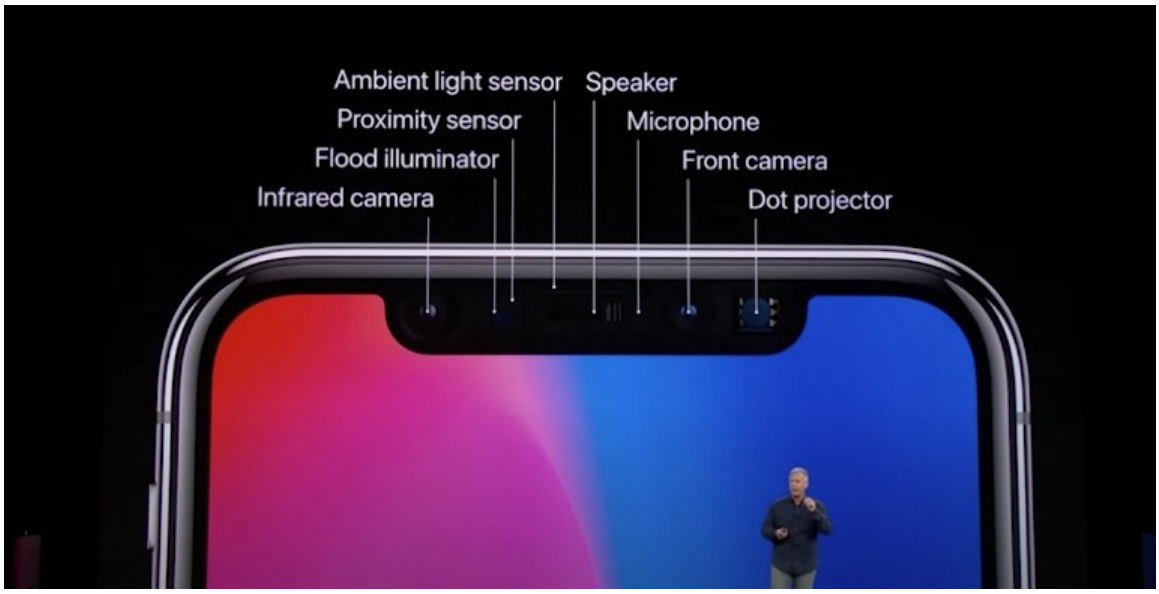


Слика 6 Дешифровање датотека

Face ID

iOS штити корисничке податке користећи хардверско шифровање. При покретању, кључ за дешифровање је доступан само ако корисник унесе исправну шифру (познатију и као ПИН). Уметање није успело исправна лозинка неколико пута резултира онемогућавањем аутентификације. Након покретања, iOS нуди лакше начине аутентификације, укључујући и отисак прста као потврда идентитета, названа Touch ID, а у новије време и препознавање лица под називом Face ID, који је уведен са iPhone X.

Face ID представља технологију препознавања лица. Технологија замењује Touch ID, систем за скенирање отиска прста, који се спомиње у каснијим поглављима.Face ID користи нешто што су творци у Apple-у назвали **„TrueDepth camera system“,** који се састоји од сензора, камера и тачкастих пројектора на врху екрана у за стварање детаљне 3D мапе лица. Сваки пут када корисник погледа телефон, систем ће извршити сигурну проверу, омогућавајући откључавање уређаја или брзу и интуитивну ауторизацију плаћања ако препозна корисника.

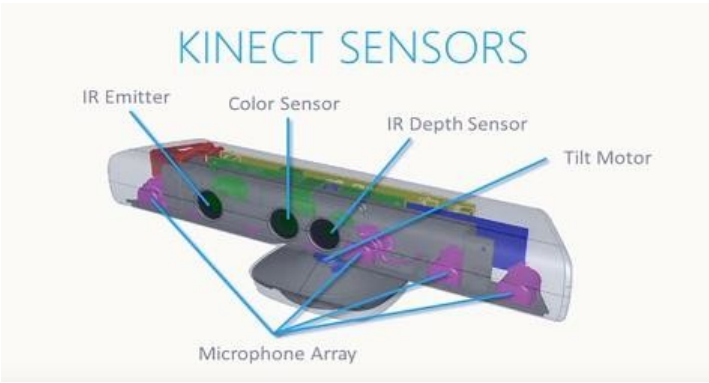


Слика 7 Компоненте „TrueDepth camera system“

Како функционише Face ID?

TrueDepth започиње традиционалном 7MP предњом „selfie“ камером. Додаје инфрацрвени емитер који на лице корисника пројектује преко 30 000 тачака. Те тачке се затим фотографишу помоћу наменске инфрацрвене камере за анализу. Постоји сензор близине, тако да систем зна када је корисник довољно близу да се активира. Сензор амбијенталног осветљења помаже систему да подеси ниво излазне светлости.
Apple такође позива Flood Illuminator који при слабом осветљењу допуњује IR слике и служи да помогне систему да добије слику лица корисника која допуњује мапу дубине. IR такође добро детектује подповршинске карактеристике коже, што онемогућава кориснику да „завара’’ систем ставивши маску за лице.
Да би се одолео дигиталним и физичким малверзацијама и покушајима искоришћавања корисничких података, камера насумично одабире редослед 2Д слика и мапа дубине и пројектује случајни узорак специфичан за уређај. Део НПУ-а трансформише ове податке у математички приказ и упоређује тај приказ са уписаним подацима који се већ налазе на сигурносној енклави. Ови уписани подаци о лицу сами су по себи математички приказ лица корисника забележеног у различитим позама.Овом приликом се чува само математички приказ лица корисника, што значи да се ни позадина не складишти.

Ово је исти тип система који користи оригинална верзија Microsoft-овог Kinect-а, који је у то време био широко хваљен због његове тачности. Претпоставља се да је Apple искористио структурални сензор светлости за развијање фацијалног препознавања. Наиме, овај сензор је развијен од стране компаније PrimeSense за оригинални Kinect 2010. а ова компанија је купљена од стране Apple компаније у 2013. Ова врста система добро функционише, али су обично потребни велики, моћни емитери и сензори.



Слика 8 Компоненте оригиналног Microsoft Kinect-а

Функција откривања пажње

Apple корпорација је уочила неке појединости при коришћењу овог новог начина заштите података. Примећује се да постоје неки људи којима функција „пажње“ неће одговарати. То би, на пример, били слабовиди људи или људи са делимично или потпуно оштећеним видом. Такви корисници не могу саопштили своју намеру тако што ће гледати у телефон. У тим случајевима, када се лице препозна (чак и са наочарима за сунце), али не виде очи, постоји опција искључења „откривања пажње“. И даље ће корисник моћи несметано да користи Face ID, али на нижем нивоу свеукупне сигурности.

Заштита корисничких података на правној основи

Највећи број корисника који сумњају на малверазцију поентирају да може доћи до давања њихових личних података властима. Одговор Apple-а је да они заправо немају приступ овим подацима. Наиме, Apple никада не преузима податке, анонимно или на било који други начин. Када обучите податке, они се одмах чувају у сигурносној енклави као математички модел који се не може реконструисати натраг у „модел лица“. Било која преквалификација(мењање постојећих математичких модела итд.) се такође тамо дешава. Лични подаци корисника се налазе на самом уређају, а не на серверу или у облаку. Једини начин до код може доћи до искоришћавања је уколико треће лице има физички приступ уређају. Међутим, и ту би било потешкоћа собзиром да су подаци криптовани, што је обрађено у претходном поглављу.

Подаци Face ID-а једино када напуштају сигурносну енклаву је ако би се слали за AppleCare техничку подршку уз пристанак корисника. Дозвољено је да корисник прегледа и одобри податке који се шаљу, укључујући слику лица тј математички модел. Ови подаци се аутоматски бришу након 90 дана.

.

Здравсттвена сигурност и прецизност

Постоје многи фактори који утичу на сигурност. Наиме, Apple компанија трвди да је вероватноћа да би случајна особа из популације могла да откључа телефон насумично изабраног корицника помоћу Face ID-а је приближно 1 према 1.000.000. Као додатну заштиту, Face ID омогућава само пет неуспешних покушаја подударања пре него што је потребна лозинка. Статистичка вероватноћа је различита за близанце и браћу и сестре који имају физичке сличности као и међу децом млађом од 13 година, јер се њихове различите црте лица нису у потпуности развиле. Због ових фактора је уведена обавезна аутентикација корицника уз помоћ лозинке тзв. ПИН-а.

Додатну проверу безбедности се врши када:

- је уређај укључен или поново покренут.
- није откључан више од 48 сати.
- Лозинка се није користила за откључавање уређаја у последњих шест и по дана, а Face ID није коришћен у последња четири сата.
- је примио команду за даљинско закључавање.
- После пет неуспелих покушаја препознавања лица.
- Након покретања хитног СОС позива притиском и држањем истовременог дугмета за јачину звука и бочног дугмета 2 секунде.

Што се тиче здравствене сигурности, систем камера TrueDepth темељно је тестиран и задовољавају међународне сигурносне стандарде. Систем TrueDepth камере је сигуран за употребу под нормалним условима употребе. Систем неће нанети никакву штету очима или кожи због малог учинка. Међутим, инфрацрвени емитери могу оштетити током поправке или растављања и тада корисник може угрозити своје здравље.

Touch ID

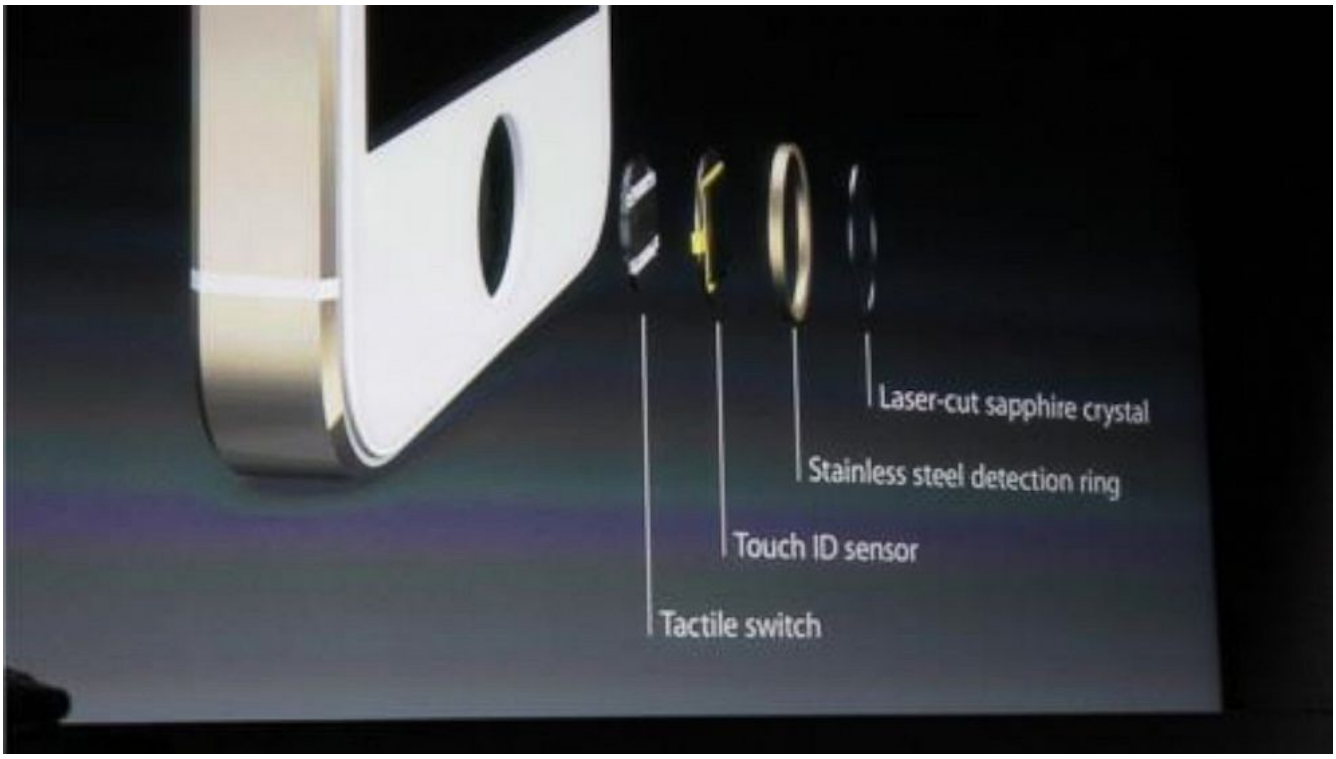
Touch ID је систем за откривање отиска прста који чини бржи,лакши и сигуран приступ подржан на Apple уређајима. Ова технологија чита податке о отисцима прстију из било ког угла и временом сазнаје више о отиску прста корисника, при чему сензор наставља да проширује мапу отиска прста јер се при свакој употреби идентификују додатни преклапајући чворови.

Apple уређаји са Touch ID сензором могу се откључати помоћу отиска прста. Touch ID не замењује потребу за лозинком уређаја или корисничком лозинком, што је и даље потребно након покретања, поновног покретања или одјаве уређаја. У неким апликацијама Touch ID се такође може користити уместо лозинке уређаја или корисничке лозинке. На пример, за откључавање бележака заштићених лозинком у апликацији Notes, за откључавање веб локација заштићених привесцима и откључавање подржаних лозинки за апликације. Међутим, лозинка уређаја или корисничка лозинка увек су потребни у неким сценаријима, када дође до промена постојеће лозинке уређаја или корисничке лозинке или да уклоните постојеће регистрације отисака прстију или направите нове.

Када сензор отиска прста открије додир прста, покреће напредни низ слика за скенирање прста и шаље скенирање у сигурну енклаву. Комуникација између процесора и Touch ID сензора одвија се преко сабирнице серијског периферног интерфејса. Процесор прослеђује податке на Secure Enclave-у, али не може да их прочита јер су шифроване. Дешифровање се врши помоћу заједничког кључа предвиђеног за сваки Touch ID сензор и одговарајућу сигурну енклаву у фабрици. Заједнички кључ је јак, случајан и различит за сваки Touch ID сензор. Размена кључа сесије користи умотавање AEC кључа, при чему обе стране пружају насумични кључ који успоставља кључ сесије и користи AEC шифровање транспорта као у претходном поглављу.

Док је векторизован за анализу, растерско скенирање корисничког прста се привремено чува у шифрованој меморији унутар Secure Enclave, а затим се одбацује. Анализа користи мапирање угла протока, што је процес са губитком који одбацује ситнице које би биле потребне за реконструкцију стварног отиска прста корисника. Добијена мапа чворова чува се без икаквих података о идентитету у шифрованом формату који може да прочита само Secure Enclave. Ови подаци никада не напуштају уређај. Није послат Apple-у нити је укључен у резервне копије уређаја.

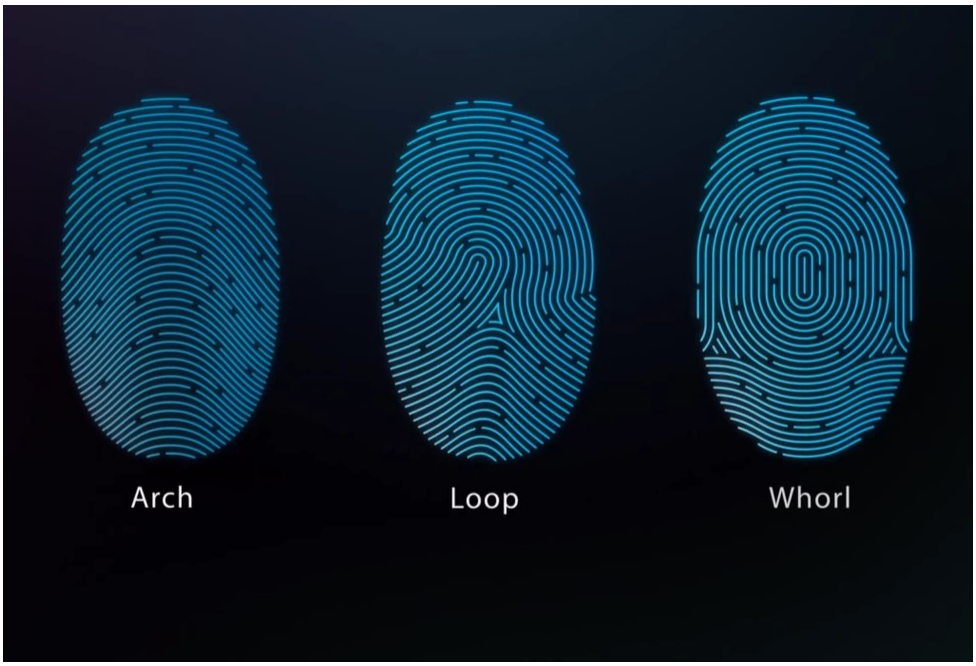
Како функционише Touch ID?



Слика 9 Компоненте Touch ID-ја

Дугме Home направљено је од сафирног кристала, а испод се налази штити сензор танак 170 микрона. Дугме Home такође има функцију сочива, омогућавајући сензору од 500 ppi да се фокусира на отисак прста. Челични прстен око дугмета је оно што открива прст корисника и обавештава Touch ID да започне очитавање отиска прста, док сензор користи напредни

капацитивни додир за снимање слика вашег отиска прста у високој резолуцији. Што се тиче софтвера, Touch ID чита отиске прстију у оријентацији од 360 степени, анализира подепидермалне слојеве коже и категорише сваки отисак у категорије лука, петље или коврџаве (слика 10)



Слика 10 Кагегорије отиска прста

Сигурност Touch ID-ја и прецизност

Touch ID мапира појединачне детаље гребена отиска прста, укључујући варијације попут пора, и заједно прикупити све податке. Touch ID користи ове податке за подударање и препознавање отисака прстију.

Сваки отисак је јединствен, па је реткост да два одвојена отиска буду довољно слична да се региструје као подударање за Touch ID. Вероватноћа да се ово догоди је 1 на 50 000 са једним уписаним прстом. А Touch ID омогућава само пет неуспешних покушаја подударања отиска прста пре него што корисник мора да унесе лозинку. Поређења ради, шансе за погађање типичне четвороцифрене лозинке су 1 на 10.000. Иако би се неки кодови, попут „1234“, могли лакше наслутити, образац отиска прста не може се лако погодити.

Закључак (Touch ID vs Face ID)

Лозинке и лозинка су пресудни за сигурност Apple уређаја, али корисници морају бити у могућности да брзо приступе својим уређајима чак и стотину пута дневно. Биометријска потврда идентитета пружа прилику да се задржи сигурност снажне лозинке а коју неће бити потребно ручно уносити, истовремено пружајући погодност брзог откључавања притиском прста или погледом. Touch ID и Face ID не замењују лозинку или шифру, али у већини ситуација чине приступ бржим и лакшим.
Face ID неће радити у одређеним случајевима, баш као ни Touch ID (хладно време, прљав сканер, када маска прелази преко скенера, уколико корисник користи погрешан прст итд.) Статистика је више на страни Face ID-ја која тврди да један у милион људи може откључати телефон корисника а да притом нису ни у каквом крвном сродству, док је тај број изузетно мањи када је у питању Touch ID (1 према 50 000).
Међутим, постоји један начин на који се Touch ID може користити, а Face ID не, а то је за откључавање iPhone-а када корисник спава.Face ID захтева да корисник има отворене очи, док Touch ID захтева само отисак прста. Постоје добре и лоше ствари у вези с овим. У несрећи би било лако откључати iPhone и контактирати члана породице. Али у већини осталих случајева, безбедност Face ID-ја се показала као боља него код Touch ID-ја.

Литература

1. How Apple’s iPhone X TrueDepth Camera Works[приступљено: 17.9.2020.] https://www.extremetech.com/mobile/255771-apple-iphone-x-truedepth-camera-works
2. Security Enclave processor for a System on a Chip ;Manu Gulati, Saratoga, CA (US); Michael J. Smith, San Francisco, CA (US); Shu-Yi Yu, Cupertino, CA (US)
3. iOS Security Framework: Understanding the Security of Mobile Phone Platforms;William Enck, Razvan Deaconescu, Mihai Chiroiu, Luke Deshotels
4. Apple Platform Security;[приступљено: 17.9.2020.] https://support.apple.com/en-gb/guide/security/welcome/web
5. Touch ID and Face ID overview[приступљено: 17.9.2020.] https://support.apple.com/guide/security/touch-id-and-face-id-overview-sec067eb0c9e/web
6. Touch ID: Inside the fingerprint scanner on Apple's iPhone 5s [приступљено: 17.9.2020.] https://gadgets.ndtv.com/mobiles/news/touch-id-inside-the-fingerprint-scanner-on-apples-iphone-5s-417141