Jihočeská univerzita v Českých Budějovicích
Přírodovědecká fakulta

Analýza biometrických autentizačních mechanismů smartphonů

Bakalářská práce

Daniel Pražák

Školitel: Ing. Petr Břehovský

České Budějovice 2019

Bibliografické údaje

Pražák, D., 2019: Analýza biometrických autentizačních mechanismů smartphonů. [Analysis of biometric authentication mechanisms in smartphones. Bc. Thesis, in Czech] – 42 p., Faculty of Science, University of South Bohemia, České Budějovice, Czech Republic.

Abstrakt

Bakalářská práce se zabývá návrhem a realizací metod za účelem analýzy nejrozšířenějších autentizačních biometrických mechanismů v chytrých telefonů. Teoretická část seznamuje čtenáře s problematikou autentizačních mechanismů a pojednává o dostupných technologiích využívaných ve smartphonech. Praktická část zahrnuje návrh a testování popsaných metod na snímačích otisků prstů a funkcí rozpoznání obličeje u chytrých telefonů s operačními systémy Android a iOS. Na závěr je vyhodnocena úspěšnost analýzy a míra zabezpečení testovaných senzorů.

Klíčová slova

čtečka otisků prstů, senzor otisků prstů, snímač otisků prstů, Touch ID, Rozpoznání obličeje, Face ID, autentizace, biometrie

Abstract

The thesis deals with the design and implementation of methods for the purpose of analyzing the most widespread authentication biometric mechanisms in smartphones. The theoretical part of the work acquaints the reader to the issue of biometric authentication mechanisms and concerns the available technologies used in smartphones. The practical part includes design and testing of described methods on fingerprint readers and face recognition functions in smartphones with operating systems Android and iOS. In conclusion, the success of the analysis and the level of security of the tested sensors are evaluated.

Keywords

fingerprint sensor, Touch ID, facial recognition, Face ID, authentication, biometrics

Prohlášení

Prohlašuji, že svou bakalářskou práci Analýza biometrických autentizačních mechanismů smartphonů jsem vypracoval samostatně pouze s použitím pramenů a literatury uvedených v seznamu citované literatury.

Prohlašuji, že v souladu s § 47b zákona č. 111/1998 Sb. v platném znění souhlasím se zveřejněním své bakalářské práce, a to v nezkrácené podobě elektronickou cestou ve veřejně přístupné části databáze STAG provozované Jihočeskou univerzitou v Českých Budějovicích na jejích internetových stránkách, a to se zachováním mého autorského práva k odevzdanému textu této kvalifikační práce. Souhlasím dále s tím, aby toutéž elektronickou cestou byly v souladu s uvedeným ustanovením zákona č. 111/1998 Sb. zveřejněny posudky školitele a oponentů práce i záznam o průběhu a výsledku obhajoby kvalifikační práce. Rovněž souhlasím s porovnáním textu mé kvalifikační práce s databází kvalifikačních prací Theses.cz provozovanou Národním registrem vysokoškolských kvalifikačních prací a systémem na odhalování plagiátů.

V Českých Budějovicích dne 10. 12. 2019

Daniel Pražák

Poděkování

Děkuji vedoucímu bakalářské práce Ing. Petru Břehovskému za metodickou, pedagogickou a odbornou pomoc a další cenné rady při zpracování mé bakalářské práce. Dále bych chtěl poděkovat Mgr. Jakubovi Geyerovi za odborné poznatky při konzultacích ohledně praktické části bakalářské práce, konkrétně při návrhu jedné z metod.

Obsah

Úvod

V současné době dochází k velkému rozšíření chytrých telefonů se čtečkou otisků prstů a funkcí rozpoznání obličeje. Pro uživatele se jedná o pohodlné a rychlé mechanismy sloužící k získání autentizace a následnému přístupu ke svému chytrému telefonu. Počátky komerčního využívání senzorů otisků prstů v telefonech se datují do roku 2013, kdy americká společnost Apple Inc. Představila první chytrý telefon, model iPhone 5s, se čtečkou otisků prstů integrovanou v domovském tlačítku a definovala tak nový způsob autentizace u smartphonů. Myšlenky se krátce poté ujali i ostatní výrobci telefonů s operačním systémem Android a čtečka otisků prstů se začala významně rozšiřovat. V současné době ji nabízejí i telefony střední třídy, a tak se tento způsob autentizace pochopitelně rozšiřuje stále k více uživatelům.

Nicméně jak správně upozorňuje společnost Kaspersky Lab [1] zabývající se globální kyber bezpečností již od roku 1997, senzory otisků prstů rozhodně nejsou bezchybné. Většina senzorů totiž nedokáže rozlišit mezi skutečným prstem a „odlitkem“, což představuje hrozbu bezpečnosti.

Jindy je zase na vině samotný výrobce smartphonu, který sice použije nejnovější dostupnou technologii, ale nedokáže ji bezpečně integrovat do svého systému. Příkladem pak jistě mohou být společnosti HTC a Samsung, které ve svých chytrých telefonech ukládaly snímky otisků prstů uživatelů v nezašifrované podobě jako soubor s příponou .bmp, tedy jako obyčejný bitmapový obrázek. Jakákoliv aplikace s povoleným přístupem k uživatelovým obrázkům a přístupem k internetu tak mohla snímky otisků prstů ukrást.

Podobně zranitelná může být i bezpečnost mechanismů pro rozpoznání obličeje, které se začaly v chytrých telefonech ve velké míře rozšiřovat od roku 2017, když společnost Apple představila technologii Face ID. Snahou ostatních výrobců bylo nabídnout autentizační mechanismus na podobné principu, namísto senzorů ale pro snímání tváře využívají pouze přední fotoaparát.

A právě v této práci se budu zabývat otázkou, zda jsou dnešní čtečky otisků prstů a funkce rozpoznání obličeje ve smartphonech bezpečné, či je možné je jednoduchým způsobem oklamat. Využiji ověřené i vlastní metody k prolomení biometrických autentizačních mechanizmů smartphonů a pokusím se jimi analyzovat nejnovějších technologie současných smartphonů od dvou různých výrobců.

1 Otisk prstu

Kapitola shrnuje historii zkoumání otisků prstů a vyzdvihuje důležité osobnosti spojené s touto problematikou. Další část kapitoly pojednává o papilárních liniích, jejich vzniku, charakteristice, zařazuje je do tříd a věnuje se jejich markantům a detailům.

1.1 Historie

Nejstarší dochovaný důkaz znalosti existence papilárních linií sahá do období několik tisíciletí před naším letopočtem, kdy indiánské kmeny, sídlící na území dnešního státu Indiana ve Spojených státech amerických, vytvářely ryté obrazy znázorňující lidskou ruku včetně papilárních linií, tzv. „petroglyfy“ [2].

První zmínky o využívání otisku prstu jako unikátního identifikačního prvku se datují do 9. století před naším letopočtem. V té době Asyřané používali specifičnost posledních článků prstů, aby zabránili falsifikaci vlastnoručně vyrobených hliněných tabulek. K podobným účelům sloužily otisky také při výrobě keramických výrobků v Řecku, Egyptě a na území Římské říše.

Jakožto prostředek k určování totožnosti osob začali otisk prstu poprvé používat v Číně. Důkazem je vůbec první spisek o otiscích čínského autora Kio Kung-yen, podle kterého byli Číňané s významem otisku dobře obeznámeni a využívali ho při obchodních záležitostech. V období od 7. do 10. století n. l. nařizoval starý čínský zákoník otiskem prstu verifikovat rozvodový dokument.

Přibližně ve stejném období začali výhod daktyloskopie využívat také v Japonsku, kde se vůbec poprvé zaměřili na otisk z kriminalistického hlediska. Konkrétně byl snímán levý palec – tzv. „bo-han“ – pouze zločincům. Odsouzení museli stvrdit svým otiskem i proti nim vznesený rozsudek. Postup byl prováděn až do roku 1868 a šlo tak o vůbec první rozsáhlou registraci otisků prstů usvědčených zločinců.

Patrně jako první, kdo se otiskům prstů začal věnovat z vědeckého hlediska, byl italský lékař a přírodovědec Marcello Malpighi, který v roce 1686 zkoumal papilární linie pod mikroskopem a popsal spirálu a smyčku, tedy dva z dnes již několika základních typů dermatoglyfů. Přibližně o sto let později rozpoznal unikátnost otisku prstu britský kreslíř a grafik Thomas Bewick, který otisk používal jako podpis u svých děl a publikací [3].

O největší přínos v oblasti daktyloskopie se postaral Jan Evangelista Purkyně, český fyziolog, který v roce 1823 ve svém latinsky psaném spisu poprvé popsal vzory papilárních linií a na základě jejich geometrického upořádání určil devět typů vzorů – oblouk, strmý oblouk, ulnární smyčka, radiální smyčka, paví oko, dvojsmyčka, spirální vír, eliptický vír a kruhový vír. Rovněž stanovil jako podstatný klasifikační znak tzv. deltu (trojúhelníkové seskupení papilárních linií). Práce však řadu let nebyla mezinárodně uznávána [4].

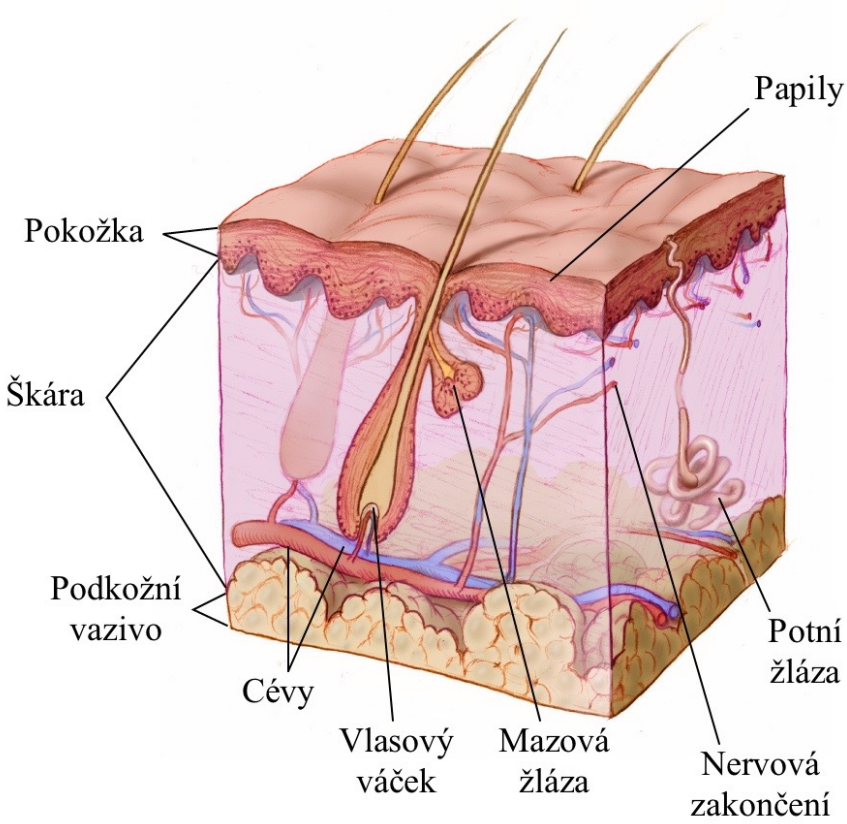
Až v roce 1888 položil základy kriminalistické daktyloskopie Dr. Henry Faulds z Tokia. Tomu se jako prvnímu podařilo určit totožnost, dopadnout a usvědčit pachatele dvou krádeží za pomoci otisků prstů sejmutých na místě činu. Jeho publikace v časopise Nature, popisující zkušenost při využití nové metody, pomohla k rozšíření daktyloskopické identifikace v kriminalistice do Velké Británie a Německa [5].

1.2 Papilární linie v rámci stavby kůže

Kůže je největší lidský orgán skládající se z vrstvy několika druhů buněk. Kromě estetické funkce chrání tělo před bakteriemi a vnějším prostředním, zajišťuje termoregulaci, umožňuje vnímat tlak, teplo, chlad a cit, zbavuje tělo odpadních látek a podílí se na příjmu potřebných vitamínů. Plocha kůže na lidském těle dospělého člověka činí 1,6 – 1,8 m^2 a váží přibližně 3 kilogramy. Její tloušťka je na různých místech těla rozdílná – od 0,5 do 4 mm. Nejtenčí kůže se nachází na očních víčkách a uchu, naopak v místech většího opotřebení a tlaku – plosky nohou, záda či dlaně – je nejtlustší.

Kůži tvoří nervová zakončení, cévy pro zásobování živinami, potní žlázy zajišťující termoregulaci, mazové žlázy sloužící k promaštění pokožky, vlasové váčky a mnoho dalších důležitých částí (obr. 1) [6]. Stavbu kůže tvoří tři hlavní vrstvy: pokožka (epidermis), škára (dermis) a podkožní vazivo (hypodermis). Ze škáry vybíhají proti pokožce hřebínkovité výběžky (tzv. papily), ve kterých se nacházejí nervová zakončení pro vnímání citu a krevní vlásečnice sloužící k výživě pokožky. Stejný vzor papil jako uvnitř kůže je tvořen i na jejím vnějším povrchu, kde představuje papilární linie dosahující výšky od 0,1 do 0,4 mm a šířky 0,2 – 0,7 mm. Místa mezi výběžky se nazývají brázdy. Kombinace papil a brázd tvoří charakteristický obraz otisku, který se nachází na dlaních, prstech rukou i nohou a na chodidlech.

Papily se začínají vytvářet již při vývoji plodu, konkrétně v prenatálním období mezi čtvrtým a pátým měsícem. V průběhu života se linie zvyšují a rozšiřují, ale jejich unikátní struktura se nikterak nemění. Vlivem stárnoucí kůže mohou specifickou kresbu linií narušovat pouze vrásky. Při poškození kůže popálením či pořezáním se papilární linie odstraní dočasně a po zahojení dojde k jejich obnově do původní podoby.



Obrázek 1: Stavba a vrstvy kůže

Z kriminalistického a bezpečnostního hlediska je významná zejména skutečnost, že kresba linií je pro daného člověka jedinečná. Na světě neexistují dva jedinci, kteří by měli stejnou kresbu papilárních linií. S jistou pravděpodobností shody lze operovat, nicméně je extrémně nízká, konkrétně jde o poměr 1:64 miliardám.

1.3 Charakteristiky otisků prstů

Klasifikace znaků průběhu papilárních linií je určována tříúrovňovým, po sobě jdoucím systémem. Nejprve je otisk zařazen do třídy, následně jsou určeny markanty a na závěr jsou rozlišovány detaily linií.

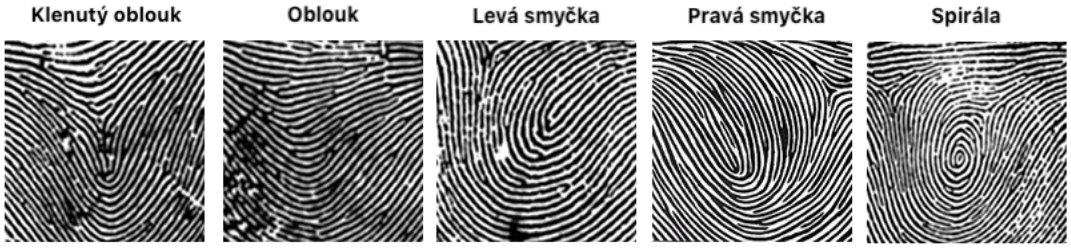
1.3.1 Singularity a třídy

Ačkoli se otisky prstu vyznačují svojí unikátností, lze je všechny zařadit do specifických tříd, které jsou charakterizovány opakujícími se vzory průběhu linií. Globální tvary se vyznačují určitým počtem singularit, jež jsou označovány jako jádro a delta. Jádro představuje pomyslný vrchol otisku, bod delta je popsán jako místo, odkud se linie rozbíhají do třech různých směrů.

Zařazení otisků do tříd výrazně urychluje vyhledávání shody, kdy není potřeba prohledávat celou databázi, ale pouze její podmnožinu. O jejich klasifikaci se zasloužil Dr. Edward Henry na přelomu 19. a 20. století. Tříd je celkem pět, ale základ tvoří tři – papilární linie jdoucí do oblouku se rozdělují na obyčejný a klenutý, linie jdoucí do smyčky jsou rozdělovány podle strany na pravou a levou (Obrázek 2) [7].

Definice tříd podle vzoru papilárních linií a singularit:

- **Klenutý oblouk** – obsahuje jedno jádro a jednu deltu, přičemž bod delty se nachází přímo pod jádrem
- **Oblouk** – neobsahuje žádnou singularitu
- **Levá smyčka** – obsahuje jedno jádro a jednu deltu, bod delty se nachází vpravo od jádra
- **Pravá smyčka** – obsahuje jedno jádro a jednu deltu, bod delty se nachází vlevo od jádra
- **Spirála** – obsahuje jedno jádro a dvě delty, jádro se nachází mezi body delty



Obrázek 2: Třídy otisků

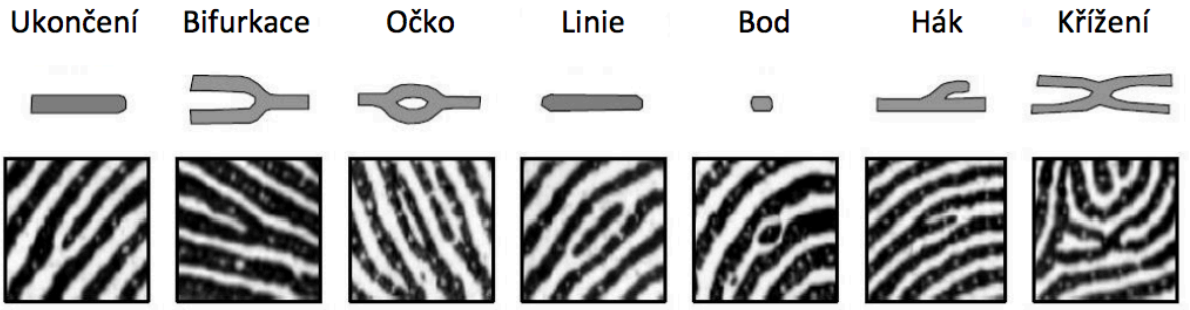
1.3.2 Markanty

Druhou úroveň při klasifikaci otisků prstů představuje určení markantů. Jde o charakteristické rysy papilárních linií, na jejichž základě probíhá porovnání otisků. Markanty jsou zpravidla zařazovány do tříd a jsou jim přiřazeny souřadnice X a Y a úhel jakým směřují. Otisk může obsahovat několik desítek markantů, přičemž nejčastějším zástupcem je tzv. vidlice, tedy rozdvojení papilárních linií.

Za markant lze obecně považovat jakoukoli nepravidelnost nebo zvláštnost v otisku. Aby byla jejich charakterizace o něco snazší, je určováno více než deset typů markantů. K základním se řadí sedm z nich.

Základní typy markantů:

- **Ukončení** – papilární linie má tvar polopřímky
- **Rozdvojení (vidlice)** – papilární linie se rozdvojuje
- **Očko** – papilární linie se spojují do kruhu
- **Linie** – papilární linie ve tvaru úsečky mezi ostatními liniemi
- **Bod** – samostatná linie ve tvaru tečky
- **Hák** – papilární linie se rozdvojuje, přičemž jedna je kratší než 3 mm
- **Křížení** – dvě papilární linie se kříží

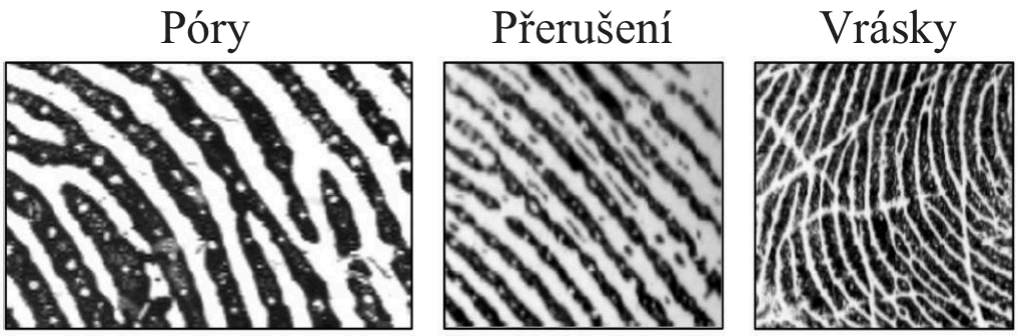


Obrázek 3: základní typy markantů

Více typů markantů rozlišují především policejní technici na odboru kriminalistické techniky a expertíz. V komerční sféře jsou většinou určovány pouze dva typy markantů – ukončení a rozdvojení, které se zároveň řadí mezi ty nejčastěji se vyskytující. Důvodem je zejména zkrácení výpočetní doby algoritmu a tím urychlení celého procesu při porovnání otisků.

1.3.3 Detaily linií

Po zařazení otisku do třídy a určení jednotlivých markantů jsou na třetí úrovni rozlišovány ještě detaily jednotlivých papilárních linií. V potaz se bere poloha pórů kůže na liniích, přerušení linií a vrásky vzniklé stárnutím kůže. Hledí se také na rozměry linií i brázd mezi nimi.



Obrázek 4: Detaily linií

Detaily linií jsou při porovnávání dvou otisků velmi cenným atributem a umožňují určit shodu s vysokou mírou přesnosti. Je v podstatě nulová pravděpodobnost, že by dva jedinci měli v rámci jednoho otisku kromě singularit a markantů shodné i detaily linií. K jejich rozpoznání a určení je však potřeba disponovat kvalitním snímky otisků ve vysokém rozlišení.

2 Snímače otisků prstů v chytrých telefonech

V podstatě nejdůležitější částí při snímání otisků jsou samotné senzory. Ty se liší nejenom způsobem snímání, ale také velikostí, cenou a hlavně bezpečností. Všechny současné senzory patří v podstatě vždy do jedné z následujících skupin: optické, kapacitní a ultrazvukové.

První čtečka otisků prstů byla použita v roce 2013 v iPhonu 5s americké společnosti Apple Inc. Konkrétně se jednalo o kapacitní senzor, který byl integrovaný přímo do domovského tlačítka telefonu. Postupem času se čtečky otisků prstů začaly objevovat i v telefonech konkurenčních značek, kdy například jihokorejská společnost Samsung nasadila do svého telefonu jednodušší verzi kapacitního senzoru, konkrétně tzv. Swipe senzor.

V poslední době se v telefonech začínají používat senzory ultrazvukové, které přináší několik výhod, kdy tou hlavní je bezpečnost. Předpokládá se, že senzory využívající ultrazvukových vln postupně v telefonech nahradí kapacitní senzory, a to především díky schopnosti naskenovat otisk prstu i skrze displej.

2.1 Kapacitní

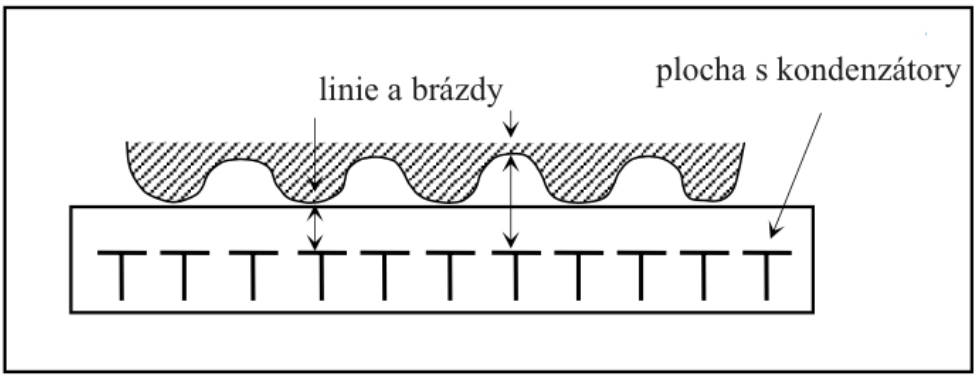
Kapacitní snímače otisků prstů jsou v současné době vůbec nejrozšířenější, přičemž jejich začátek komerčního využívání sahá do 90. let minulého století. Jedná se o senzory, které jsou nejčastěji k nalezení v současných chytrých telefonech, i když je pomalu začínají nahrazovat senzory ultrazvukové.

Kapacitní snímač se řadí mezi polovodičové senzory. Jedná se o dvourozměrné pole složené z destiček mikro kondenzátorů, které jsou zabudované do čipu, čímž je vytvořen skener. Ten má tak velkou citlivost, že po přiložení prstu dokáže díky změně elektrického náboje rozeznat, kde jsou papilární linie. V místě, kde mezi kondenzátorem a prstem dojde ke změně náboje, se nachází papilární linie neboli hřeben. Naopak v místě, kde ke změně elektrického náboje nedojde, se nachází brázda. Snímač je pak schopný zaznamenat, v jakém místě přesně došlo ke změně náboje a v jakém naopak ne. Následně převodník analogového signálu na digitální dokáže zaznamenané údaje předat v příslušné formě dále ke zpracování, kdy jsou porovnány s již naskenovanými vzory.

Schopnost kapacitního skeneru přesně rozeznat otisky prstů, je přímo úměrně dána počtem kondenzátorů. Jednodušší snímače disponují jen několika stovkami kondenzátorů. Naopak kvalitní skenery mají kondenzátorů několik tisíc. Zpočátku se v chytrých telefonech používaly senzory otisků prstů s malým počtem kondenzátorů, tudíž snímače nebyly tak

bezpečné, a navíc ani nebyly tak přesné a rychlé. Nejnovější telefony disponující senzorem otisků prstů se ale mohou pochlubit již kvalitním snímačem s několika tisíci kondenzátory.

Hlavní výhodou kapacitních skenerů je především bezpečnost. Kapacitní senzory v telefonech navíc reagují převážně na specifickou změnu velikosti náboje v kondenzátorech při kontaktu s lidskou pokožkou. Proto není jednoduché kapacitní snímač obelstít například vytištěnou 3D mapou otisku. Na prolomení je potřeba mít skutečně kvalitní snímek otisku prstu a použit vodivý inkoust.



Obrázek 5: Schéma kapacitního senzoru

2.2 Ultrazvukové

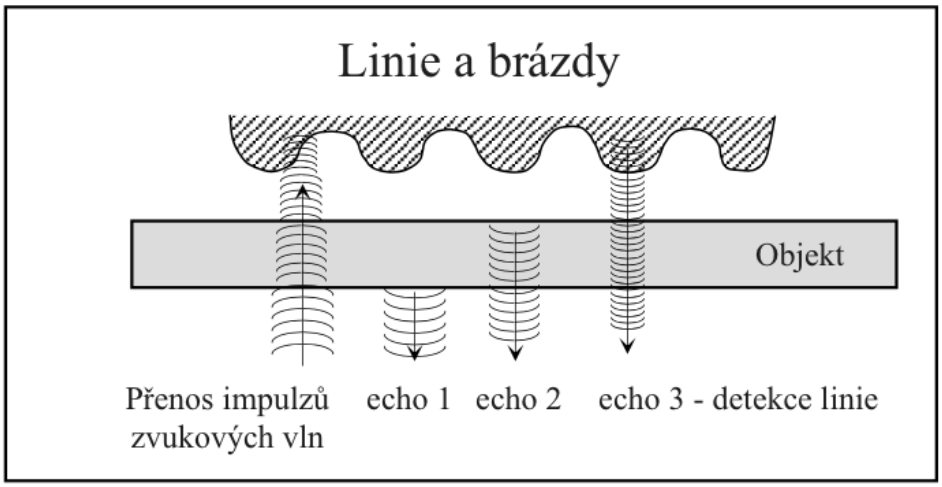
Druhým zástupcem čteček otisků prstů v chytrých telefonech, jsou snímače ultrazvukové. Ty jsou nejenom nejnovější, ale také nejpokročilejší. Hlavní předností ultrazvukových vln je schopnost pronikat skrze materiály, což se v případě chytrých telefonů projeví jako výhoda především při snaze docílit co nejmenších rozměrů. Ultrazvukové snímače jsou totiž schopné naskenovat otisk prstu například i skrze displej, čímž odpadá nutnost integrovat čtečku na záda telefonu nebo do fyzického domovského tlačítka pod displejem.

Ultrazvukový snímač je založený na odesílání akustických signálů směrem k prstu a zachycování tzv. echo signálů při každé změně impedance. Vyslané signály se od snímaného prstu odrazí a vrací se zpět k ultrazvukovému senzoru. Přijímač v závislosti na době, za kterou se signál vrátil, vyhodnotí, zdali se ultrazvukový signál odrazil od papilární linie či od brázdy. Čím déle bude prst na snímač přiložený, tím detailnější otisk prstu se podaří naskenovat.

Výhod ultrazvukového snímače otisků prstů je hned několik. V první řadě je možné otisk naskenovat i za předpokladu, že je prst špinavý. Ultrazvukovým signálům nevadí ani vlhkost nebo dokonce voda, tudíž na rozdíl od kapacitních senzorů nemají ty ultrazvukové

problémy s potem na rukou. Největší výhodou je ovšem samotná bezpečnost, která je dokonce vyšší než u senzorů kapacitních. Prolomit ultrazvukový snímač je tak možné pouze na softwarové úrovni.

Nevýhodami jsou naopak déle trvající proces skenování, větší mechanické díly, a především pak vyšší pořizovací cena jednotlivých součástek. Proto v současné době nalezneme ultrazvukové čtečky otisků prstu jen ve vybraných telefonech, ale s jejich masivnějším rozšířením se do budoucna počítá, a to především kvůli jejich schopnosti skenovat prst skrze displej.



Obrázek 6: Schéma ultrazvukového senzoru

3 Mechanismy rozpoznání obličeje v chytrých telefonech

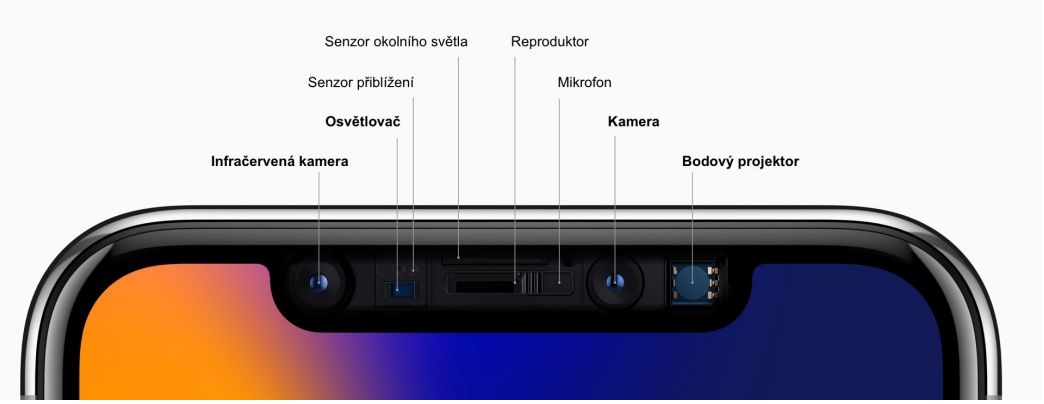
Vyjma snímačů otisků prstů se poslední roky začíná ve smartphonech stále častěji objevovat další autentizační mechanismus, který k odemykání telefonu využívá biometrii. Je jím funkce rozpoznání obličeje, jež se v chytrém telefonu poprvé objevila už v roce 2011 (ještě dříve než senzor otisků prstů), a to s příchodem systému Android 4.0. V té době ji jako první smartphone nabízel Galaxy Nexus společnosti Google. [8]. Metoda se ale příliš neujala, na čemž se z části podílela její nespolehlivost a minimální zájem jak ze strany ostatních výrobců, tak zákazníků. O dva roky později ji navíc zastínila autentizační metoda spočívající ve snímání otisků prstů.

V dnešní době se ale odemykání pomocí tváře u uživatelů těší čím dál větší oblibě, což dokazuje i výzkum společnosti Counterpoint, podle něhož tímto mechanismem momentálně disponuje 40 % chytrých telefonů na trhu a v roce 2020 by to podle dostupné analýzy mělo být dokonce 64 % [9]. O zásadní rozšíření se postarala společnost Apple, která v roce 2017 představila iPhone X s funkcí zvanou Face ID – sofistikovanou biometrickou autentizační metodou, která ke skenování tváře používá celou řadu senzorů. Ve snaze dohnat konkurenci začali obdobné systémy nabízet ve svých smartphonech také ostatní výrobci. Jejich mechanismy ale nejsou na takové úrovni jako zmíněné Face ID, protože ve většině případů ke skenování obličeje používají pouze přední kameru a vytvářejí si tak jenom snímky tváře ve dvourozměrné podobě. Právě proto lze dnešní mechanismy rozpoznání obličeje v telefonech rozdělit na ty, které umí snímat tvář ve 3D a na ty, které ji snímají ve 2D.

3.1 Snímání ve 3D

Skenování obličeje v trojrozměrné podobě představuje pokročilejší a bezpečnější mechanismus, který zpravidla nelze oklamat klasickou fotografií. Daná metoda ke snímání používá přední kameru jen částečně a většinu údajů získává z ostatních senzorů, jež skenují tvář pomocí infračerveného světla.

Například u funkce systému Face ID od společnosti Apple se při snímání obličeje kombinují data z několika senzorů, které se společně s předním fotoaparátem označují jako TrueDepth camera. Kromě kamery je při snímání obličeje využíván také osvětlovač, infračervený bodový projektor a infračervená kamera [10].



Obrázek 7: Senzory potřebné pro trojrozměrné snímání

Proces snímání probíhá v několika krocích. Osvětlovač nejprve nasvítí obličej infračerveným světlem, což systému pomůže detekovat tvář i za minimálního světla, nebo pokud má osoba nasazené brýle, pokrývku hlavy a podobně. Do toho bodový projektor promítá na obličej 30 000 infračervených teček, které se odráží od původního nasvícení. Ty následně snímá infračervená kamera a vytváří z nich hloubkovou mapu tváře, čímž získává přesné údaje o obličeji a zároveň detekuje značnou část mimiky [11].

Veškerá data jsou poté předána procesoru, konkrétně neuronovému enginu, který na základě hloubkové mapy vytvoří matematický model, jenž pak porovnává s uloženými údaji o obličeji. Veškerá data jsou uložena v bezpečnostní architektuře Super Enclave a jsou tak oddělena od zbytku systému a aplikací. Data se nezálohují, nenahrávají se na servery a ani je nelze zpětně reprodukovat a sestavit z nich obličej.

3.2 Snímání ve 2D

Snímání tváře pouze ve dvourozměrné podobě nabízí dnes více než polovina chytrých telefonů, které funkcí rozpoznání obličeje disponují [9]. Funkce si vystačí pouze s přední fotoaparátem, který pořídí snímek obličeje a následně jej porovnání s předlohou. Pokud mechanismus není doplněn o další bezpečnostní prvky, tak většinou není schopný určit, zdali se jedná o skutečný obličej uživatele či pouze o jeho fotografii.

Výrobci do svých telefonů implementují mechanismus pro snímání tváře ve 2D hlavně proto, aby snížili výrobní náklady. Mnody se tak spoléhají pouze na algoritmus dané funkce, který může například kontrolovat, zda se tvář před kamerou hýbe.

Praktická část

Tato kapitola se zabývá praktickou částí, tedy návrhem, realizací a testováním metod sloužících k analýze biometrických autentizačních mechanizmů smartphonů.

4 Metodika a cíle

Cílem práce je otestovat míru zabezpečení jednotlivých typů senzorů otisků prstů, které se od roku 2013 začaly komerčně využívat v chytrých telefonech, a funkcí rozpoznání obličeje, které výrobci integrují do smartphonů v posledních letech. Primárním účelem tedy je získat autentizaci, tím i přístup do telefonu a v konečném důsledku i ke všem datům, aplikacím a jejich obsahu, které jsou v telefonu uloženy.

Určité, převážně novější druhy mechanismů ale mohou být komplexněji zabezpečené, jejich prolomení se nemusí podařit a přístup do telefonu tak nebude získán. Za těchto okolností bude vždy popsáno, jak se určitý typ biometrického autentizačního zabezpečení během pokusů o prolomení choval – zda rozeznal falzifikovaný otisk či obličej a odmítl autentizaci, nebo jestli ani nezaregistroval pokus o prolomení.

Oba druhy autentizačních metod budou testovány na odlišném zařízení. Lišit se budou nejenom výrobci telefonů, ale také nainstalované mobilní operační systémy, tím i způsob a míra zabezpečení mechanismu, ukládání a následné porovnání otisku či tváře s předlohou uloženou v zařízení.

5 Snímače otisků prstů

Snímání otisků prstů patří v současné době k nejrozšířenější biometrické autentizační metodě v chytrých telefonech. Důvodem je nejenom snadná implementace příslušných senzorů do zařízení, ale především pak snižující se cena potřebných komponent. Proto čtečkami otisků disponují už i smartphony zařazující se do střední a nižší střední třídy.

Nejširší zastoupení mají senzory kapacitní. Ty výrobci integrují nejčastěji na zadní část telefonu nebo do fyzických domovských tlačítek pod displejem, sporadicky se pak objevují v tlačítku sloužícího pro zapínání umístěného na boku telefonu. Prvním smartphonem s kapacitní čtečkou otisků prstů byl iPhone 5s, telefon společnosti Apple představený v roce 2013.

Vývoj nových technologií spolu s vyššími nároky zákazníků zapříčinily, že výrobci začali do chytrých telefonů integrovat nový typ senzoru, jmenovitě ultrazvukový. Jeho hlavní benefit spočívá v možnosti implementace pod OLED displej, skrze který je schopný snímat přiložený otisk. V případě čtečky fungující na bázi ultrazvukových vln je také značnou předností vyšší míra zabezpečení a spolu s tím spojená schopnost skenovat otisk ve 3D.

5.1 Testovaná zařízení

Pro účely testování byla vybrána celkem dvě zařízení s ohledem na použitý senzor a jeho nejnovější generaci. Každé zařízení představuje zástupce jednoho typu snímače otisků prstů používaného v odvětví chytrých telefonů. Při výběru byly také zohledněny dva nejrozšířenější mobilní operační systémy – Google Android a Apple iOS – kdy každý z nich má jednoho zástupce.

Zvoleny byly chytré telefony, které při daných specifikacích – typ senzoru a druh systému – disponují nejaktuálnějšími technologiemi v době psaní bakalářské práce. Snahou tak bylo dosáhnout co možná nejspravedlivějších porovnání.

5.1.1 Apple iPhone 8 Plus

Zástupce pro kapacitní senzor byl zvolen Apple iPhone 8 Plus představený na podzim roku 2017. Jedná se o nejnovější telefon s platformou iOS, jenž nabízí snímač otisků prstů. Apple kapacitní senzor ve svých zařízeních označuje jako Touch ID a v případě zvoleného modelu se jedná již o druhou generaci snímače, která je rychlejší, nikoli však zabezpečenější.

Senzor je integrován do hlavního tlačítka Domů nacházejícího se na přední straně

telefonu v okraji pod displejem. Tloušťka senzoru činí 170 mikronů a zaznamenává obraz otisku v rozlišením 500 ppi (pixels per inch, v překladu: pixelů na palec). Snímač je chráněn laserově broušeným křišťálovým sklem, jež zároveň slouží jako čočka, která zaostří na bříško prstu. O registraci prstu se stará ocelový kroužek v okolí tlačítka, který po přiložení otisku vyšle k senzoru pokyn k zahájení skenování [12].

Stěžejní informací pro tuto bakalářskou práci je, že Touch ID snímá jen subepidermální vrstvu kůže, tedy že ignoruje odumřelou kůži prstu a skenuje jen novou kůži pod ní. Tím by měl snímač snadno rozeznat, zda se jedná o falešný otisk prstu či nikoli. Při testování a následném vyhodnocování bude tento fakt zohledňován.

Ze snímku Touch ID provede inteligentní analýzu a otisk zařadí do kategorie v závislosti na tvaru papilárních linií – oblouk, smyčka či spirála. Vyhodnoceny jsou také markanty, drobné rozdíly v jejich směru způsobené strukturou pórů i struktura jejich okrajů.

Informace jsou následně zašifrovány a uloženy jako matematické vyjádření do bezpečnostní architektury Super Enclave, jež je součástí hlavního procesoru. Díky tomu jsou data oddělena od systému i aplikací a nelze k nim získat přístup. Data se ani nijak nezálohují a nikdy je nelze použít ke zjištění shody v jiné databázi otisků prstů nebo z nich zpětně sestavit obraz otisku [13].

5.1.2 Samsung Galaxy S10

Ultrazvuková čtečka otisků prstů byla testována na Samsungu Galaxy S10, který zároveň představuje nejaktuálnějšího zástupce s tímto snímačem. Telefon byl představen začátkem roku 2019 a v době psaní bakalářské práce nabízí nejmodernější technologii ultrazvukového senzoru v kategorii smartphonů.

Telefon disponuje 3D ultrazvukovým snímačem od společnosti Qualcomm. Senzor o tloušťce menší než 0,2 mm je integrován pod displej, skrze který emituje zvukové vlny a pomocí nich mapuje jedinečný vzor otisku prstu – vlny snímají drobné vzduchové mezery mezi prstem a povrchem displeje, čímž určují linie a brázdy. Získaná data jsou následně předána procesoru k vyhodnocení, zda se jedná o shodu s dříve naskenovaným otiskem či nikoli [14].

Zabezpečení snímače je zajištěno několika způsoby. Hlavní přednost spočívá ve schopnosti pomocí ultrazvukových vln naskenovat trojrozměrný obraz otisku prstu, což představuje také výhodu oproti dříve používaným dvojrozměrným optickým snímačům. Pro účely bakalářské práce je podstatný především fakt, že senzor při snímání otisku detekuje i průtok krve v prstu. Dodatečná ochrana by měla znemožnit čtečku oklamat falešným otiskem v podobě fotografie nebo odlitku.

Čtení pulzů také vede ke snazšímu rozpoznání otisku, pokud je prst mokrý nebo špinavý, čímž je zajištěna větší uživatelská přívětivost. Detekce průtoku krve může být navíc použita k monitorování srdeční frekvence, k měření BMI a analýze hladiny cukru v krvi. Tím se značně rozšiřuje funkcionalita senzoru, kterou ostatní typy čteček (kapacitní a optické) nejsou schopné z technologického hlediska nabídnout [15].

5.2 Návrh metod

Za účelem analýzy míry zabezpečení kapacitního a ultrazvukového senzoru otisků prstů ve výše uvedených telefonech byly zvoleny dvě rozdílné metody. První z nich představuje 3D model otisku zrekonstruovaný z dvojrozměrné předlohy. Druhá metoda spočívá v tvorbě odlitku přímo z prstu jedince.

Metody byly zvoleny a navrženy s ohledem na testované typy senzorů tak, aby ve všech případech existovala jistá pravděpodobnost jejich prolomení. Brány v potaz byly technologické možnosti jednotlivých snímačů, jejich proces snímání otisku a přítomnost dalších prvků zajišťujících vyšší bezpečnost (viz kapitola 5.1.2).

V rámci realizace vybraných metod byla zohledněna jejich finanční náročnost. V úvahu byla brána také dostupnost technologií k rekonstrukci modelu a odlitku otisku s tím, že první vybraná metoda představuje sofistikovanější způsob zhotovení a druhá je méně náročná jak z finančního, tak z technologického hlediska.

Následující kapitoly popisují proces návrhu a realizace jednotlivých metod za účelem následného otestování zabezpečení a analýzy senzorů otisků prstů v telefonech.

5.2.1 3D Otisk

První, technologicky i finančně náročnější zvolená metoda představuje vytvoření 3D modelu otisku prstu z dvojrozměrné předlohy. Proces se skládá z několik částí – nejprve bude otisk sejmut ze skleněného povrchu za pomoci daktyloskopické sady, získaný vzorek se následně vyfotografuje a převede z rastrové do vektorové grafiky pro účely vytvoření 3D modelu za pomoci softwaru, který bude sloužit jako předloha pro tisk na 3D tiskárně.

5.2.1.1 Sejmutí otisku

Jedním z hlavních cílů metody je získání otisku prstu bez vědomí majitele telefonu, tedy například z předmětů zabavených v rámci domovní prohlídky vykonané policejním orgánem. K těmto účelům byla použita kriminalistická sada pro snímání daktyloskopických vzorků, jež byla zapůjčena od Policie České republiky, Krajského ředitelství policie Jihočeského kraje, z odboru kriminalistické techniky a expertiz.

Zapůjčená daktyloskopická sada obsahovala:

- 50 ml daktyloskopický prášek Argentorat
- 50 ml daktyloskopický prášek Černý standard
- 1 ks jemný štětec Spokar s šířkou stírací plochy 2,54 cm
- 2 ks ultra jemný štětec „veverka“ s číselným označením NO. 1-0031
- 1 ks daktyloskopická páska transparentní s rozměry 5 x 914 cm
- 10 ks černé pozadí s rozměry 5 x 10 cm
- 10 ks bílého pozadí s rozměry 5 x 10 cm

Pro zajištění otisku prstu ze skla byl použit daktyloskopický prášek Argentorat, jemný štětec Spokar, ultra jemný štětec „veverka“ a 1 kus černého pozadí zmenšených rozměrů 2,5 x 5 cm.

Obrázek 8: Použitá sada pro sejmutí otisku ze skla

Na otisk prstu umístěného na skle bylo nejprve pomocí jemného štětce naneseno odpovídající množství Argentoratu. Následně za pomoci ultra jemného štětce byl krouživými pohyby prášek odstraněn z míst brázd otisku, čímž se zvýraznily papilární linie a dosáhlo se tak výsledku o odpovídající kvalitě. Přiložením černého pozadí přilnavou stranou na otisk došlo k jeho sejmutí – otisk se včetně detailů obtiskl na plochu pozadí a zároveň se zrcadlově otočil. Nakonec byl sejmutý otisk přelepen transparentní fólií, aby nedošlo k narušení detailů papilárních linií.

Obrázek 9: Proces snímání otisku

5.2.1.2 Vytváření 3D modelu

Pro potřeby vytvoření 3D modelu byl otisk nejprve zachycen 12megapixelovým fotoaparátem s teleobjektivem o šířce 52 mm a ohniskovou vzdáleností f/2.4. Ke zvolení této techniky jsem se rozhodl po konzultaci s jedním z policistů z odboru kriminalistické techniky a expertiz, kde používají metodu na podobném principu – pro zachycení všech podstatných detailů je snímek s dvanácti miliony pixely (rozlišení 4032 × 3024 pixelů) dostačující. Nabízelo se také použití skeneru – ať už samostatné jednotky, nebo takového, který je součástí tiskárny – nicméně výsledný sken by nebyl v dostatečně vysokém rozlišení.

Pořízená fotografie byla následně exportovaná do profesionálního grafického editoru Adobe Photoshop ve verzi 19.0. Za pomoci dostupných nástrojů byla na snímek aplikována tzv. alfa maska, čímž se vyznačily papilární linie a celkově došlo ke zvýraznění struktury otisku. Aplikace masky je nutná pro následný postup, kdy je fotografie otisku převáděna do vektorů.

Při exportu do formátu SVG (Scalable Vector Graphics, v překladu: škálovatelná vektorová grafika) se nicméně některé papilární linie na několika místech přerušily a jiné se naopak spojily. Efekt se projevil obzvláště v centru a ve spodní třetině otisku. Tím došlo ke ztrátě několika detailů.

Problém částečně představuje kvalita sejmutého otisku prstu pomocí daktyloskopické sady. V místě jádra otisku jsou linie často spojené, což může být zapříčiněno neodborným nanesením daktyloskopického prášku. Ve výsledných testech by uvedená nedokonalost

pravděpodobně nepředstavovala problém, ale při snaze převést fotografii otisku do vektorů v požadované kvalitě je spíše nežádoucí, protože narušuje celkovou strukturu otisku.

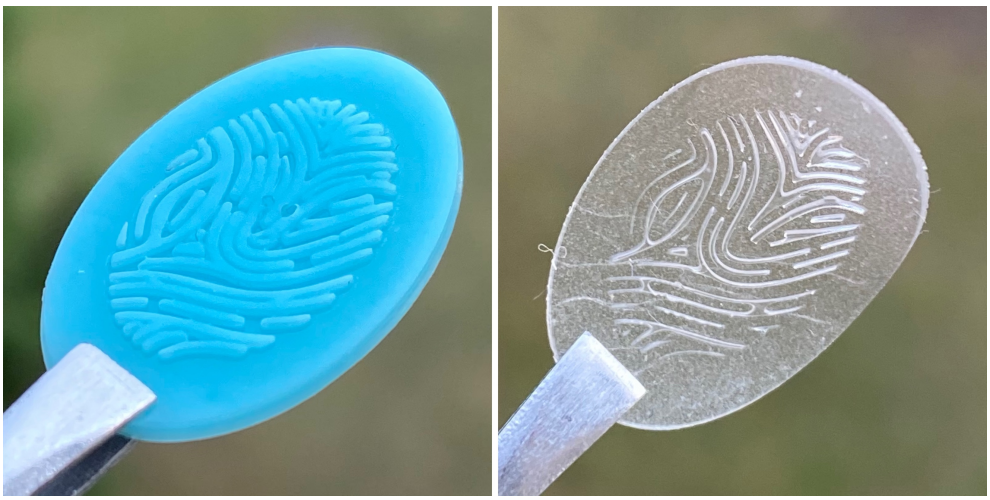
I navzdory výše popsaným nedokonalostem působil vyexportovaný otisk z obecného hlediska uceleně a některé markanty zůstaly zachovány. Po předchozí domluvě byl proto konzultován s panem Mgr. Jakubem Geyerem z Přírodovědecké fakulty Jihočeské univerzity, který se specializuje na 3D tisk. Během konzultací se dospělo k závěru, že pomocí standardní 3D tiskárny, která k tisku využívá termoplast/filament (FDM/FFF), není možné otisk vytisknout. Tiskárny tohoto typu nejsou v praxi schopné kvalitně tisknout v řádech desetin milimetrů, což je pro tisk papilárních linií bezpodmínečně nutné – linie dosahují výšky od 0,1 do 0,4 mm a šířky od 0,2 do 0,7 mm (viz kapitola 1.2).

Vzhledem k nutnosti zachytit potřebné detaily byla nakonec použita 3D tiskárna Original Prusa SL1 v hodnotě 34 990 korun, kterou Přírodovědecká fakulta před nedávnem zakoupila. Jedná se o nový typ 3D tiskárny, jež používá k tisku metodu MSLA, tedy kombinaci LCD panelu a UV diody, za pomoci kterých vytvrzuje tekutou pryskyřici do velice tenkých vrstev o výšce pouze 0,01 mm – v praxi je ale vhodnější pohybovat se o trochu výše, kolem 0,025 až 0,1 mm [17].

Díky unikátním vlastnostem tiskárny bylo možné použít dvě různé vysoce kvalitní UV fotocitlivé 405nm tekuté pryskyřice, po jejichž vytlačení vznikly výtisky se zcela odlišnými vlastnostmi. První je tvrdý, azurový, a především pak bohatší na detaily – podařilo se vytisknout většinu papilárních linií a vznikla tak kopie částečného otisku. Druhý výtisk je flexibilní a transparentní, avšak disponuje minimem detailů – vytiskly se jen části malého počtu papilárních linií, což je k analýze senzorů otisků prstů v testovaných smartphonech nedostačující. Horší vyobrazení drobných detailů je v případě tohoto typu pryskyřice jednou z negativních vlastností, což je uvedené i v popisu základních vlastností produktu [18].

Obrázek 10: Výtisk na 3D tiskárně z původní předlohy

Výsledek tisku byl nicméně z velké části ovlivněn předlohou, tedy obrazem otisku převedeného do vektorů a následně do 3D. Právě přerušení a spojení některých linií způsobilo, že výtisk na flexibilním materiálu není tak kvalitní. Z tohoto důvodu byl pro účel analýzy navržen zcela univerzální otisk, který disponuje papilárními liniemi s obecně definovanými rozměry a tvary a obsahuje několik základních markantů. Otisk je navržen tak, aby byl co největší a obsahoval tudíž co možná nejvíce detailů, ale zároveň aby ještě splňoval horní hranici rozměrů otisku z hlediska výšky, šířky i rozestupů mezi jednotlivými liniemi. Takto velký otisk bychom u člověka našli jen sporadicky, ale lze předpokládat, že snímače ve smartphonech jej budou akceptovat, a proto bude zajímavé provést analýzu, zdali jej přidají do systému a přijmou při následném pokusu o autentizaci či nikoli.



Obrázek 11: Výtisk univerzálního otisku na 3D tiskárně

5.2.2 Odlitek otisku

Druhou, z technologického hlediska jednodušší a finančně dostupnější metodu představuje vytvoření odlitku prstu. Za pomoci tavné partony a tekutého lepidla bude zkonstruována poměrně přesná kopie otisku prstu s detaily papilárních linií a některými markanty. Metoda byla zvolena zejména kvůli rychlému procesu přípravy a nízkým nákladům, kdy se cena potřebných materiálů pohybuje okolo dvě stě českých korun.

Příprava metody s sebou přináší i jistá negativa. Zejména je nutné mít k dispozici osobu, u níž se bude kopie prstu provádět. V rámci kriminalistického vyšetřování je možné otisk získat podle §114 Trestního řádu, kdy osoby spojené s vyšetřováním mají povinnost se takovému úkonu podrobit. Pokud by osoba měla v případu postavení obviněného nebo podezřelého (po sdělení podezření), je možné úkon provést i formou fyzického donucení, a to po předchozím souhlasu státního zástupce [19].

Za předpokladu, že analýza některého z testovaných senzorů skončí kladným výsledkem, pak by popsaná metoda mohla být za jistých okolností použita v rámci kriminalistické činnosti.

5.2.2.1 Vytváření odlitku

Pro vytvoření odlitku byla použita tenká hliníková fólie o tloušťce 20 mikronů, tavná patrona značky Pattex, tavná pistole Tuson a školní voděodolné lepidlo Elmer's zakoupené ze Spojených státech amerických. Materiály byly snadno dostupné – lepidlo lze z USA objednat z aukčního portálu eBay a zbylé příslušenství je k sehnání v tuzemských obchodech. Souhrnná cena materiálů činila 220 Kč.

Tabulka 1: Cena materiálů pro tvorbu odlitku

Produkt	**Cena**
Hliníková fólie	17 Kč
Tavná pistole Tuson	88 Kč
Tavná patrona Kreator	4 Kč
Lepidlo Elmer's	111 Kč
CELKEM	220 Kč

Proces výroby odlitku není nikterak složitý. Důležité je pouze přiložit prst na rozehřátý materiály ve správnou chvíli, tedy kdy má vhodnou teplotu a zároveň ideální vlastnosti k okopírování papilárních linií.

Tavnou pistolí Tuson byl nejprve roztaven jeden z konců tavné patrony a následně byl rozehřátý vzorek umístěn na hliníkovou fólii (postačil vystřižený kousek o čtvercovém půdorysu s rozměry 20 x 20 cm). Ještě do mírně rozehřátého vzorku byl položen prst otiskem směřujícím dolů. Tím byl vytvořen na detaily bohatý odlitek otisku se všemi papilárními liniemi a s velkým zastoupením markantů.

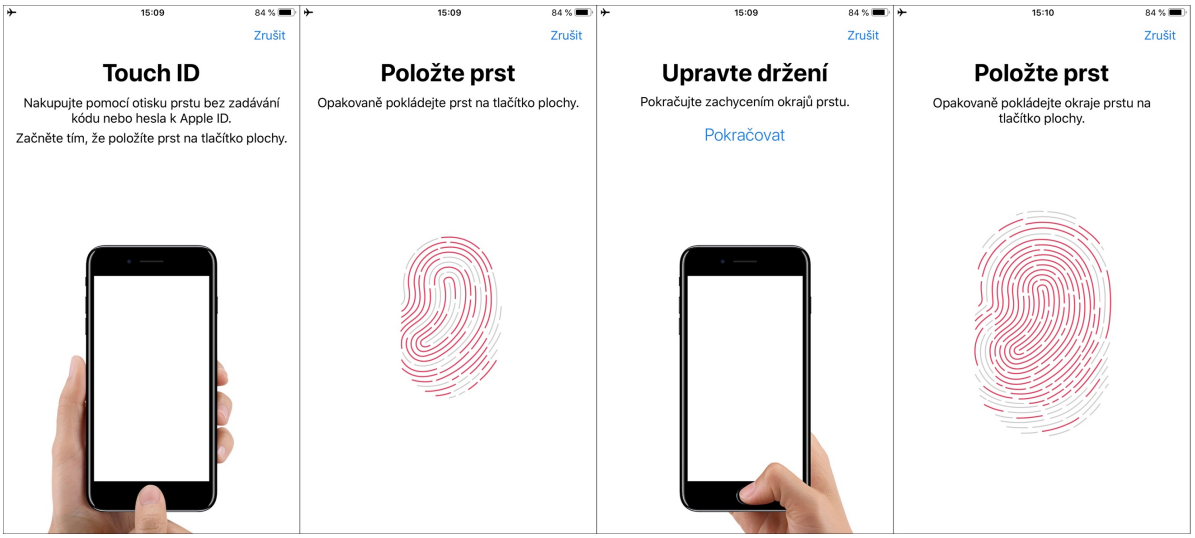
Takto odlitý otisk je zrcadlově otočený a senzor otisků prstů v telefonu by jej vyhodnotil jako nesprávný otisk. Odlitek je navíc příliš silný, a tak nemůže nabýt kapacitních vlastností. Z formy je proto potřeba vytvořit ještě jeden odlitek. Pro tyto účely bylo použito lepidlo Elmer's, jehož tenká vrstva byla nanesena na vytvořenou formu z tavné patrony. Lepidlo je potřeba rozlít, případně rozfoukat tak, abych se na původním odlitku vytvořil jen tenký povlak. Následně musí lepidlo zaschnout, což je proces trvající přibližně hodinu. Poté už je možné vrstvu sloupnout z původního odlitku – je potřeba postupovat opatrně, protože může snadno dojít k poškození vrstvy. Po úspěšném sejmutí se získá věrná kopie otisku s kýženými vlastnostmi.

Obrázek 12: Postup výroby odlitku

5.3 Analýza senzorů

5.3.1 Kapacitní

Testování kapacitního senzoru probíhalo na iPhonu 8 Plus, na kterém byl nainstalovaný v době psaní bakalářské práce nejnovější dostupný operační systém – Apple iOS 13.2. Nejprve bylo nutné do zařízení naskenovat skutečný otisk prstu. Přidání otisku se provádí v Nastavení – Touch ID a kódový zámek. Systém vyžaduje opakovaně, osmkrát přiložit prst na snímač. Následně je nutné ještě upravit držení a znovu, tentokrát šestkrát přiložit prst, aby snímač zachytil i jeho okraje a získal obraz celého otisku.



Obrázek 13: Přidání otisku na iPhone 8 Plus

Možnosti testování jsou v případě iPhonu 8 Plus, resp. iOS omezené – systém po pěti neúspěšných pokusech vyžaduje zadání přístupového hesla. Z tohoto důvodu bylo u každé testované metody provedeno pět pokusů o prolomení, což by byl i maximálně povolený počet v případě, že by se do zařízení chtěla pomocí falzifikátu dostat neoprávněná osoba.

Senzor byl analyzován celkem třemi různými typy falešných otisků – tvrdým 3D výtiskem z fotocitlivé azurové pryskyřice značky Prusa, flexibilním 3D výtiskem z pryskyřice Monocure 3D Rapid FLEX100 a odlitkem zhotoveného z lepidla Elmer's. V závislosti na použitých materiál bylo možné předpokládat i odlišné výsledky.

Při analýze tvrdým 3D výtiskem senzor nezaregistroval přiložený falzifikát. Byť jsou papilární linie na výtisku znatelné, čtečka se je ani nepokusila rozeznat, protože nezahájila proces snímání. Šlo o předpokládané chování snímače, jelikož 3D výtisk je příliš pevný, nepoddajný, a především vysoký a nemá tudíž kapacitní vlastnosti.

Analýza flexibilním 3D výtiskem byla o něco úspěšnější. Po přiložení senzor vždy zahájil snímání, protože falzifikát byl přikládán společně s prstem (jehož otisk nebyl do telefonu přidaný) a tudíž nabýval kapacitních vlastností. Nicméně vzhledem k nedokonalosti výtisku a detailů jednotlivých linií nebylo možné kapacitní senzor prolomit a všechny pokusy o odemčení skončily neúspěchem.

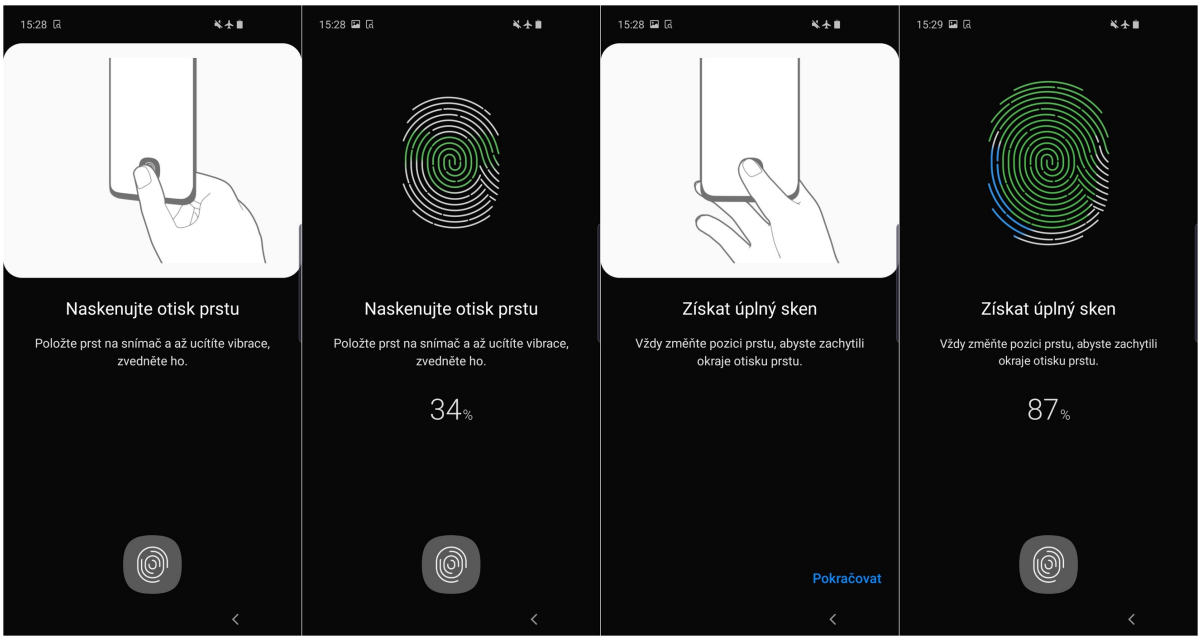
Poslední část analýzy kapacitního senzoru probíhala za pomoci odlitku, který byl také přikládán společně s prstem, jehož otisk nebyl do telefonu přidaný. Snímač ve všech případech poznal, že se jedná o otisk a zahájil snímání. Při prvních dvou pokusech odmítal falzifikovaný otisk schválit. Nakonec se ale podařilo senzor odlitkem prolomit ve třech pokusech z pěti a byl získán plný přístup do zařízení. K prolomení pomohlo, když se odlitek přilnul ke kůži prstu. Jistou roli hrály i zahřáté ruce, jež napomáhaly k vytváření potu na prstech, který se následně propíjel skrze slabou vrstvu odlitku a umožňoval tak senzoru rozeznat jednotlivé papilární linie, jež však byly jen odlité.

Pro zajištění komplexní analýzy byl kapacitní snímač podroben ještě jednomu speciálnímu testu prostřednictvím 3D výtisku univerzálního otisku s obecně definovanými rozměry a tvary (viz poslední odstavec kapitoly 4.2.1.2). Na základě poznatků z předchozích analýz byl pro tyto účely použitý pouze flexibilní výtisk z pryskyřice Monocure 3D Rapid FLEX100, protože je schopen nabýt kapacitních vlastností. Záměrem bylo nejprve přidat univerzální otisk jakožto vzor do systému a následně se jím pokusit zařízení odemknout. Případný úspěch by předznamenal, že za pomoci této metody lze snímač oklamat a že jedinou překážkou je nedostatečná kvalita původního výtisku. Nicméně již při procesu přidávání nebyl snímač schopný jednotlivé papilární linie a brázdy naskenovat. Překážkou byla tloušťka materiálu, avšak ještě tenčí výtisk již není možné na použité 3D tiskárně Original Prusa SL1 zhotovit.

5.3.2 Ultrazvukový

Testování ultrazvukového senzoru probíhalo na smartphonu Galaxy S10 od společnosti Samsung. V době psaní bakalářské práce byl na telefonu nainstalovaný nejaktuálnější systém – Google Android 9.0 s nadstavbou Samsung One UI ve verzi 1.1 – a aplikována byla i nejnovější úroveň opravy zabezpečení Android z 1. listopadu 2019.

Otisk se do telefonu přidává v Nastavení – Biometrika a zabezpečení – Otisky prstů, kde lze po zadání přístupového kódu zvolit volbu Přidat otisk prstu. Proces vyžaduje opakované přikládání prstu na vyhrazené místo displeje, pod kterým je čtečka integrovaná. Snímání v závislosti na otisku a způsobu přikládání je realizováno až patnáctkrát. Následně je nutné ještě minimálně pětkrát přiložit hrany prstu, aby systém získal kompletní 3D otisk.



Obrázek 14: Přidání otisku prstu na Galaxy S10

Také v případě nové verze systému Android jsou možnosti testování omezené. Telefon umožňuje maximálně dvacet neúspěšných pokusů snímání, přičemž po každém pátém je nutné počkat třicet sekund. Po dvacátém neúspěšném pokusu vyžaduje systém zadání přístupového hesla, což představuje jeden z nejběžnějších ochranných prvků.

Ultrazvukový senzor byl taktéž analyzován třemi různými typy falešných otisků – tvrdým 3D výtiskem z fotocitlivé azurové pryskyřice značky Prusa, flexibilním 3D výtiskem z pryskyřice Monocure 3D Rapid FLEX100 a odlitkem zhotoveného z lepidla Elmer's. I zde lze v závislosti na použitých předpokládat odlišné výsledky.

Analýza pomocí tvrdého 3D výtisku skončila negativním výsledkem. Ultrazvukový senzor nezaregistroval přiložený falzifikát a nezahájil proces snímání, ač se původně dalo

předpokládat, že vzhledem k zachyceným detailům linií na výtisku by mohl být senzor prolomen. Během analýzy bylo zjištěno, že i ultrazvukový senzor jistým způsobem ověřuje kapacitní vlastnosti přiloženého otisku, a to prostřednictvím displeje, na který je prst během snímání přikládán. I zde tedy výsledky analýzy značně ovlivnil materiál, ze kterého byl 3D výtisk otisku zhotoven.

Při analýze flexibilním 3D výtiskem ultrazvukový senzor zaregistroval přiložený otisk, ale ve všech pokusech poznal, že jde o falzifikát. Na negativním výsledku analýzy se opět podílela nedokonalost výtisku papilárních linií.

Do třetice byla ultrazvuková čtečka otisků podrobena analýze za pomoci odlitku, který byl přikládán na displej spolu s prstem, aby byl zahájen proces skenování. Snímač na odlitek zareagoval jako na otisk a zařízení se odemklo hned prvním pokusu o autentizaci. Senzor se podařilo odlitkem prolomit i navzdory jeho bezpečnostním mechanismům, které mají být schopné například detekovat průtok krve v prstu a skenovat otisk ve 3D podobě (viz kapitola 5.1.2).

Aby byla analýza komplexní a srovnatelná s analýzou kapacitního snímače, byl i v případě ultrazvukové čtečky otestován univerzální otisk. Opět byl použit flexibilní a transparentní 3D výtisk z pryskyřice Monocure 3D Rapid FLEX100. Také zde bylo nejprve nutné univerzální otisk přidat do systému jakožto předlohu a následně se pokusit jím zařízení odemknout. Proces přidávání otisku byl úspěšný a navzdory nutnosti jej přiložit na snímač celkem dvacetkrát byl ve všech případech zaznamenán. Díky tomu se univerzálním otiskem následně podařilo zařízení také odemknout, což je do značné míry zajímavý poznatek. Lze tedy předpokládat, že pokud by byl skutečný otisk dostatečně velký, byl pomocí daktyloskopické sady sejmut co možná nejpreciznějí, následně kvalitně předveden do elektronické podoby a zejména pak do vektorů s minimální ztrátou detailů, pak by se s velkou pravděpodobností podařilo zabezpečení ultrazvukového senzoru prolomit a získat přístup do zařízení.

5.4 Výsledky

Pro účely analýzy snímačů otisků prstů ve smartphonech byly navrhnuty dvě rozdílné metody – 3D otisk a odlitek prstu. Analyzovány byly dva typy senzorů – kapacitní a ultrazvukový – fungující na odlišném principu, přičemž každý z nich se nacházel na jiném smartphonu. Zařízení byla vybrána tak, aby disponovala nejnovější iterací dané technologie, a tudíž aby byly již eliminovány veškeré potencionální bezpečnostní nedostatky. Důležitý je také fakt, že telefony byly od značek Apple a Samsung, které se momentálně řadí mezi trojici

největších výrobců smartphonů na světě [20].

Navzdory nízkým pořizovacím nákladům a do jisté míry jednoduché přípravě byla při analýze obou senzorů úspěšná metoda spočívající v tvorbě odlitku otisku. Byť má tato metoda svá negativa, protože při přípravě vyžaduje přítomnost daného jedince, tak dokazuje, že oba typy senzorů jsou zranitelné, protože jejich zabezpečení lze snadno obejít pomocí falzifikovaného otisku. Dané zjištění je zajímavější ještě o to, že oba snímače mají disponovat bezpečnostními prvky (skenování subepidermální vrstvy kůže či kontrola průtoku krve v prstu), které by měly pomoci falešný otisk rozeznat. Nicméně jak z výsledku analýzy vyplývá, uvedená zabezpečení spíše nefungují, což je dáno pravděpodobně tím, že se výrobci snaží čtení otisků ve smartphonech maximálně zrychlit, aby zvýšili uživatelskou přívětivost celého mechanismu.

Druhá použitá metoda, spočívající ve tvorbě otisku na 3D tiskárně, už tolik úspěšná nebyla, i přesto ale přinesla zajímavé poznatky. Důležité je především zjištění, že pro tisk otisku se nelze spoléhat na standardní 3D tiskárnu, která využívá termoplast/filament (FDM/FFF), ale je potřeba využít nový typ 3D tiskárny, jenž tiskne pomocí metody MSLA. Předloha pro tisk musí být dostatečně kvalitní a mít co možná největší zastoupení detailů. I když se zhotovenými otisky nepodařilo prolomit ani jeden z obou testovaných senzorů, následná analýza pomocí univerzálního otisku potvrdila, že minimálně ultrazvukový senzor registruje falešný otisk jako skutečný a lze jím smartphone odemknout. Tím se opět potvrzuje, že zabezpečení daného snímače není zcela dostačující.

Tabulka 2: Analýza senzorů otisků prstů

	Kapacitní senzor	**Ultrazvukový senzor**
3D otisk (tvrdý)	Přístup zamítnut	Přístup zamítnut
3D otisk (flexibilní)	Přístup zamítnut	Přístup zamítnut
Odlitek otisku	Přístup povolen	Přístup povolen
Univerzální 3D otisk (tvrdý)	Přístup zamítnut	Přístup zamítnut
Univerzální 3D otisk (flexibilní)	Přístup zamítnut	Přístup povolen

6 Mechanismy rozpoznání obličeje

Druhou nejčastěji zastoupenou biometrickou autentizační metodou ve smartphonech je funkce rozpoznání obličeje. Ta se v chytrých telefonech poprvé objevila už v roce 2011 (ještě dříve než senzor otisků prstů), a to s příchodem systému Android 4.0. V té době ji jako první smartphone nabízel Galaxy Nexus společnosti Google. Metoda se ale příliš neujala, na čemž se z části podílela její nespolehlivost a minimální zájem jak ze strany ostatních výrobců, tak zákazníků. O dva roky později ji navíc zastínila jiná biometrická autentizační metoda spočívající ve snímání otisků prstů.

Skenování obličeje jakožto prostředek pro autentizaci uživatele se začalo ve smartphonech rozšiřovat až v posledních letech. Aktuálně touto autentizační metodou disponuje 40 % chytrých telefonů na trhu a v roce 2020 by to podle dostupné analýzy mělo být dokonce 64 %. O zásadní rozšíření mechanismu se postarala společnost Apple, která v roce 2017 představila iPhone X s funkcí zvanou Face ID – sofistikovaným systémem rozpoznání obličeje, který ke skenování používá celou řadu senzorů, včetně infračerveného projektoru a kamery. Ve snaze dohnat konkurenci začali obdobné systémy nabízet ve svých smartphonech také ostatní výrobci. Jejich mechanismy ale nejsou na takové úrovni jako zmíněné Face ID, protože ve většině případů používají ke skenování obličeje pouze přední kameru a vytvářejí si tak fotografie obličeje ve dvourozměrné podobě.

6.1 Testovaná zařízení

Pro účely analýzy byly zvoleny dva chytré telefony s ohledem na jejich výrobce, druh mechanismu a typ operační systém. Vybrány tak byly zařízení společností Apple a Samsung, jež se na trhu se smartphony řadí mezi největší výrobce. Analýze byly podrobeny nejnovější vlajkové modely těchto značek – iPhone 11 Pro a Galaxy S10 – které jsou v mnoha parametrech srovnatelné.

Cílem bylo, aby výběrem zmíněných telefonů bylo možné otestovat oba druhy mechanismu rozpoznání obličeje, tedy jak sofistikovanější metody skenování tváře ve 3D za pomoci infračerveného světla, tak i velmi rozšířeného, avšak základního systému snímání obličeje ve dvojrozměrné podobě.

6.1.1 Apple iPhone 11 Pro

Pokročilejší a bezpečnější mechanismus rozpoznání obličeje byl testován na iPhonu 11 Pro. Jedná se o nejnovější smartphone společnosti Apple, který si odbyl debut letos na podzim. Funkce rozpoznání obličeje je na telefonu označovaná jako Face ID a v případě zvoleného modelu se jedná o její vůbec nejnovější iteraci, jež dokáže snímat obličej z většího úhlu.

Face ID při snímání obličeje kombinuje data z několika senzorů, které se společně označují jako TrueDepth camera a jsou umístěny ve výřezu v horní části displeje. Kromě přední kamery je při snímání obličeje využíván také osvětlovač, infračervený bodový projektor a infračervená kamera.

Proces snímání probíhá v několika krocích. Osvětlovač nejprve nasvítí obličej infračerveným světlem, což systému pomůže detekovat tvář i za minimálního světla, nebo pokud má osoba nasazené brýle, pokrývku hlavy a podobně. Do toho bodový projektor promítá na obličej 30 000 infračervených teček, které se odráží od původního nasvícení. Ty následně snímá infračervená kamera a vytváří z nich hloubkovou mapu tváře, čímž získává naprosto přesné údaje o obličeji a zároveň detekuje značnou část mimiky.

Veškerá data jsou poté předána procesoru, konkrétně neuronovému enginu, který na základě hloubkové mapy vytvoří matematický model, který pak porovnává s uloženými údaji o obličeji.Data jsou uložena v bezpečnostní architektuře Super Enclave a jsou tak oddělena od zbytku systému a aplikací. Nezálohují se, nenahrávají se na servery a ani je nelze zpětně reprodukovat a sestavit z nich model obličeje.

Důležitým poznatkem také je, že Face ID se neustále učí, protože při každém použít znovu vytváří hloubkovou mapu tváře a všímá si změn v obličeji, například růstu vousů či makeupu. Systém funguje i v naprosté tmě.

6.1.2 Samsung Galaxy S10

Pro účely testování základní funkce rozpoznání obličeje ve smartphonech byl zvolen Galaxy S10. Telefon byl představen na začátku roku 2019 a jedná se o vlajkový model jihokorejské společnosti Samsung. Mechanismus nemá žádné specifické označení a v rámci telefonu je pojmenován pouze jako „Rozpoznávání obličeje“.

Funkce ke skenování obličeje nevyužívá speciální senzory a vystačí si pouze s předním fotoaparátem, který je umístěný ve speciálním otvoru v displeji (tzv. průstřel). Konkrétně se jedná o kameru s rozlišením 10 megapixelů, světelností f/1,9 a širokým objektivem o průměru 26 mm. Právě použitý fotoaparát je jediným benefitem Galaxy S10 oproti ostatním smartphonům, které disponují funkcí rozpoznání obličeje na stejném principu. Kamera je schopná pořídit kvalitnější snímek, který je bohatší na detaily tváře.

Při snímání se na pozadí pořídí pouze dvourozměrný snímek obličeje. Při slabém světle umí telefon dočasně zvýšit jas displeje, aby si obličej nasvítil. Snímek je následně předán procesoru a za pomoci algoritmu je ověřováno, zda se jedná o shodu s dříve naskenovanou tváří či nikoli. Vzhledem k jednoduchosti celého procesu snímání se mechanismus neumí adaptovat na změny tváře a pokud se výrazně změní vzhled uživatele, tak nemusí být jeho obličej rozpoznán.

6.2 Návrh metody

Při zkoumání možností, jak provést analýzu mechanismů rozpoznání obličeje byly brány v potaz již realizované testy zahraničních médií, případně nová zjištění, která vyžadují tuto problematiku pravidelně sledovat. Samotné mechanismy se totiž neustále vyvíjí nejen z hlediska hardwaru, ale také po softwarové stránce, tudíž výrobci můžou na nové testy rychle zareagovat a vydat opravnou aktualizaci, která změní algoritmus pro rozpoznávání tváře. Zatímco tedy na začátku roku 2019 holandská nezisková organizace Consumentenbond svým testem dokázala, že pouhou fotografií lze odemknout až 40 % smartphonů se systémem rozpoznání obličeje [22], nyní o téměř rok později už jsou některé mechanismy tohoto typu vůči tomuto triku již imunní.

Vzhledem k výše zmíněnému se nabízelo vyzkoušet o něco propracovanější způsob analýzy. Stále ale bylo účelem, aby daná metoda byla finančně nenáročná a co možná nejjednodušší, tedy aby například bylo možné použít fotografii obličeje daného uživatele, která je volně přístupná na sociálních sítích.

Za jistých okolností by se pro účely analýzy nabízela tvorba 3D masky. K tomu se ve svém testu rozhodl například zahraniční magazín Forbes, který si ale nechal masku zkonstruovat v profesionálním studiu, kde se 3D sken obličeje vytváří složením snímků z 96 digitálních zrcadlovek [23]. Vytvoření falešného obličeje je tedy finančně velmi náročné a nelze jej realizovat v běžných podmínkách.

Proto bylo potřeba zvolit střední cestu, tedy aby metoda nebyla finančně náročná a zároveň aby analýza nebyla provedena jen pomocí vytisknuté fotografie obličeje, vůči které už jsou některé mechanismy imunní. Řešením nakonec bylo zobrazení fotografie na prohnutém LCD monitoru LG38WK95C s uhlopříčkou 38 palců. Právě prohnutí displeje mělo do jisté míry simulovat 3D efekt snímku s potencionálem dané mechanismy.

Pro účel analýzy byla testovací fotografie záměrně stažena ze sociální sítě. Jednalo se o běžnou fotografii z přední kamery fotoaparátu, kde byla daná osoba zachycena z relativně blízké vzdálenosti. Podobné snímky má na sociálních sítích veřejně k dispozici většina uživatelů a pokud by tedy při následné analýze došlo k prolomení některého z mechanismů, znamenalo by to, že lze danou technologii prolomit i ne příliš kvalitním snímkem, který může mít k dispozici v podstatě kdokoli.

Nicméně aby se zvýšily šance na úspěšné prolomení mechanismů, byla fotografie ještě před provedením analýzy exportovaná do profesionálního grafického editoru Adobe Photoshop ve verzi 19.0. Zde se na snímku provedly základní úpravy, kdy se nepatrně zaostřily detaily a došlo k navýšení hodnoty kontrastu.

6.3 Analýza mechanismů

6.3.1 Face ID

Prvním testovaným mechanismem bylo Face ID na iPhonu 11 Pro, na němž byl v době psaní bakalářské práce nainstalovaný nejnovější dostupný operační systém Apple iOS 13.2. Ještě před analýzou bylo nutné do zařízení naskenovat skutečný obličej. Sken následně slouží jako předloha během snímání obličeje při pokusu o autentizaci. Obličej se přidává v Nastavení – Face ID a kód – Nastavit Face ID. Obličej je nutné nastavit do záběru a poté otáčet hlavou tak, aby byly vidět rysy tváře ze všech úhlů. Následně je potřeba ten samý proces podstoupit ještě jednou. Tím si Face ID vytvoří dva skeny obličeje, které používá jako předlohu.

Face ID má poměrně striktní pravidlo, jež omezuje počet neúspěšných pokusů skenování. Systém se uzamkne, pokud třikrát po sobě nerozezná obličej, respektive usoudí, že se neshoduje s předlohou, a odemknout jej lze pouze zadáním kódu zámku. Jde o poměrně

efektivní prvek, jak snížit pravděpodobnost prolomení. Zároveň do jisté míry omezuje proces analýzy, protože odemknutí snímkem obličeje musí být úspěšné maximálně na třetí pokus.

Samotné testování mechanismu probíhalo za denního světla, kdy byl jas monitoru nastavený na 70 %. Telefon byl před monitorem ve vzdálenosti 10-20 centimetrů a byl umístěn rovnoměrně s obrazovkou. Face ID detekuje, zdali se uživatel na telefon přímo dívá a vyžaduje tak oční kontakt. Nicméně i navzdory tomu, že byla dodržena popsaná pravidla, se nepodařilo mechanismus prolomit. Face ID dokonce fotku ani nedetekovalo jako obličej.

Negativní výsledek analýzy bylo možné předpokládat. Face ID aktuálně představuje v oblasti chytrých telefonů nejpokročilejší mechanismus pro autentizaci pomocí obličeje. Jeho hlavní výhoda spočívá v tom, že dokáže skenovat obličej ve trojrozměrné podobě, tudíž jej nelze prolomit pouhou fotografií, ač zobrazené na zahnutém monitoru.

6.3.2 Rozpoznávání obličeje Samsung

Testování druhého typu mechanismu rozpoznání obličeje probíhalo na smartphonu Samsung Galaxy S10, na kterém byl nainstalovaný nejaktuálnější systém Google Android 9.0 s nadstavbou Samsung One UI ve verzi 1.1. V zařízení byla aplikovaná nejnovější úroveň opravy zabezpečení Android z 1. listopadu 2019. Mechanismus nemá v případě daného smartphonu konkrétní jméno a samotná společnost Samsung jej označuje jako „Rozpoznávání obličeje“.

Obličej se do telefonu přidává v Nastavení – Biometrika a zabezpečení – Rozpoznávání obličeje. Hned v prvním kroku výrobce upozorňuje, že daná autentizační metoda je považována za méně bezpečnou než jiné tipy zámků, a také podotýká, že funkce nemusí tvář rozpoznat, pokud se značně změní její vzhled. V další kroku se systém ptá, zdali má uživatel nasazené brýle. Poté už se pomocí přední kamery vytvoří sken obličeje. Snímání tváře probíhá jen jednou a celý proces trvá přibližně dvě sekundy. V posledním kroku je možné mimo jiné zvolit, zda se má aktivovat rychlejší rozpoznání obličeje, čímž se sníží zabezpečení a zvýší se pravděpodobnost, že funkce rozpozná video nebo fotografii nesprávně jako obličej. Tato funkce byla pro analýzu deaktivovaná, protože cílem bylo otestovat plné zabezpečení mechanismu.

Také Samsung má u své funkce rozpoznávání obličeje pravidlo, které snižuje pravděpodobnost prolomení. Mechanismus se automaticky deaktivuje po pěti neúspěšných pokusech skenování a následně vyžaduje zadání přístupového heslo případně gesta (záleží na preferencích uživatele). Funkce je tak o něco více benevolentní než Face ID, i tak ale dané

pravidlo může ovlivnit výsledky.

Testování probíhalo za stejných podmínek jako při analýze Face ID – za denního světla a při nastaveném 70% jasu monitoru. I zde byl telefon před monitorem ve vzdálenosti 10-20 centimetrů. Nicméně rozpoznávání obličeje v podání Samsungu nedetekuje pozornost a telefon tudíž nebylo nutné umisťovat rovnoměrně s obrazovkou. Namísto toho byl mírně nakloněn tak, aby s monitorem svíral úhel přibližně 45° a zároveň byl umístěn do jeho spodní třetiny – podobně jako když uživatel drží smartphone v ruce a dívá se na obrazovku směrem dolů.

Popsaná metoda se prokázala jako efektivní. Telefon se podařilo fotografií vyobrazenou na prohnutém monitoru odemknout hned při první pokus a následně i při každém dalším. Autentizace proběhla okamžitě a mechanismus ani nedal delší prodlevou znát jakoukoli pochybnost, že by fotografii shledával za falzifikát.

Úspěšnost analýzy bylo možné vzhledem k míře zabezpečení mechanismu předpokládat, nikoli však to, že bude takto jednoduchá a že se podaří získat přístup do zařízení hned při prvním pokusu. Z velké části se na tom podílel fakt, že monitor byl mírně prohnutý, a tudíž lépe evokoval skutečný obličej.

6.4 Výsledky

Analýza mechanismů rozpoznání obličeje ve smartphonech probíhala za pomoci jedné metody. K její realizaci se dospělo zjišťováním různých poznatků z ostatních testů a byla upravena tak, aby měla pravděpodobnost úspěchu a zároveň aby nebyla finančně náročná. Analýzou byly podrobeny dva typy mechanismů rozpoznání obličeje – Face ID (trojrozměrné snímání) a Rozpoznávání obličeje Samsung (dvojrozměrné snímání) – a byly zvoleny proto, že fungují na odlišném principu, a že se nachází na vlajkových smartphonech společností, patřící mezi největší výrobce chytrých telefonů na světě [20], jež používají rozdílné operační systémy.

Provedená analýza potvrdila předpoklad ohledně míry zabezpečení jednotlivých mechanismů rozpoznání obličeje. Face ID je pokročilý systém, který pro snímání obličeje používá několik senzorů, především infračervený bodový projektor a infračervenou kameru, díky čemuž je schopný zaznamenat podrobný sken tváře ve 3D. Právě vzhledem k propracovanosti celého mechanismu se nepodařilo Face ID prolomit pomocí fotografie, byť byla vyobrazena na prohnutém monitoru. Od roku 2017, kdy Apple Face ID představil, se zabezpečení celého systému podařilo prolomit pouze jednou, a to za pomoci speciálně

vytvořené 3D masky, jejíž zhotovení vyžadovalo investici přibližně 5 tisíc korun [24]. Od té doby se podobný úspěch nepodařilo zopakovat [23].

Naproti tomu rozpoznání obličeje Samsung u smartphonu Galaxy S10 nikterak vysokou míru bezpečné nenabízí, což potvrdila i provedená analýza. Mechanismus se podařilo prolomit hned při prvním pokusu pouhou fotografií na prohnutém monitoru. Snímek byl navíc stažen ze sociální sítě, kde při nahrávání prochází kompresí, a kam si většina uživatelů veřejně umisťuje své fotografie, jež mohou být následně zneužity k podobným účelům. I když Samsung na možná bezpečnostní rizika upozorňuje už během procesu přidávání obličeje, je nežádoucí, aby se takto minimálně zabezpečený autentizační mechanismus v telefonu vůbec nacházel, obzvlášť vezmeme-li v potaz, že jde o vlajkový model největšího výrobce smartphonů.

7 Ostatní biometrické autentizační mechanismy

Některé smartphony disponují i jinými autentizačními mechanismy, než čtení otisku prstu nebo rozpoznání obličeje. Jejich výskyt je ale sporadický a některé dokonce nabízí pouze jeden chytrý telefon na trhu. Od jiných se naopak upustilo kvůli jejich uživatelské nepřívětivosti.

7.1 Skener oční duhovky

Krátce před rozšířením funkce skenování obličeje působila velice slibně metoda skenování oční duhovky. Tu jako první výrobce nabídl Microsoft v telefonu Lumia 950, který byl představený v roce 2015. O rok později se funkce zvaná Iris Scanner rozšířila především zásluhou společnosti Samsung, který ji integroval do telefon Galaxy Note 7 a poté také do dalších svých vlajkových modelů.

Mechanismus funguje na podobném principu jako funkce rozpoznání obličeje ve 3D. Duhovka se skenuje za pomoci senzoru vyzařujícího infračervené světlo. Díky tomu je tak schopná provést autentizaci i v naprosté tmě nebo například skrze brýle.

Ostatní výrobci smartphonů ani vývojáři aplikací ale skeneru oční duhovky nevěnovali přílišnou pozornost, a proto se od implementace tohoto typu biometrické autentizace začalo postupně opouštět. Samsung ji letos dokonce přestal do svých telefonů integrovat a začal se více spoléhat na funkci rozpoznání obličeje.

Skener oční duhovky v rámci bakalářské práce nebyl podroben analýze, protože realizace metody sloužící k potencionálnímu prolomení je finančně náročná, jelikož vyžaduje koupi nákladného fotoaparátu se schopností pořídit snímek za pomoci infračerveného světla. Právě o to se v roce 2017 pokusili vědci z Chaos Computer Club, kteří speciální snímek následně upravili, vytiskli na 3D tiskárně a na kopii očí přiložili kontaktní čočky [25]. Zabezpečení skeneru oční duhovky se tímto způsobem podařilo prolomit na Galaxy S8. Samsung se nicméně později k celé záležitosti vyjádřil se slovy, že výše popsané by bylo možné pouze za velmi vzácného souběhu několika okolností [26].

7.2 Skener krevního řečiště

Úplnou novinkou na poli biometrických autentizačních mechanismů ve smartphonech je skenování krevního řečiště v dlani. Funkci letos v červenci představila společnost LG jako jeden ze způsobů, jak se uživatel může autentizovat při odemykání telefonu.

Mechanismus je označován jako HandID a nachází se v chytrém telefonu LG G8S ThinQ. Skenování krevního řečiště v dlani probíhá pomocí infračerveného světla, které vyzařují a snímají senzory, jež jsou součástí systému Z Camera.

Jedná se o pokročilou autentizační metodu, kterou se zatím nepodařilo prolomit a vzhledem k aktuálnosti novinky ani neexistují informace, že by se o to někdo pokusil. Replikovat stavbu krevního řečiště v dlani je složité a vytvořit falzifikát alespoň s minimální pravděpodobností úspěšnosti je za pomoci cenově dostupných materiálů a základního vybavení nemožné. Analýza tohoto nového biometrického autentizačního mechanismu nebyla zrealizovaná i vzhledem k faktu, že testovací zařízení stojí 11 tisíc korun.

Závěr

Bakalářské práce byla zaměřena na analýzu biometrických mechanismů smartphonů. Cílem práce bylo navrhnout a zrealizovat metody k analýze snímačů otisk prstů a funkcí skenování obličeje používaných v chytrých telefonech.

Teoretická část bakalářské práce je vymezena tématům zabývající se historií klasifikací otisků prstů, stavbou papilárních linií v rámci lidské kůže, zařazení otisků do specifických tříd, popsáním markantů a detailů. Druhým tématem, které tvoří teoretický rámec práce, je charakteristika senzorů otisků prstů používaných ve smartphonech. Pozornost je věnována rozdílům mezi kapacitním a ultrazvukovým snímačem. Shrnuty jsou také základní charakteristiky mechanismů rozpoznání obličeje.

Předmětem praktické části bakalářské práce je shrnutí konkrétních specifikací dvou analyzovaných senzorů a mechanismů rozpoznání obličeje, kterými disponují vybraná zařízení. Další část byla věnována návrhu a realizaci metod aplikovaných při analýze senzorů a funkcí detekce tváře. Zrealizovat se podařilo všechny metody.

Výsledky získané prostřednictvím analýzy biometrických mechanismů chytrých telefonů v podobě senzorů otisků prstů vykazují zranitelnost u kapacitního i ultrazvukového snímače, a to jak vytvořeným odlitkem prstu, tak v případě ultrazvukového senzoru také prostřednictvím univerzálního otisku zhotoveného na 3D tiskárně.

Výsledkem analýzy biometrických mechanismů pro rozpoznání obličeje je závěr, že základní systém pro snímání tváře ve dvourozměrné podobně pomocí přední kamery je zranitelný a lze jej snadno prolomit pomocí upravené fotografie zobrazené na prohnutém monitoru. Naproti tomu systém Face ID, který obstarává trojrozměrné snímání tváře za pomoci infračerveného světla, nevykazuje podle provedené analýzy zranitelnost

Seznam použité literatury

[1] KOCHETKOVA, Kate. Mobile fingerprint sensors: more or less secure?. *Kaspersky Lab* [online]. 2016 [cit. 2016-05-15]. Dostupné z: https://www.kaspersky.com/blog/fingerprints-sensors-security/10951/

[2] JEDLIČKA, Miroslav. Kriminalistická daktyloskopie. *Kriminalistika* [online]. [cit. 2019-04-15]. Dostupné z: http://kriminalistika.eu/daktyl/daktyl.html

[3] SAMS, C. Journal of the Forensic Science Society: Thomas Bewick—His Mark. Issue 4. England: Elsevier, 1975. ISBN 0015-7368.

[4] GRZYBOWSKI, Andrzej. Clinics in Dermatology: Jan Evangelista Purkynje (1787–1869): First to describe fingerprints [online]. 2015 [cit. 2019-04-16]. Dostupné z: https://www.sciencedirect.com/science/article/pii/S0738081X14001539

[5] TREDOUX, Gavan. Henry Faulds: the Invention of a Fingerprinter [online]. 2003 [cit. 2019-04-16]. Dostupné z: http://galton.org/fingerprints/faulds.htm

[6] BLISS, Don. Skin Anatomy. In: National Cancer Institute [online]. May 26, 2010 [cit. 2016-05-15]. Dostupné z: https://visualsonline.cancer.gov/details.cfm?imageid=4604

[7] SHOEWU, Oluwagbemiga a N. T. MAKANJUOLA. Biometric-based Attendance System: LASU Epe Campus as Case Study. In: ResearchGate [online]. January 2014 [cit. 2016-04-30]. Dostupné z: https://www.researchgate.net/publication/326493967_Biometric-based_Attendance_System_LASU_Epe_Campus_as_Case_Study

[8] SABATINL, Matthew. Face Unlock — Android 4.0 Ice Cream Sandwich 4.0's Most Personal Feature. *Androidauthority* [online]. October 21, 2011 [cit. 2019-12-11]. Dostupné z: https://www.androidauthority.com/face-unlock-android-4-0-ice-cream-sandwich-most-personal-feature-27693/

[9] NAIYA, Pavel. More than one billion smartphones to feature facial recognition in 2020. *Counterpoint Research* [online]. February 7, 2018 [cit. 2019-12-11]. Dostupné z: https://www.counterpointresearch.com/one-billion-smartphones-feature-face-recognition-2020/

[10] Apple unveils iPhone X. In: Youtube [online]. 12. 9. 2017 [cit. 2019-11-20]. Dostupné z: https://youtu.be/aEoVcYQ8caM. Kanál uživatele Global News

[11] About Face ID advanced technology: Learn how Face ID helps protect your information on your iPhone and iPad Pro. Apple [online]. October 29, 2019 [cit. 2019-11-30]. Dostupné z: https://support.apple.com/en-us/HT208108

[12] Apple Special Event. September 10, 2013 In: Youtube [online]. 8.10.2013 [cit. 2018-05-25]. Dostupné z: https://youtu.be/yBX-KpMoxYk. Kanál uživatele Apple

[13] BREWER, Teresa a Natalie KERRIS. Apple Announces iPhone 5s—The Most Forward-Thinking Smartphone in the World [online]. September 10, 2013 [cit. 2018-5-25]. Dostupné z: https://www.apple.com/newsroom/2013/09/10Apple-Announces-iPhone-5s-The-Most-Forward-Thinking-Smartphone-in-the-World/

[14] Feast Your Eyes on the Future: The Galaxy S10's Stunning Display: Beefed-Up Biometric Security. *Samsung Newsroom* [online]. February 21, 2019 [cit. 2019-03-16]. Dostupné z: https://news.samsung.com/global/in-depth-look-1-feast-your-eyes-on-the-future-the-galaxy-s10s-stunning-display

[15] CHENG, Francisco. Samsung Galaxy S10 taps Qualcomm 3D Sonic Sensor for top-notch security and accuracy. *OnQ Blog* [online]. February 20, 2019 [cit. 2019-03-16]. Dostupné z: https://www.qualcomm.com/news/onq/2019/02/20/samsung-galaxy-s10-taps-qualcomm-3d-sonic-sensor-top-notch-security-and-accuracy

[16] PRŮŠA, Josef. Představujeme Original Prusa SL1 – novou open-source SLA 3D tiskárnu. *Josefprusa* [online]. 25. 09. 2018 [cit. 2019-12-10]. Dostupné z: https://josefprusa.cz/original-prusa-sl1-nova-sla-3d-tiskarna/

[17] Transparentní pryskyřice flexibilní. *Shop.prusa3d* [online]. [cit. 2019-12-10]. Dostupné z: https://shop.prusa3d.com/cs/resiny/1000-transparentni-pryskyrice-flexibilni-1kg.html

[18] Zákon č. 141/1961 Sb., trestní řád, ve znění pozdějších předpisů. Prohlídka těla a jiné podobné úkony, § 114.

[19] HOLST, Arne. Global market share held by leading smartphone vendors from 4th quarter 2009 to 3rd quarter 2019. *Statista* [online]. Nov 11, 2019 [cit. 2019-12-11]. Dostupné z: https://www.statista.com/statistics/271496/global-market-share-held-by-smartphone-vendors since-4th-quarter-2009/

[20] Original Prusa SL1. *Prusa3d* [online]. 2019 [cit. 2019-12-11]. Dostupné z: https://www.prusa3d.cz/original-prusa-sl1/

[21] Stavebnice 3D tiskárny Original Prusa i3 MK3S. *Shop.prusa3d* [online]. [cit. 2019-12-11]. Dostupné z: https://shop.prusa3d.com/cs/3d-tiskarny/180-stavebnice-3d-tiskarny-original-prusa-i3-mk3s.html

[22] KULCHE, Peter. Gezichtsherkenning op smartphone niet altijd veilig. *Consumenten bond* [online]. April 15, 2019 [cit. 2019-12-11]. Dostupné z: https://www.consumentenbond.nl/veilig-internetten/gezichtsherkenning-te-hacken

[23] BREWSTER, Thomas. We Broke Into A Bunch Of Android Phones With A 3D-Printed Head. *Forbes* [online]. December 13, 2018 [cit. 2019-12-11]. Dostupné z: https://www.forbes.com/sites/thomasbrewster/2018/12/13/we-broke-into-a-bunch-of-android-phones-with-a-3d-printed-head/#5d0559d41330

[24] Bkav's new mask beats Face ID in "twin way": Severity level raised, do not use Face ID in business transactions [online]. 10-11-2017 [cit. 2019-12-11]. Dostupné z: https://www.bkav.com/top-news/-/view-content/65202/bkav-s-new-mask-beats-face-id-in-twin-way-severity-level-raised-do-not-use-face-id-in-business-transactions

[25] Chaos Computer Clubs breaks iris recognition system of the Samsung Galaxy S8 [online]. 2017 [cit. 2019-12-1]. Dostupné z: https://www.ccc.de/en/updates/2017/iriden

[26] Samsung se vyjádřil k prolomení čtečky oční duhovky Galaxy S8 [online]. 2017 [cit. 2019-12-1]. Dostupné z: https://samsungmagazine.eu/2017/05/25/samsung-se-vyjadril-k-prolomeni-ctecky-ocni-duhovky-galaxy-s8/

Seznam tabulek

Seznam obrázků