Srovnání bezpečnosti vybraných operačních systémů mobilních komunikačních zařízení

Lukáš Konečný

Bakalářská práce
2020

Univerzita Tomáše Bati ve Zlíně
Fakulta logistiky a krizového řízení

Univerzita Tomáše Bati ve Zlíně
Fakulta logistiky a krizového řízení
Ústav ochrany obyvatelstva

Akademický rok: 2019/2020

ZADÁNÍ BAKALÁŘSKÉ PRÁCE
(projektu, uměleckého díla, uměleckého výkonu)

Jméno a příjmení:	**Lukáš Konečný**
Osobní číslo:	**L17193**
Studijní program:	**B2825 Ochrana obyvatelstva**
Studijní obor:	**Ochrana obyvatelstva**
Forma studia:	**Prezenční**
Téma práce:	**Srovnání bezpečnosti vybraných operačních systémů mobilních komunikačních zařízení**

Zásady pro vypracování

1. Zpracujte rešerši současného stavu předmětné problematiky.
2. Analyzujte bezpečnost vybraných operačních systémů mobilních komunikačních zařízení.
3. Proveďte komparaci vybraných operačních systémů mobilních komunikačních zařízení z hlediska bezpečnosti.
4. Sumarizujte získané výsledky a identifikujte nejbezpečnější operační systém mobilních komunikačních zařízení.

Rozsah bakalářské práce:
Rozsah příloh:
Forma zpracování bakalářské práce: **tištěná/elektronická**

Seznam doporučené literatury:

1. JIRÁSEK, Petr, Luděk NOVÁK a Josef POŽÁR. *Výkladový slovník kybernetické bezpečnosti: Cyber security glossary.* Třetí aktualizované vydání. Praha: Policejní akademie ČR v Praze, 2015. ISBN 978-80-7251-436-6.
2. KOLOUCH, Jan. *Cybercrime.* Praha: CZ.NIC, z.s.p.o., 2016. CZ.NIC. ISBN 978-80-88168-15-7.
3. KOLOUCH, Jan a Pavel BAŠTA. *CyberSecurity.* Praha: CZ.NIC, z.s.p.o., 2019. ISBN 978-80-88168-31-7.

Další odborná literatura dle doporučení vedoucího bakalářské práce.

Vedoucí bakalářské práce: **Ing. Petr Svoboda**
Ústav ochrany obyvatelstva

Datum zadání bakalářské práce: **1. listopadu 2019**
Termín odevzdání bakalářské práce: **15. května 2020**

L.S.

doc. Ing. Zuzana Tučková, Ph.D.
děkanka

prof. Ing. Dušan Vičar, CSc.
ředitel ústavu

V Uherském Hradišti dne 2. prosince 2019

PROHLÁŠENÍ AUTORA BAKALÁŘSKÉ PRÁCE

Beru na vědomí, že:

- bakalářská práce bude uložena v elektronické podobě v univerzitním informačním systému a dostupná k nahlédnutí;
- na moji bakalářskou práci se plně vztahuje zákon č. 121/2000 Sb. o právu autorském, o právech souvisejících s právem autorským a o změně některých zákonů (autorský zákon) ve znění pozdějších právních předpisů, zejm. § 35 odst. 3;
- podle § 60 odst. 1 autorského zákona má Univerzita Tomáše Bati ve Zlíně právo na uzavření licenční smlouvy o užití školního díla v rozsahu § 12 odst. 4 autorského zákona;
- podle § 60 odst. 2 a 3 autorského zákona mohu užít své dílo – bakalářskou práci nebo poskytnout licenci k jejímu využití jen s předchozím písemným souhlasem Univerzity Tomáše Bati ve Zlíně, která je oprávněna v takovém případě ode mne požadovat přiměřený příspěvek na úhradu nákladů, které byly Univerzitou Tomáše Bati ve Zlíně na vytvoření díla vynaloženy (až do jejich skutečné výše);
- pokud bylo k vypracování bakalářské práce využito softwaru poskytnutého Univerzitou Tomáše Bati ve Zlíně nebo jinými subjekty pouze ke studijním a výzkumným účelům (tj. k nekomerčnímu využití), nelze výsledky bakalářské práce využít ke komerčním účelům;
- pokud je výstupem bakalářské práce jakýkoliv softwarový produkt, považují se za součást práce rovněž i zdrojové kódy, popř. soubory, ze kterých se projekt skládá. Neodevzdání této součásti může být důvodem k neobhájení práce.

Prohlašuji,

- že jsem na bakalářské práci pracoval samostatně a použitou literaturu jsem citoval. V případě publikace výsledků budu uveden jako spoluautor.
- že odevzdaná verze bakalářské práce a verze elektronická nahraná do IS/STAG jsou obsahově totožné.

V Uherském Hradišti, dne: 15. 5. 2020

Jméno a příjmení studenta: Lukáš Konečný

.....
podpis studenta

ABSTRAKT

Tato bakalářská práce se zaměřuje na porovnání bezpečnosti vybraných operačních systémů mobilních komunikačních zařízení. Teoretická část se zabývá základními pojmy a legislativou související s touto problematikou, poté je vytvořen seznam operačních systémů. Cílem teoretické části je také stručná strukturální analýza vybraných operačních systémů s definováním aktuálních zranitelností těchto operačních systémů. Cílem praktické části je analýza zabezpečení s využitím multikriteriální analýzy pro srovnání bezpečnosti vybraných operačních systémů a identifikace nejbezpečnějšího operačního systému mobilních komunikačních zařízení a základních možností zabezpečení těchto operačních systémů.

Klíčová slova: android, bezpečnost, ios, mobilní, operační systém, zařízení

ABSTRACT

That bachelor thesis focuses on the security comparison of selected operating systems of mobile communication devices. The theoretical part deals with basic terms and the legislation related to this issue, then is created a list of operating systems. The theoretical part also aims at providing a brief structural analysis of chosen operating systems with defining vulnerabilities of these operating systems. The practical part goal is to come up with security analysis and use of a multi-criteria analysis for comparison of the security of selected operating systems and identify the most secure operating system of mobile communication devices and basic security options for these operating systems.

Keywords: android, security, ios, mobile, operating system, device

Rád bych poděkoval svému vedoucímu Ing. Petru Svobodovi, Ph.D. za cenné rady, jeho ochotu a věnovaný čas. Velké díky patří také mé rodině za možnost studovat a jejich podporu po celou dobu studia.

Prohlašuji, že odevzdaná verze bakalářské práce a verze elektronická nahraná do IS/STAG jsou totožné.

OBSAH

ÚVOD

V dnešní době je mobilní zařízení nedílnou součástí našeho života, kterou používáme k usnadnění naší práce, či k udržení kontaktu s blízkými anebo jen pro zábavu. Na tato zařízení ukládáme různá citlivá data, jakými mohou být např. přihlašovací údaje, telefonní čísla, přihlašovací kódy k internetovému bankovnictví apod.

Ovšem i mobilní zařízení mohou být napadena útočníky. Tímto způsobem můžeme nešťastně přijít o drahocenná citlivá data, nebo naše finanční prostředky.

Jedním z hlavních článků pro zajištění bezpečnosti mobilních zařízení jsou operační systémy, které jsou nainstalované na mobilních zařízeních už z výroby. O udržování a zvyšování bezpečnosti se starají samotní výrobci těchto operačních systémů, ale nedílnou součástí jsme také my, takže musíme dbát co nejvíce na to, aby naše zařízení mělo nejvyšší šanci odolávat případným únikům dat. K zvýšení zabezpečení slouží různé bezpečnostní funkce a služby třetích stran.

V práci byla nejvíce využita metoda sběru dat a informací. Další metodou bylo pozorování a následný vědecký popis při kterém byl kladen důraz na správnost a vhodnost volby pojmů, úplnost záznamů a objektivitu. Metodou explanace bylo zjištěno, jakým způsobem může být zařízení napadeno. Dále byla použita analýza pro zjištění úrovně zabezpečení operačních systémů, a poté komparace pro porovnání této úrovně zabezpečení.

Bakalářská práce si klade za cíl zpracování rešerše a definici základních pojmů a legislativy týkající se předmětné problematiky. Dalšími cíli jsou identifikace současných operačních systémů mobilních komunikačních zařízení a vytvoření soupisu těchto operačních systémů, následně analýza struktury vybraných operačních systémů a pojednání o jejich zranitelnostech.

Cílem praktické části je analýza zabezpečení operačních systémů s využitím multikriteriální analýzy. Ta bude sloužit pro srovnání bezpečnosti vybraných operačních systémů identifikaci nejbezpečnějšího operačního systému mobilních komunikačních zařízení. Na závěr budou zmíněny základní možnosti zabezpečení těchto operačních systémů.

I. TEORETICKÁ ČÁST

1 ZÁKLADNÍ POJMY A PRÁVNÍ NORMY

Pro pochopení problematiky bezpečnosti operačních systémů mobilních komunikačních zařízení je nejprve nutné vysvětlit některé základní pojmy a uvést základní právní normy týkající se této oblasti.

1.1 Základní pojmy

V následující podkapitole se pokusím vybrat ty nejzákladnější a nejvhodnější základní pojmy které se týkají této problematiky.

Autenticita

Vlastnost, která nám říká že entita je tím, za co se prohlašuje, podobně jako autentizace. (Jirásek, Novák a Požár, 2015)

Autentizace

Jedná se o záruku, která nám říká, že prohlašovaná charakteristika, osoba nebo jakýkoliv subjekt je správný nebo je za toho za koho se vydává, po autentizaci následuje autorizace. (Jirásek, Novák a Požár, 2015) (Autentizace, ověření, identifikace (Authentication), 2018)

Autorizace

Udělení práv, které zahrnuje umožnění přístupu k informacím nebo k nějakému úkonu či operaci, na základě přístupových práv. Po udělení práv následuje autentifikace. (Jirásek, Novák a Požár, 2015) (Autorizace, oprávnění (Authorization), 2017)

Autentifikace

Proces, který ověří identitu osoby nebo zařízení. Po zadání přihlašovacích údajů systém ví, kdo jsme a zda jsme to skutečně my. (Authentication, 2018)

Bezpečnost

Jedná se o vlastnost prvku např. informačního systému, který je na určité úrovni chráněn proti ztrátám, nebo také stav ochrany na určité úrovni proti ztrátám. Bezpečnost informačních technologií zahrnuje ochranu důvěrnosti, integrity a dosažitelnosti při zpracování, úschově, následné distribuci a prezentaci těchto informací. (Jirásek, Novák a Požár, 2015)

Bezpečnost informací

Uplatnění základních bezpečnostních opatření a postupů, které slouží k:

- Ochraně informací před jejich možnou ztrátou nebo kompromitací (ztráta důvěrnosti, integrity, autentičnosti, odpovědnosti, nepopíratelnosti a spolehlivosti), případně k jejich zajištění a přijetí nápravných opatření.
- Zachování dostupnosti informací a schopnosti s těmito informacemi pracovat v rozsahu přidělených oprávnění.

Tyto opatření zahrnují bezpečnost počítačů, přenosu, emisí, šifrovací bezpečnost a odhalování možných ohrožení těchto systémů a jejich předcházení. (Jirásek, Novák a Požár, 2015) (Čermák, 2011)

Bezpečnost komunikací

Použití bezpečnostních opatření v komunikacích znemožní neoprávněným osobám získat důležité informace, které lze získat z přístupu k této komunikaci a z jejího vyhodnocení, nebo které zajistí požadovanou autentičnost této komunikace. (Jirásek, Novák a Požár, 2015)

Informační a komunikační technologie

Pod pojmem informační a komunikační technologie si může představit veškerou techniku, která se zabývá zpracováním a přenosem informací a tím zpravidla bývá výpočetní a komunikační technika a její programové vybavení. (Jirásek, Novák a Požár, 2015)

Mobilní zařízení

Zpravidla každé přenosné elektronické zařízení, obvykle s dotykovým displejem a možností připojení na internet, které má operační systém.

Operační systém

Jedná se o programový prostředek, který nám dovoluje ovládat zařízení, řídí operace programů nebo aplikací, které mohou poskytovat různé služby, např. přidělování prostředků, rozvrhování, řízení vstupů a výstupů a správu dat. Je v činnosti od prvního zapnutí zařízení až po jeho vypnutí. (Jirásek, Novák a Požár, 2015)

Kybernetický prostor

Je digitální prostředí, které umožňuje vznik, zpracování a vzájemnou výměnu informací, tvořené informačními systémy, službami a sítěmi elektronických komunikací. Na tento prostor mohou být cíleny také nežádoucí útoky proti zájmům jiné osoby. (Jirásek, Novák a Požár, 2015) (Kolouch a Bašta, 2019)

Kybernetický útok

Tento útok můžeme definovat jako útok na IT infrastrukturu za účelem způsobit poškození a odcizení citlivých, strategicky důležitých informací a to např. osobních údajů, nežádoucí spam apod. (Jirásek, Novák a Požár, 2015) (Kolouch a Bašta, 2019)

Osobní údaj

Osobní údaj je jakákoliv informace o známém nebo rozeznatelném subjektu, které se k němu vztahují.

Mezi obecné osobní údaje se řadí:

- Jméno a příjmení.
- Pohlaví.
- Věk.
- Datum narození.
- Osobní stav.
- IP adresa a fotografie.

Citlivými osobními údaji se zabývá obecné nařízení o ochraně osobních údajů GDPR. (Škorničková, 2018)

Citlivé osobní údaje

„Citlivé osobní údaje jsou speciální kategorií podle GDPR, která zahrnuje údaje o rasovém či etnickém původu, politických názorech, náboženském nebo filozofickém vyznání, členství v odborech, o zdravotním stavu, sexuální orientaci a trestních deliktech či pravomocném odsouzení osob. Tyto údaje mohou subjekt údajů samy osobě poškodit ve společnosti, v zaměstnání, ve škole či mohou zapříčinit jeho diskriminaci. Do kategorie citlivých údajů GDPR nově zahrnuje genetické a biometrické údaje. Zpracování citlivých osobních údajů podléhá mnohem přísnějšímu režimu, než je tomu u obecných údajů.“ (Škorničková, 2018)

1.2 Základní právní normy

V souvislosti s kybernetickou trestnou činností a kybernetickou bezpečností je nutné uvést i základní právní normy, které se týkají této problematiky:

- ***Zákon č. 181/2014 Sb., o kybernetické bezpečnosti a o změně některých souvisejících zákonů (zákon o kybernetické bezpečnosti).***

  V zákoně jsou uvedeny povinnosti subjektů ve vztahu ke kybernetické bezpečnosti, dále požadavky na bezpečnost informačních a komunikačních technologií apod.

- ***Vyhláška č. 82/2018 Sb., vyhláška o bezpečnostních opatřeních, kybernetických incidentech, reaktivních opatřeních, náležitostech podání v oblasti kybernetické bezpečnosti a likvidaci dat (vyhláška o kybernetické bezpečnosti).***

  Vyhláška se podrobně věnuje náležitostem ohledně bezpečnostních opatřeních, bezpečnostních incidentech a také v neposlední řadě likvidaci dat apod.

- ***Zákon č. 127/2015 Sb., o elektronických komunikacích.***

  Zákon upravuje na základě práva Evropské unie podmínky pro podnikání a výkon státní správy, dále regulaci trhu v oblasti elektronických komunikací apod.

- ***Zákon č. 101/2000 Sb., o ochraně osobních údajů.***

  Tento zákon se zabývá naplnění práva každého na ochranu osobních údajů před neoprávněným zasahováním do soukromí, dále upravuje práva a povinnosti při zpracování osobních údajů apod. (Kolouch, 2016)

V této kapitole nebylo cílem uvést konečný výčet všech zákonů a základních pojmů, které se dotýkají této problematiky, ale uvést ty nejdůležitější. V následující kapitole bude proveden soupis operačních systémů mobilních komunikačních zařízení.

2 SOUPIS MOBILNÍCH OPERAČNÍCH SYSTÉMŮ

Dnešní mobilní komunikační zařízení obsahují už od výroby předem předinstalovaný operační systém. V této kapitole bude vytvořen seznam těchto operačních systémů. Následně je stručně charakterizuji a vytvořím graf procentuálního zastoupení jednotlivých operačních systémů na zařízeních.

Mobilních operačních systémů je celá řada, ale zde bude vypsáno několik nejznámějších operačních systémů. Dále se bude následující kapitola zaměřovat na dva nejpoužívanější operační systémy a ty se pokusím více probrat.

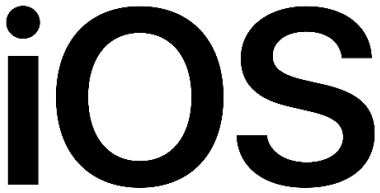
2.1 Android (Google)

Operační systém Android je vyvíjen společností Google jako open-source, což je program s otevřeným zdrojovým kódem, který lze upravovat podle potřeby výrobce zařízení. K jádru operačního systému také patří další software a tou je Middleware nebo česky někdy označován jako „softwarové lepidlo“ (jedná se o software, který poskytuje další služby namísto pouze původních integrovaných v jádru operačního systému), a také předem nainstalované aplikace, které slouží k základnímu používání zařízení. Jednotlivé verze Androidu se označují odvozeninami různých desertů, jako jsou například: Cupcake, Donut, Ice Cream Sandwich apod., kde každý nový název další verze systému má začáteční písmeno podle následujícího písmena dle abecedy, a přináší samozřejmě novinky a vylepšení. V dnešní době se jedná o nejrozšířenější operační systém mobilních komunikačních zařízení. (Beal, 2011)

Obrázek 1: Nové logo Androidu (Armin, 2019)

2.2 iOS (Apple)

iOS je operační systém vyvíjený společností Apple. Původně byl vytvořen pouze pro iPhone zařízení, ale později se rozšířil i na další zařízení jakými jsou např. iPad, iPod Touch apod. Tento operační systém na rozdíl od Androidu je určen pouze pro zařízení od společnosti Apple, nikoliv pro zařízení třetí strany. Apple iOS je odvozen od operačního systému Mac OS X. Jedná se o jeden z nejpoužívanějších operačních systémů. (Beal, 2011)



Obrázek 2: Logo iOS (IOS logo, c2016-2019)

2.3 Windows Phone (Microsoft)

Windows Phone je operační systém od společnosti Microsoft používaný v chytrých telefonech a mobilních zařízeních s dotykovými displeji anebo i bez něj. Tento systém tak jako Android mohou používat výrobci chytrých zařízení třetích stran. Aktuálně se tento operační systém už nepoužívá, stále ho ale můžeme najít na starších od společnosti Microsoft. (Beal, 2011)

2.4 Symbian (Nokia)

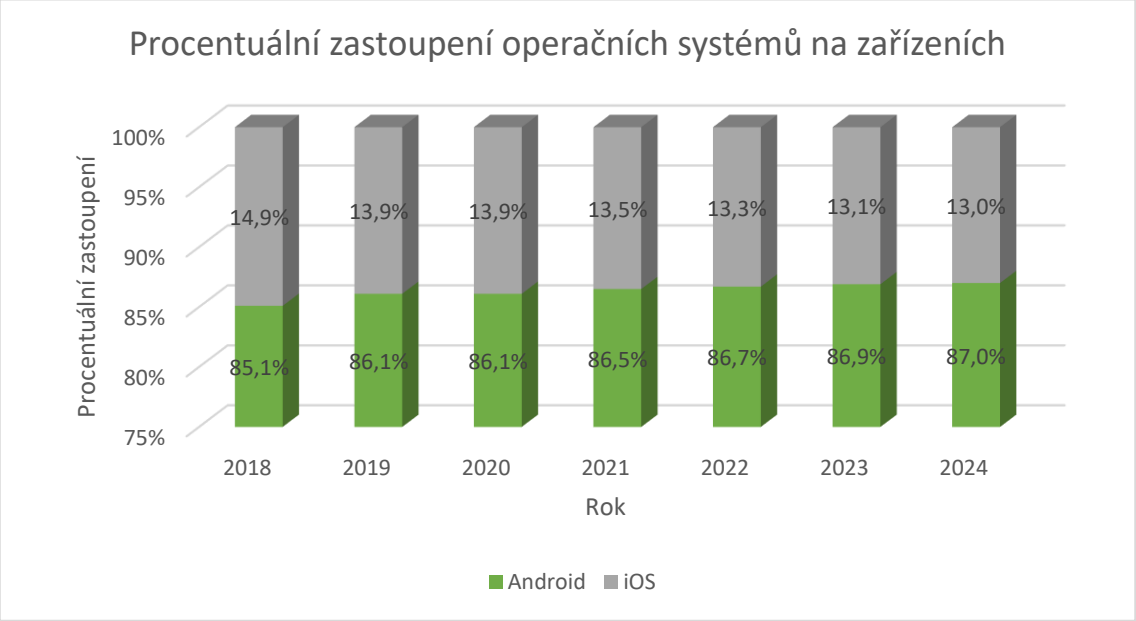
Jedná se o operační systém od společnosti Nokia. Objevuje se na starších tlačítkových mobilních telefonech, ale prodávaly ho a propagovaly jiné obchodní značky. Nokia nadále nevyvíjí Symbian jako open-source projekt. (Beal, 2011)

2.5 BlackBerry (RIM)

BlackBerry je operační systém původně vyvíjen společností Research in Motion pro kapesní zařízení, která umožňují synchronizaci dat v zařízení s tím, co je na firemním serveru. Tyto zařízení se vyznačují hlavně identickými vysouvacími klávesnicemi. (Beal, 2011)

2.6 Další operační systémy

Dalšími operačními systémy mobilních komunikačních zařízení mohou být také Bada (Samsung Electronics) OS používaný původně na smartphonech Samsungu. MeeGo (Nokia a Intel) tento OS býval na smartphonech, tabletech ve vozidlech apod. Jeden z dalších je také Palm OS (Garnet OS) tento operační systém můžeme nalézt na PDA zařízeních (přenosných malých počítačů), a jako poslední je operační systém WebOS, který využívala společnost HP (Hewlett-Packard). (Beal, 2011)



Obrázek 3: Graf procentuálního zastoupení operačních systémů na zařízeních s předpovědí z dubna 2020 (Chau a Reith, 2020)

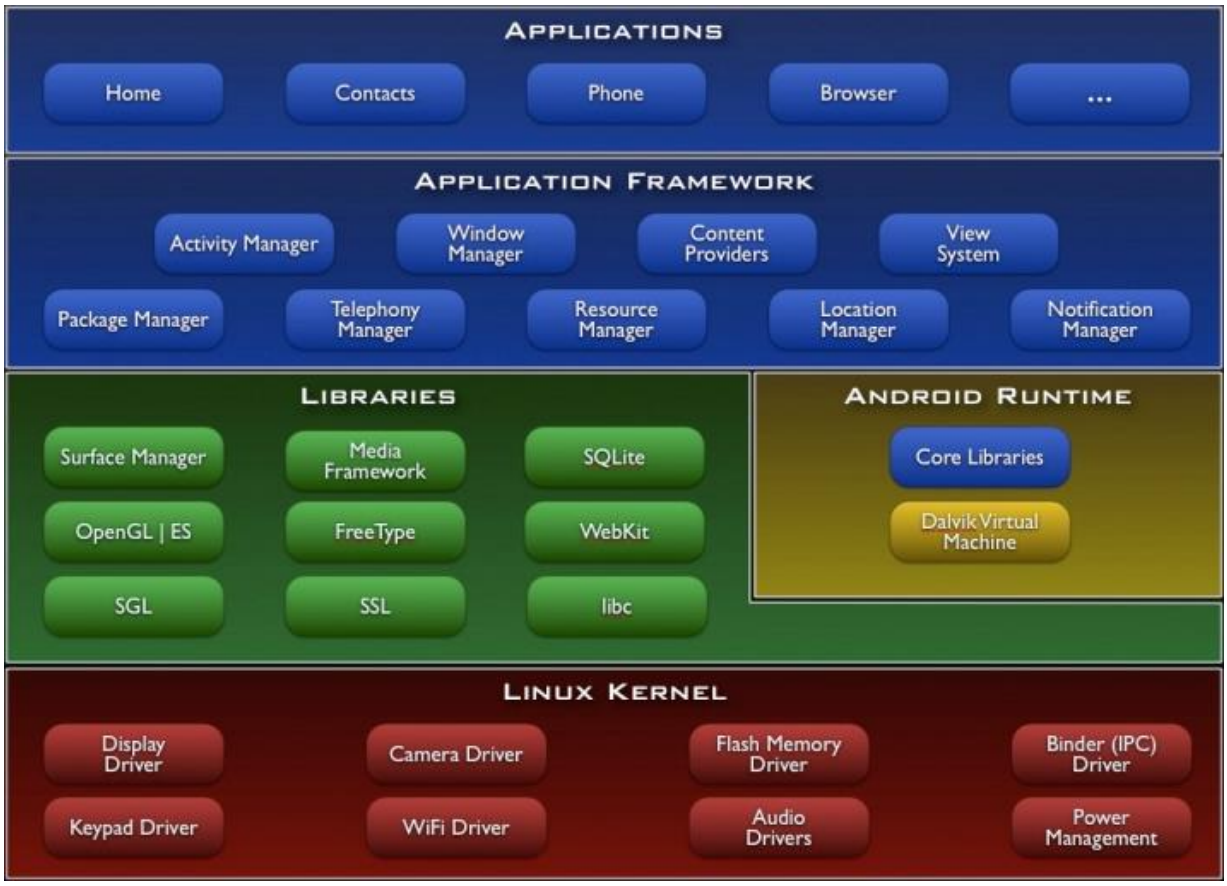
Podle webu IDC můžeme z grafu vyčíst, že největší zastoupení na zařízeních má operační systém Android, který je v prvním čtvrtletí roku 2020 na zhruba 86 % ze všech zařízeních. Operační systém iOS je zatím na zhruba 14 % ze všech zařízeních. Ostatní operační systémy aktuálně už nenajdeme na skoro žádném zařízení, nebo je jejich procentuální zastoupení zanedbatelné. Graf obsahuje také předpověď na další roky, jak by se mohlo toto procentuální zastoupení měnit. V této práci se budu věnovat těmto dvěma operačním systémům.

3 STRUKTURA OPERAČNÍCH SYTÉMŮ ANDROID A IOS

V následující kapitole si něco povíme o struktuře neboli jádru operačního systému Android a iOS, rozebereme si je na části a jednotlivě se je pokusím popsat. Jak už víme z předešlé kapitoly, kde byl android popsán velmi stručně, tento systém je tzv. „open-source“ což znamená že jeho zdrojový kód lze upravovat, takže výrobci zařízení, kteří použijí tento operační systém ho můžou nadále měnit. iOS je naopak proprietární operační systém tedy s uzavřeným kódem. Android jako takový, je v podstatě už upravený systém vycházející z linuxového jádra. Linuxové jádro je nejčastějším používaným upravovaným jádrem u např. osobních počítačů a serverů. (Jak vypadá Android uvnitř?, 2011)

3.1 Struktura Androidu

Struktura systému se dá nejlépe popsat dle následujícího obrázku a dále bude popsána v jednotlivých částech:



Obrázek 4: Struktura operačního systému Android (Jak vypadá Android uvnitř?, 2011)

Bootloader a ROM

Tuto součást na obrázku nenajdeme, protože je jakýmsi samostatným programem neboli „zavaděčem“ pro spuštění samotného operačního systému. Nejedná se tedy o součást struktury operačního systému. Bootloader přesněji řečeno nahraje jádro operačního systému do operační paměti. Další funkcí bootloaderu je ale také předání parametrů operačnímu systému, umožňuje spustit různé testy pro zjištění funkčnosti operačního systému při např. havárii operačního systému. Slouží také k nahrání nové ROM. U části ROM se také nejedná o součást operačního systému. ROM tedy „Read only memory“ je paměť která slouží pouze ke čtení je to tedy paměť, ve které je uložen vlastní operační systém. Lze do ní zapisovat pouze ve zvláštním režimu. Jsou to tedy soubory vlastního operačního systému, které jsou zde uloženy. Součástí ROM je tzv. „Radio ROM“ což je paměť ve které jsou uloženy informace o operátorovi, základní ovladače hardwaru a také informace o čipu. Paměť ROM je také rozšířena různé programy a vlastní úpravy systému podle výrobce zařízení nebo operátora. Poslední součástí je paměti ROM je CID Lock (Carrier ID), kde se jedná o mechanismus výrobce nebo distributora zařízení, které má zabránit uživatelům nahrání neoficiální ROM. Tuhle ochranu lze odstranit, ale vlastník zařízení poté přichází o záruku. (Jak vypadá Android uvnitř?, 2011)

3.1.1 Kernel

První hlavní součástí je samotné jádro Linux Kernel. Tato jedna z hlavních součástí operačního systému nám zajišťuje komunikaci mezi hardwarem a softwarem zařízení (ovladači). Dále tato součást zajišťuje správu procesů, napájení, paměti, zajišťuje nám síťové připojení apod. (Jak vypadá Android uvnitř?, 2011)

3.1.2 Libraries

Knihovny obsahují řádky kódů, které jsou napsány v programovacím jazyce C/C++ a umožňují základní funkce systému. Surface manager nám zajišťuje zobrazování aplikací a jejich vrstvení. Open GL a SGL jsou knihovny pro práci s grafikou. Media framework nám slouží k práci s multimediálními soubory apod., kde můžeme nalézt kodeky pro přehrání různých formátů videa a zvuku. Knihovna SQLite nám slouží pro ukládání dat a práci s nimi. Webkit je vykreslovací jádro pro prohlížeč a FreeType se stará o vykreslování písma a šifrování dat. (Jak vypadá Android uvnitř?, 2011)

3.1.3 Android Runtime

Tato součást systému se stará o bezproblémový běh aplikací. Jelikož zdrojový kód některých aplikací není napsaný v nativním programovacím jazyku C/C++ ale jsou napsány v programovacím jazyku Java, tak tato součást se stará o převod zdrojového kódu do nativního programovacího jazyku. Dále se zde nachází také Java knihovny. (Jak vypadá Android uvnitř?, 2011)

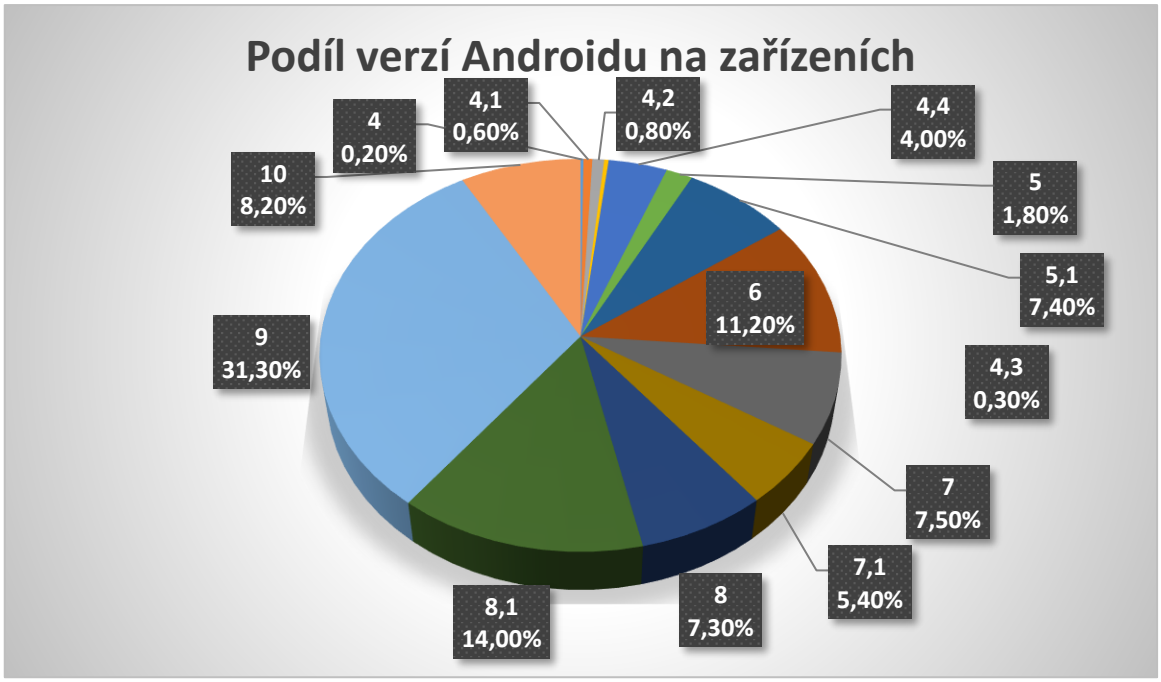
3.1.4 Application framework

Tato součást obsahuje další potřebné knihovny napsané v programovacím jazyku Java, které tvoří systémové API (Appliaction Programming Interface) což je programové rozhraní pro pracování s prvky operačního systému. Vývojář má zde přístup ke grafickým prvkům systému, obsahu různých aplikací apod. (Jak vypadá Android uvnitř?, 2011)

3.1.5 Applications

Zde už se nachází samotné aplikace systému, jakými jsou např. kontakty, telefonování, prohlížeč apod. (Jak vypadá Android uvnitř?, 2011)

Na následujícím grafu bude znázorněn podíl verzí Androidu na zařízeních uživatelů.



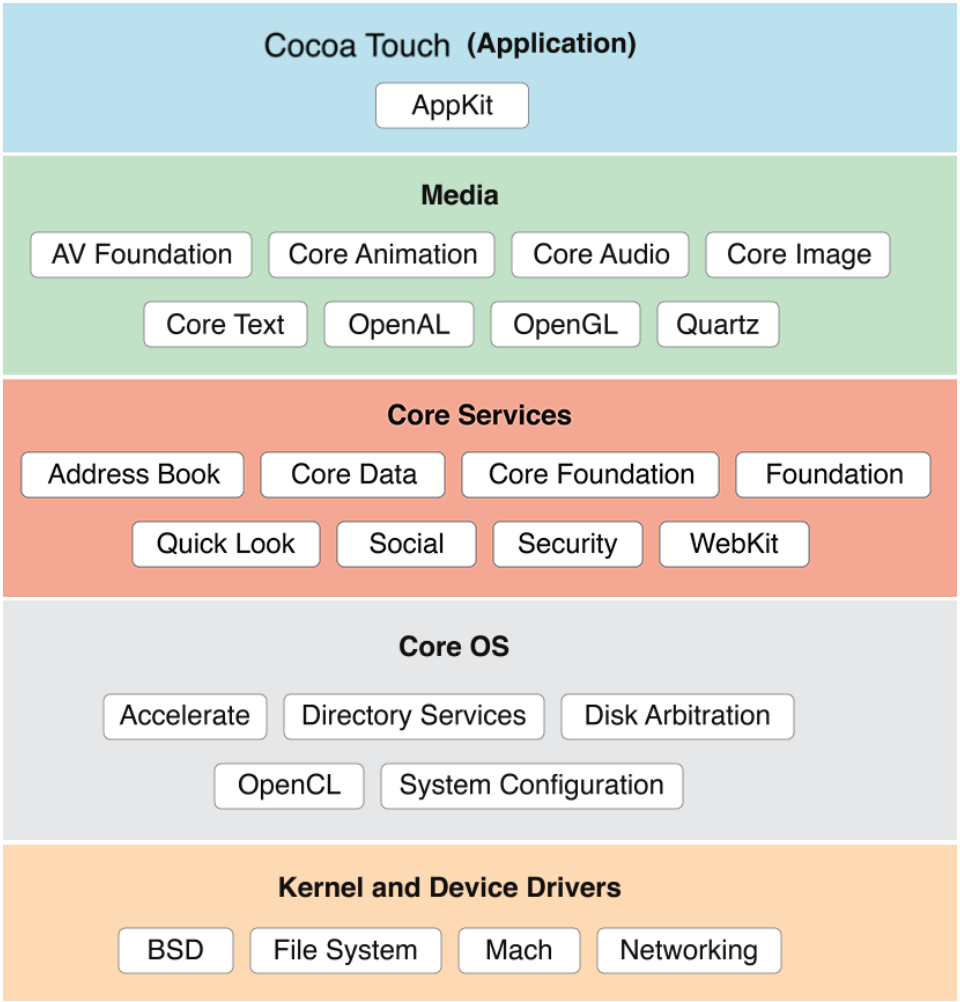
Obrázek 5: Graf podílu verzí Androidu na zařízeních z dubna 2020 (Václavík, 2020)

Podle serveru Cnews.cz můžeme z grafu vyčíst, že verze 4.x běží na 5,9 % všech zařízení, dále potom verzi 5.x můžeme nalézt na 9,2 % všech zařízeních, verze 7.x běží na 12,9 % všech zařízeních. Jedny z největších podílů zabírají verze 8.x a 9.x a to dohromady 52,6 %. Nejaktuálnější verze 10 běží podle těchto dat na 8,2 % všech zařízeních. Nové bezpečnostní aktualizace jsou vydávány pro určitá zařízení a to výrobcem, nikoliv Googlem samotným podle verze operačního systému. (Václavík, 2020)

3.2 Struktura iOS

V následující části bude vysvětlena základní struktura neboli jádro operačního systému iOS, který vyvíjí společnost Apple. Jak už bylo zmíněno výše, tento operační systém nenajdeme na žádném zařízení třetí strany ale pouze na zařízeních společnosti Apple. Tím pádem se hlavní směr vývoje operačního systému iOS upírá pouze na firmu Apple.

iOS původně pochází z operačního systému Mac OS X, ten zase původně sdílel základní strukturu operačního systému Darwin. Operační systém Darwin je tzv. „open-source“ operační systém, který byl vydán společností Apple v roce 2000, který zformuloval dnes používaný operační systém macOS na zařízeních Mac apod. Skládá se z 5 hlavních částí. (Remaker, 2018) (IOS Apple, c1999–2019)



Obrázek 6: Struktura operačního systému iOS (Lucideus, 2019)

3.2.1 Kernel and Device Drivers

V této vrstvě je obsaženo jádro a ovladače pro celé mobilní zařízení. Můžeme zde také nalézt ovladače pro připojení k internetu, ale také mikrojádro Mach a BSD, které poskytují vysoce výkonná síťová zařízení a podporu pro více integrovaných souborových systémů. (Lucideus, 2019) (Understanding Xamarin iOS - Build Native iOS App, 2019)

3.2.2 Core OS

Tato vrstva poskytuje funkce ostatním technologiím, mezi které patří např. Accelerate Framework, které nabízí rozhraní pro práci s matematickými funkcemi, nebo také zaručuje bezpečnost citlivých dat. V této vrstvě se také nachází různá systémová konfigurace apod. (IOS Apple, c1999–2019)

3.2.3 Core Services

Jedná se o vrstvu základních služeb, která se skládá ze základních služeb, jakými jsou např. adresář, zabezpečení, sociální sítě a nadace, které poskytují aplikacím základní funkce. Tato vrstva také poskytuje přístup k základním zdrojům potřebným pro aplikaci. Umožňuje konkrétně např. provádět platby uvnitř aplikace, sledovat polohu uživatele, přístup k aplikaci iTunes Store nebo přístup k audio a video souborům. (IOS Apple, c1999–2019) (Understanding Xamarin iOS - Build Native iOS App, 2019)

3.2.4 Media

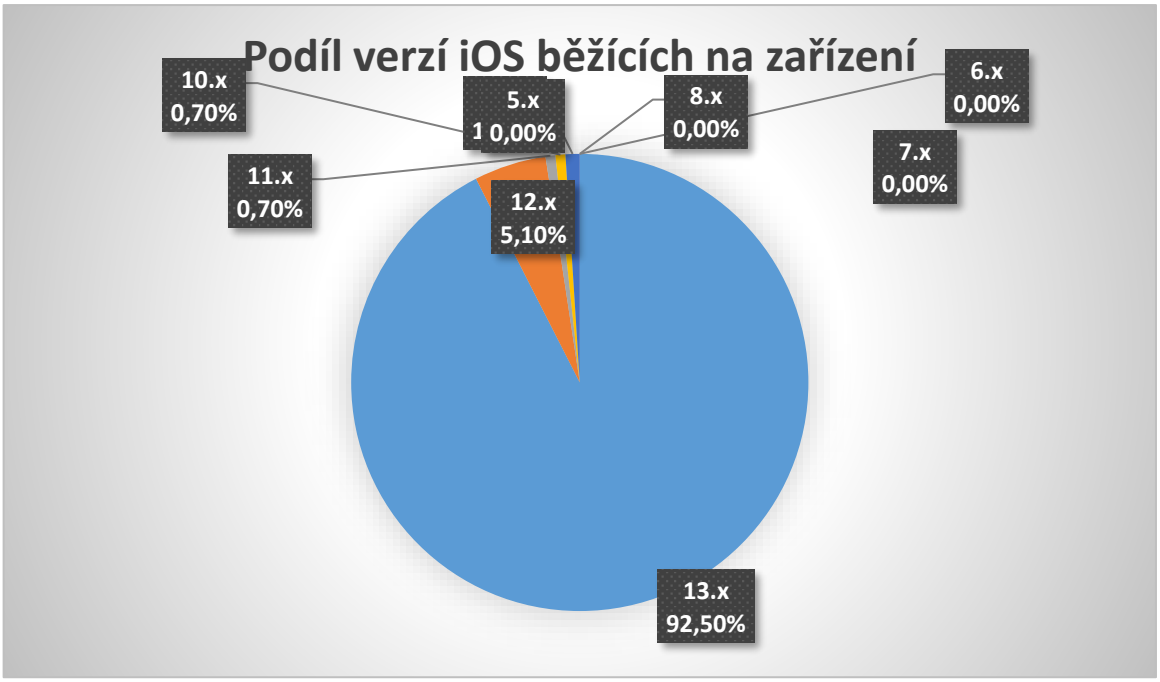
Tato vrstva umožňuje použít dvou rozměrnou a tří rozměrnou grafiku, animace, obrazové efekty a profesionální zvukové a obrazové funkce do mobilní aplikace. (Understanding Xamarin iOS - Build Native iOS App, 2019)

3.2.5 Cocoa touch

Tato vrstva se stará o vzhled aplikací. Poskytuje nám také přístup k hlavním funkcím systému, jakými jsou např. kontakty, kamera, dotykový vstup, sdílení s jinými aplikacemi, push oznámení (zobrazení oznámení i když aplikace není spuštěná) apod.

Umožňuje také provádět více procesů zároveň tzv. multitasking, dále poskytuje spojení mezi více zařízeními apod. (IOS Apple, c1999–2019) (Understanding Xamarin iOS - Build Native iOS App, 2019)

V následujícím grafu bude znázorněn podíl verzí iOS běžících na zařízeních.



Obrázek 7: Graf podílu verzí iOS běžících na zařízeních z ledna 2020 (Smith, 2020)

Z grafu je zřejmé že více než 92 % zařízení běží na nejnovější verzi iOS 13.x. Na zhruba asi 5 % zařízeních běží starší verze 12.x. Z Tohoto lze usuzovat, že na většině zařízeních je nainstalována nejnovější verze operačního systému iOS, což z hlediska bezpečnosti je velmi dobré číslo. Společnost Apple se vyznačuje tím, že podporuje svým novým softwarem poměrně už hardwarově stará zařízení a tím pádem pořád udržuje jejich bezpečnost na co největší možné úrovni oproti společnosti Google.

4 AKTUÁLNÍ ZRANITELNOSTI SYSTÉMŮ

V této kapitole budou vypsány aktuální chyby, bezpečnostní trhliny, hrozby každodenního používání mobilních zařízení, které mají vliv na bezpečnost uživatelů a jejich soukromí na operačních systémech Android a iOS. Každý operační systém nebo aplikaci vytváří lidé a tím pádem zde mohou vzniknout určitá slabá místa. Tyto slabá místa vznikají nejvíce už při samotném vývoji, kdy vývojáři mohou v samotném kódu operačního systému nebo aplikace udělat chybu a hrozí zde riziko, že tyto slabá místa nebudou rychle odhalena a opravena, ovšem zařízení může být také napadeno z důvodu špatného zabezpečení zařízení vinnou vlastníka tohoto zařízení. Každou novou verzí operačního systému nebo aplikace se vývojáři snaží opravit předešlé chyby a snaží se najít ony slabá místa, ovšem nalezení všech dosavadních chyb nebo slabých míst je v podstatě nemožné, protože vždy se nějaká chyba nebo slabé místo najde. Důležitá ochrana proti těmto zranitelnostem je mít vždy na svém zařízení nejaktuálnější verzi operačního systému a aplikace, neméně důležité jsou také nejaktuálnější bezpečnostní záplaty, vhodné je také používat ověřené aplikace. V závěru kapitoly budou vytvořeny tabulky a grafy s počty zranitelností.

4.1 Obecné hrozby mobilní zařízení

Následující hrozby jsou jedny z nejvážnějších pro zabezpečení těchto zařízení. Počty těchto hrozeb neustále rostou, takže je zapotřebí naše zařízení těmto hrozbám vystavovat co nejméně.

1) Únik dat

Přes mobilní aplikace často dochází k nechtěným únikům dat. Častý důvod úniku těchto dat je zapříčiněno povoleními neboli oprávněními aplikace přístupu k částem zařízení např. do úložiště. Tyto aplikace pak mohou posílat osobní případně firemní data na vzdálené servery, kde s nimi mohou pracovat inzerenti nebo už dokonce počítačoví zločinci.

Jako obrana proti nechtěnému úniku dat je nutné při povolení oprávnění dávat pozor, jestli opravdu toto povolení udělit či nikoliv. (Top 7 Mobile Security Threats: Smart Phones, Tablets, & Mobile Internet Devices – What the Future has in Store, 2020)

2) Nezabezpečené Wi-Fi sítě

Když jsou k dispozici veřejné Wi-Fi si můžeme říct proč nevyužít internet zadarmo a zbytečně si nečerpat svá mobilní data na zařízení, ale právě tyto veřejné Wi-Fi sítě jsou často nezabezpečeny, takže jsou další hrozbou pro naše zařízení.

Proto je vhodné při používání těchto veřejných Wi-Fi sítí nechodit do internetového bankovnictví apod. kde by vzniklo riziko vyzrazení vašich hesel a údajích vaší kreditní karty. (Top 7 Mobile Security Threats: Smart Phones, Tablets, & Mobile Internet Devices – What the Future has in Store, 2020)

3) Spoofing sítí

Při spoofingu sítí dochází v podstatě k vytvoření falešných přístupových bodů pro připojení, která zároveň vypadají jako veřejné Wi-Fi sítě, ale ve skutečnosti se jedná o past. Tyto sítě můžeme nalézt na veřejných místech jakými jsou např. kavárny, letiště apod. V některých případech útočníci vyžadují po uživateli vytvoření jakéhosi „účtu“ doplněného heslem. Mnoho lidí používá totiž stejnou kombinaci e-mailu a hesla pro více služeb a zde může dojít k ohrožení vašich e-mailů, elektronických obchodů a dalších informací.

Proto je vhodné jako opatření proti tomuto spoofingu při případném vytváření „účtu“ zvolit jedinečné heslo pro případ vyzrazení. (Top 7 Mobile Security Threats: Smart Phones, Tablets, & Mobile Internet Devices – What the Future has in Store, 2020)

4) Phishingové útoky

Tyto útoky jsou známé tím, že vám na e-mail dojde na první pohled důvěrný e-mail ovšem zdání může klamat a tento e-mail může být použit jako návnada pro napadení vašeho zařízení, při kliknutí např. na odkaz v tomto e-mailu.

Jako ochrana proti phishingovému útoku se jeví jednoduché ověření e-mailové adresy odesílatele např. na webu. (Top 7 Mobile Security Threats: Smart Phones, Tablets, & Mobile Internet Devices – What the Future has in Store, 2020)

5) Spyware

Jedná se o software navržený pro shromažďování dat z vašeho zařízení a zasílání ho třetí straně bez vašeho souhlasu nebo znalosti uživatele. Dochází k shromažďování dat, jakými jsou např. hesla, PINy, čísla kreditních karet apod. (Top 7 Mobile Security Threats: Smart Phones, Tablets, & Mobile Internet Devices – What the Future has in Store, 2020)

4.2 Android

V následující části budou zmíněny některé zranitelnosti týkající se operačního systému Android. Existuje jich celá řada, ale zde budou zmíněny pouze ty nejznámější za poslední dobu.

4.2.1 StrandHogg

StrandHogg je název pro jednu z nejaktuálnějších zranitelností systému Android. O této nové zranitelnosti informovala norská bezpečnostní společnost Promon. Tato společnost popsala, kde se nachází se nachází problém, ale také zmínila, že tato chyba je neustále zneužívána a v bezpeční není v podstatě nikdo. Jedná se o malware určený k proniknutí do systému. Tato chyba se týká multitaskingu, což je schopnost systému provádět několik procesů zároveň. Jakákoliv aplikace tedy může převzít jakoukoliv identitu v rámci tohoto procesu. Tento malware tak může takřka posbírat všechna oprávnění, aniž by toho byl uživatel vědom. Může také uživateli nabídnout okno s vyplněním přístupových údajů a tím zaslat útočníkovi vaše přihlašovací údaje.

Tato chyba se týká všech verzí systému Android i nejaktuálnější verze 10. Útočník může poslouchat přes mikrofon, fotit fotografie a používat kameru, číst a posílat SMS zprávy, volat a nahrávat hovory, získat polohu a GPS informace, kontakty apod. (Vaculík, 2010) (StrandHogg: Serious Android vulnerability leaves most apps vulnerable to attacks, 2006)

4.2.2 Zero-day chyba

Bezpečnostní tým Googlu, který je známý pod jménem Project Zero objevil v Androidu bezpečnostní chybu. Po nainstalování škodlivé aplikace nebo navštívení podvodné stránky chyba umožňovala útočníkům přístup k telefonu, nainstalovat další viry, odposlouchávat zařízení, nebo přistupovat k datům která jsou na něm uložená včetně fotografií a videí.

Bylo také potvrzeno že tuto chybu využívala Izraelská společnost NSO, která poskytuje vládním organizacím nástroje za, pomocí kterých mohou vniknout do zařízení s operačními systémy Android a iOS.

Ještě před vytvořením záplaty se útočníkům podařilo tuto bezpečnostní chybu zneužít – jedná se tedy o tzv. Zero-day chybu.

Pokud máte nainstalovaný antivirový program ani ten nemusí v tomto případě pomoci. Zajímavé je že některé telefony jsou proti těmto útokům imunní. Google také zveřejnil seznam postižených telefonů. (Stovky milionů mobilů v ohrožení. Oprava nebezpečné trhliny chybí, 2019) (Google zjistil obří bezpečnostní chybu v Androidu z roku 2017. Využívala ji izraelská organizace, 2019)

4.2.3 Napadení PNG obrázkem

V Androidu se nacházely tři zranitelnosti, které umožňovaly napadnout zařízení po otevření upraveného obrázku ve formátu PNG. Tyto chyby se vyskytovaly ve verzích od čísla 7 až po číslo 9.

Google tuto bezpečnostní chybu zveřejnil v rámci bulletinu a už v únoru roku 2019 na ni vydal bezpečnostní záplatu. Uživatelé, kteří mají telefon v rámci projektu Android One, těch se tato chyba netýkala, ty totiž měly záplatu nainstalovanou ihned. (Kluska, 2019)

4.2.4 Aplikace QRecorder

V roce 2018 se v obchodě s aplikacemi Google Play vyskytovala aplikace s názvem QRecorder což byla důvěryhodná kopie původní originální aplikace QRecorder, jednalo se tedy o její klon. Účelem této aplikace mělo být nahrávání telefonních hovorů. Kupodivu jednou z aktualizací této aplikace se následně aplikace snažila nainstalovat škodlivý kód. Tento škodlivý kód se nainstaloval, pokud bylo v nastavení zařízení povolena položka instalace aplikací z neznámých nebo neověřených zdrojů. Jestliže uživatel mněl tuto položku povolenou, pak útočník měl přístup k bankovním účtům uživatele a mohl ukrást peníze. Dále útočník mohl číst příchozí SMS zprávy, přes které přichází ověřovací SMS zprávy pro potvrzení bankovní transakce, pokud ověřovací zprávy chodí na stejné zařízení. Tímto způsobem útočník připravil přibližně 5 lidí o skoro 2 miliony korun. Z tohoto důvodu vyplývá, že je vhodné používat pro ověřování bankovních transakcí jiné zařízení, které zároveň neslouží k ovládání bankovnictví. Za oficiální aplikací QRecorder stojí autor „PA Production“, a ona podvodná aplikace měla autora „NickBaza“. Autoři této škodlivé aplikace si od originálního autora pravé aplikace QRecorder koupili zdrojový kód a doplnili ho o tuto škodlivou činnost. (Hák, 2018)

4.3 iOS

A v další podkapitolce budou pro změnu vybrány jedny z nejznámějších aktuálních zranitelností dle mého názoru pro operační systém iOS.

4.3.1 Checkm8 (iOS)

Řada odborníků v oblasti bezpečnosti odhalili váznou bezpečnostní trhlinu na zařízeních iPhone. Tato trhlina pravděpodobně postihuje stovky milionů smartphonů Apple.

Ohroženy jsou zařízení s čipy řadou A5 až A11, což znamená že postiženy jsou zařízení od iPhonu 4 S až po iPhone X. Problém je v tom že chyba je v podstatě neopravitelná. Pokud máte zařízení se softwarovou úpravou Jailbreak, tak útočníkům dáváte možnost k získání kontroly a možnost ovládat vaše zařízení.

Chyba se týká bootovací paměti ROM, kterou nelze číst ani do ní zapisovat, proto se tato chyba nedá opravit. Jedinou možností, jak by se dala tato chyba opravit by byla možná pouze tehdy, že by musela být vyměněna celá čipová sada telefonu, tím pádem jediná možnost ochrany je pořídit si novější zařízení, které používá čipset A12 a vyšší.

Pro uživatele tady existuje výhoda a to ta, že útočník nemůže zařízení napadnout zařízení vzdáleně, ale musí se k němu fyzicky dostat a napadnout ho například přes USB port, následně by útočník musel prolomit váš PIN kód. Další nespornou výhodou je, že pokud je zařízení po napadení restartováno, přístup útočníku k telefonu se tím ztratí. (Palyza, 2018)

4.3.2 Hacknutí přes webovou stránku (iOS)

Výzkumníci ze skupiny Google Project Zero odhalili zranitelnost, která patří mezi jedny z největších v celé historii iOS. Jednalo se o škodlivý malware, který zneužíval chyb ve vestavěném webovém prohlížeči Safari.

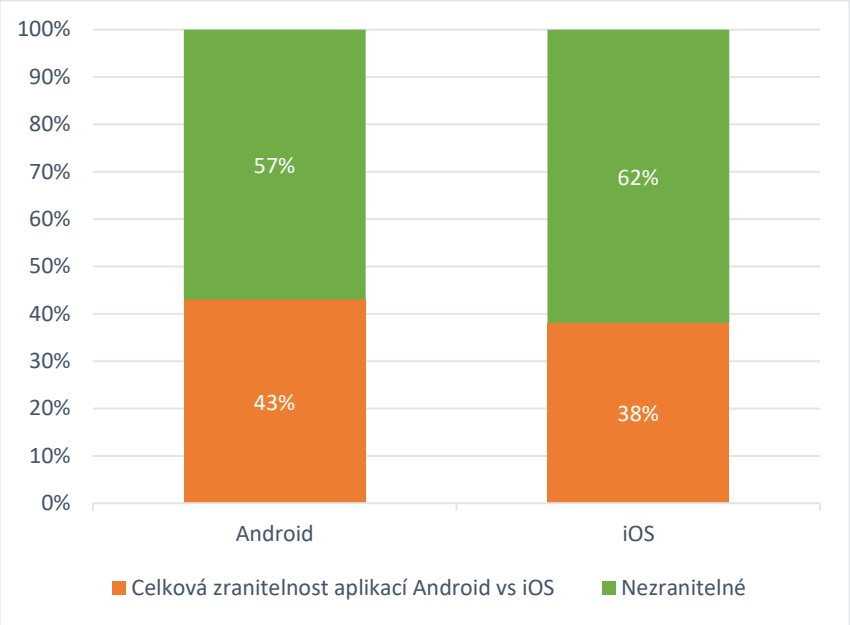
K napadení vašeho zařízení stačilo pouze navštívit infikovanou webovou stránku. Tato chyba se nacházela ve verzích iOS 10 až po iOS 12.

Malware fungoval tak, že při navštívení infikované stránky se spustil na pozadí škodlivý kód, který se vložil do zařízení. Malware sloužil ke sbírání a posílání polohových dat. Tento malware se vložil do paměti zařízení, takže mohly být sbírány zprávy z aplikace iMessage. Dokázal také dokonce obejít sandboxing. (Škuta, 2018)

4.4 Komparace počtu zranitelností operačních systémů Android a iOS

V této kapitole budou vytvořeny různé tabulky a grafy spojené se zranitelností Androidu a iOS.

Aplikace pro Android mají tendenci obsahovat kritické zranitelnosti o něco častěji než aplikace pro iOS. Tento rozdíl není však tak významný a celková úroveň zabezpečení aplikací pro Android a iOS je zhruba stejná.

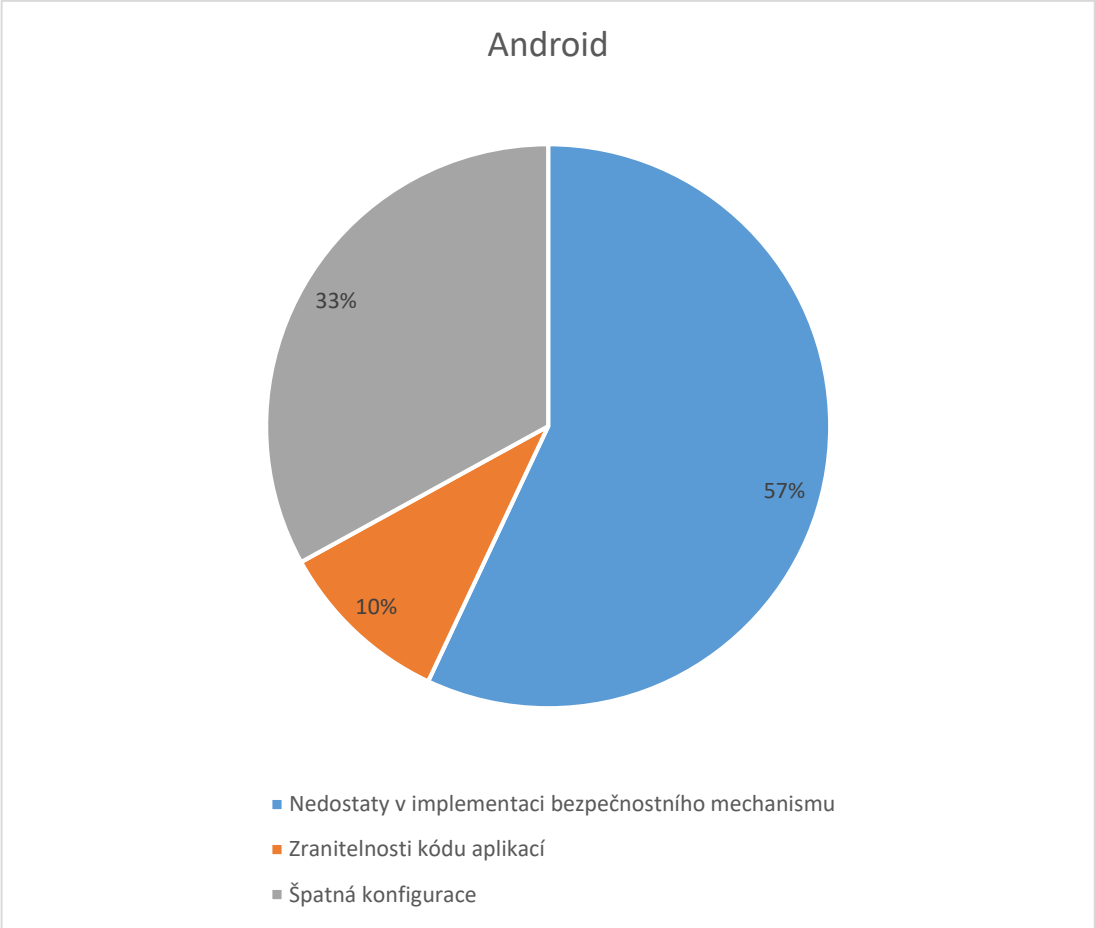


Obrázek 8: Graf celkové zranitelnosti aplikací Android vs iOS z června 2019 (Vulnerabilities and threats in mobile applications, c2002-2020)

Android v celkové zranitelnosti aplikací obsahuje zhruba 43 % kritických zranitelností. iOS však o něco méně a to 38 %.

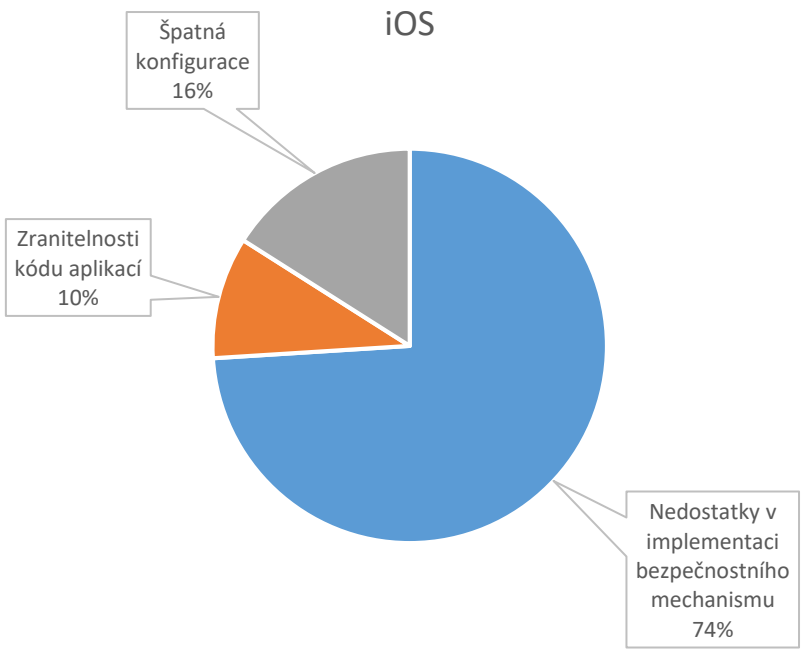
Zranitelnosti na straně operačního systému jsou tvořeny zhruba 60 % a zbylých 40 % na straně vývojáře. 89 % zranitelných míst lze zneužít bez fyzického přístupu k zařízení a zbylých 11 % lze zneužít pouze s fyzickým přístupem k zařízení. 56 % zranitelných míst lze zneužít bez administrátorských práv (jailbreak nebo root) a zbylých 46 % lze s administrátorskými právy. (Vulnerabilities and threats in mobile applications, c2002-2020)

Následující grafy popisují typy zranitelností aplikací dle operačního systému.



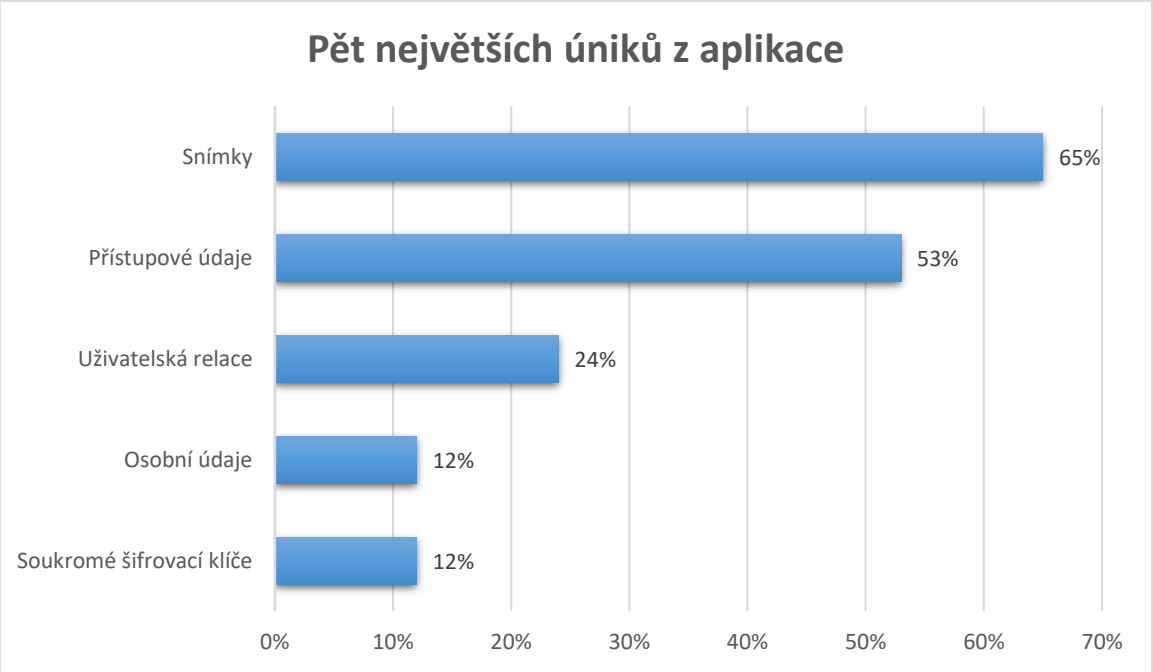
Obrázek 9: Graf zranitelnosti podle typu Android z června 2019 (Vulnerabilities and threats in mobile applications, c2002-2020)

Z grafu vyplývá, že největší zranitelnosti, které ovlivňují bezpečnost se objevují jako nevhodná opatření v bezpečnostních mechanismech nebo je jich nedostatek, dále pak druhé nejvíce zastoupené zranitelnosti se týkají nevhodné konfigurace celé aplikace a jako poslední se jeví zranitelnost kódu samotné aplikace.



Obrázek 10: Graf zranitelnosti podle typu iOS z června 2019 (Vulnerabilities and threats in mobile applications, c2002-2020)

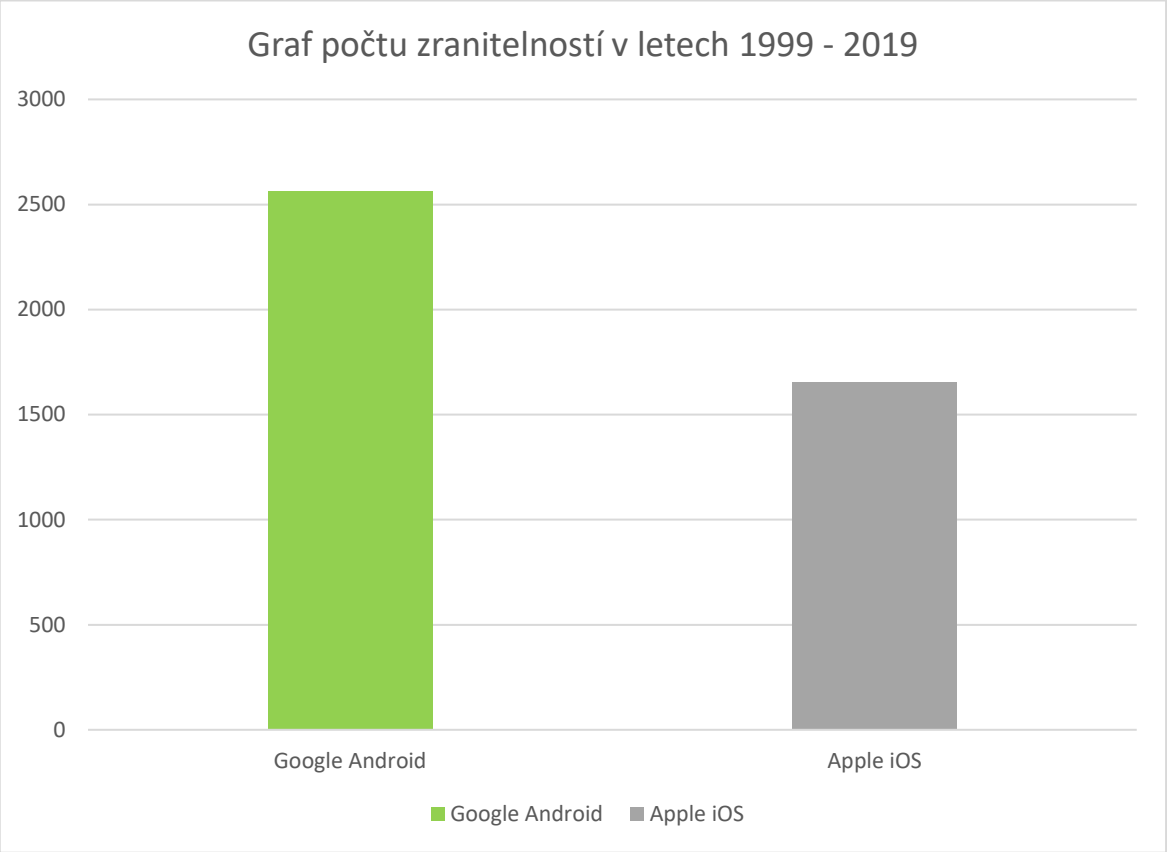
Z těchto grafů můžeme vidět, že zvýšení zranitelnosti operačních systémů je způsobeno nedostatky v implementaci bezpečnostních mechanismů. (Vulnerabilities and threats in mobile applications, c2002-2020)



Obrázek 11: Graf pěti největších úniků z aplikace z června 2019 (procento zranitelných aplikací) (Vulnerabilities and threats in mobile applications, c2002-2020)

Z Grafu vyplývá, že z aplikace mohou uniknout např. přístupové údaje nebo snímky, a proto je nutné, aby aplikace ukládaly např. přístupové údaje a snímky do adresářů, která jsou šifrovaná nebo využít jednu z moderních technologií jako je např. Touch ID nebo Face ID. Jedná se o citlivá data a ty by aplikace měla chránit opravdu přísně a znemožnit případnému útoku, aby byly tyto data odcizeny či vyzrazeny.

Na následujícím grafu je možné vidět, jak jsou na tom se zranitelností operační systémy Android a iOS od roku 1999 až po rok 2019, co do počtu nahlášených a objevených bezpečnostních trhlin.



Obrázek 12: Graf počtu zranitelností v letech 1999-2019 (Čížek, 2019)

Z grafu vyplývá, že nejděravější operační systém v letech 1999-2019 byl Android. Počty zranitelností nemusí být ve skutečnosti natolik přesné, protože se jedná pouze o chyby, které byly objeveny a nahlášeny.

II. PRAKTICKÁ ČÁST

5 NATIVNÍ BEZPEČNOSTÍ FUNKCE OPERAČNÍCH SYSTÉMŮ ANDROID A IOS

V následující kapitole bude vytvořen check-list se základními bezpečnostními funkcemi, zda daný operační systém touto funkcí disponuje či nikoliv. Následně bude rozebrána bezpečnost obou operačních systémů podrobně.

5.1 Bezpečnost Androidu

Google poskytuje různé primární služby pro zabezpečení zařízení které běží na Androidu.

- **Google Play** – Jedná se o kolekci služeb, kde uživatelé mohou instalovat a nakupovat aplikace, poskytuje také kontrolu komunity, ověření licence pro aplikace, skenování zabezpečení aplikace a další bezpečnostní služby.
- **Aktualizace pro Android** – Jde o aktualizační službu, přes kterou zařízení mohou instalovat aktualizace, které jim přináší nové funkce a aktualizace zabezpečení;
- **Služby aplikací** – Umožňují aplikacím používat cloudové funkce, jakými jsou např. zálohování dat, nastavení aplikací apod.
- **Ověření aplikací** – Tato služba nás bude varovat nebo přímo zablokuje instalaci škodlivých aplikací, průběžně také prohledává aplikace v zařízení, zda nejsou škodlivé.
- **SafetyNet** – Je to systém pro detekci narušení soukromí, který pomáhá sledovat Google, zmírňuje známé bezpečnostní hrozby a dokáže identifikovat nové vzniklé bezpečnostní hrozby.
- **SafetyNet Atestation** – Pomáhá chránit vaši aplikaci před bezpečnostními hrozbami, včetně manipulace se zařízeními, možné chybné adresy URL, falešnými uživateli apod.
- **Správce zařízení Android** – Jedná se o aplikaci, která slouží k nalezení ztraceného zařízení. (Secure an Android Device, 2020)

Android používá svoji architekturu pro zabezpečení své platformy Android, kde se snaží o následující prvky:

- Chránit aplikace a uživatelská data, chránit systémové prostředky včetně sítě, izolaci aplikací od systému, navzájem od ostatních aplikací a od uživatele.

- Robustní zabezpečení na úrovni operačního systému pomocí linuxového jádra.
- Povinnou karanténu aplikací, které se mu zdají být škodlivé.
- Zabezpečená komunikace mezi procesy.
- Podepisování aplikací a udělování oprávnění aplikaci na základě povolení uživatele. (Secure an Android Device, 2020)

5.1.1 Bezpečnostní programy Androidu

Mezi hlavní součásti programu zabezpečení Android patří:

- **Přezkoumání návrhu** – Protože je Android tzv. „open-source“ projekt tak každá hlavní funkce je přezkoumávána technickými a bezpečnostními prostředky s příslušnými prvky zabezpečení integrovanými do architektury systému.
- **Testování a kontrola kódu** – Během vývoje platformy podléhají komponenty vytvořené Androidem přísným kontrolám zabezpečení, cílem těchto kontrol je identifikovat slabá místa a možné zranitelnosti v dodatečném předstihu před vydáním.
- **Open source a komunitní recenze** – Umožňují kontrolu jakoukoli zúčastněnou stranou a např. i uživatelem.
- **Reakce na incident a měsíční aktualizace** – Android monitoruje reakce o potenciálních zranitelnostech, a proto se následně snaží rychle zmírnit zranitelnost pro minimalizaci rizika a poskytuje měsíční záplaty.

5.1.2 Soukromí na Androidu

Nejprve je nutné věnovat pozornost **povolení u těchto aplikací**, a umožnit uživatelům kontrolu nad tím, jak je aplikace bude používat. Aplikaci je vhodné povolovat oprávnění pouze na funkce, které opravdu potřebujete k využívání této aplikace. Nesmíme zapomenout, že uživatel může vybrat možnost znovu se neptat, tím pádem se aplikace později už nebude ptát na tato povolení, což může znamenat ztrátu kontroly nad touto aplikací.

Za zmínku také stojí **využití polohy**, jestliže aplikace by podle vašeho usouzení neměla mít přístup k vaší poloze, určitě toto povolení neudělujte. V nejnovější verzi Androidu 10 povolení využití polohy funguje pouze když se aplikace právě používá.

Zacházení s daty bezpečně je důležitou součástí udržení soukromí uživatele. Proto aplikace šifruje tyto data i bez ohledu na jejich citlivost a ukládá je do interního úložiště, kde ostatní aplikace do této části úložiště nemohou přistupovat.

Vytváření náhodných identifikátorů zaručí že aplikace nebude ukládat informace spojené se sériovými čísly zařízení apod. (Privacy best practises, 2019)

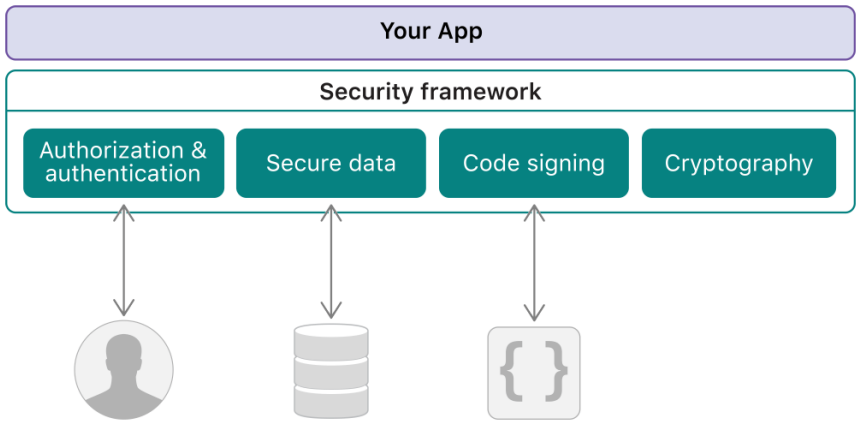
5.2 Bezpečnost iOS

V této kapitole bude rozebrán základní rámec zabezpečení, poté zde budou vypsány základní bezpečnostní programy.

Rámec zabezpečení slouží k ochraně informací, navazování důvěry a řízení přístupu k softwaru.

Bezpečnostní služby obecně podporují tyto cíle:

- Autentizace a poté selektivně udělení přístupu ke zdrojům (autorizace), automatické vytvoření silného hesla.
- Zabezpečení dat přes síťové připojení.
- Zajištění platnosti kódu, který má sloužit pro kontrolu.
- Šifrování. (Security, 2020)



Obrázek 13: Bezpečnostní rámec (Security, 2020)

5.2.1 Bezpečnostní programy iOS

V této kapitole budou vypsány základní nativní bezpečnostní programy a služby pro zvýšení zabezpečení operačního systému iOS.

Zabezpečení hardwaru

Zabezpečení softwaru vyžaduje opatření zabudované v hardwaru. Proto mají zařízení Apple, na kterých běží operační systém iOS bezpečnostní funkce zavedené přímo v křemíku, ze kterého je vyroben procesor zařízení.

- **Secure Enclave** – Koprocesor, který poskytuje základ pro šifrování dat, bezpečné spuštění a biometrii spouští dvě služby.
    - **Touch ID –** Jedná se o rychlou a jednoduchou kontrolu otisků prstů, po které může uživatel odemknout své zařízení, nebo potvrdit platbu apod. pro ověření identity.
    - **Face ID –** Taktéž se jedná rychlou a jednoduchou kontrolu tentokrát obličeje, po které může uživatel své zařízení odemknout; je založena na HW úrovni což je bezpečnější způsob než na softwarové úrovni.
- **Boot ROM** – úplně první kód provedený procesorem při spuštění zařízení, výhodou procesoru je, že jej nemůže změnit jak výrobce Apple, tak ani útočník. (Apple Platform Security, 2019)

Zabezpečení systému

Tato část se věnuje hlavně kontrole správného softwaru při spuštění zařízení.

- **Bezpečné spuštění –** Po spuštění zařízení systém zkontroluje, zda jsou všechny komponenty podepsané společností Apple, aby byla zajištěna integrita a důvěrnost.
- **Autorizace systémového softwaru** – I při aktualizaci operačního systému dochází ke kontrole důvěrnosti a znemožňuje nainstalovat starší verze operačního systému, kvůli možnosti zneužití bezpečnostních děr pro provedení útoku na zařízení,
- **Kontrola integrity operačního systému** – Zabránění úprav jádra operačního systému a ovladačů zařízení. (Apple Platform Security, 2019)

Šifrování a ochrana dat

Zabezpečený spouštěcí řetězec, zabezpečení systému a zabezpečení aplikací pomáhají zajistit, že na zařízení běží pouze důvěryhodný kód a aplikace. Data jsou také chráněna šifrováním, a to v případě ztráty zařízení nebo spuštění nedůvěryhodného kódu. Proto tato funkce poskytuje možnost vzdáleného okamžitého a úplného smazání zařízení.

Zabezpečení aplikací

Aplikace patří mezi jeden z nejdůležitějších prvků moderní bezpečnostní architektury. I když nám tyto aplikace poskytují uživatelům výrazné výhody v oblasti produktivity, mohou také negativně ovlivnit zabezpečení systému, stabilitu, uživatelská data, pokud se s nimi špatně zachází.

Pro získání aplikací slouží služba **App Store**, kde všechny aplikace jsou izolovány pro zajištění nejpřísnějších kontrol.

Zabezpečení služeb

Pro zabezpečení služeb, jakými jsou např. cloudová úložiště (iCloud), synchronizace, ověřování, platby (Apple Pay), zasílání zpráv (iMessage), komunikace (FaceTime), iTunes, Find Me, slouží Apple ID což se jedná v podstatě o jedno heslo, které umožní přístup k těmto službám. (Apple Platform Security, 2019)

5.2.2 Soukromí na iOS

Soukromí na operačním systému iOS je také jako na Androidu zajišťováno několika funkcemi, které chrání naše osobní údaje a zabraňují jejich vyzrazení.

Safari

Jedná se o prohlížeč, který obsahuje nejmodernější funkce, které pomáhají chránit naše soukromí a chrání nás před sledováním napříč weby a tím minimalizují data předaná třetím stranám.

Jednou z hlavních funkcí je **prevence inteligentního sledování**, kde se obsah třetí strany oddělí od ostatních údajů prohlížení, který se používá pro sledování.

Další funkcí je **obrana proti vytvoření „otisků prstů“**, čímž Safari zabraňuje webovým stránkám vytvářet kombinace charakteristik vašeho zařízení, který vás sleduje.

Po zapnutí **soukromého prohlížení** Safari nepřidává navštívené weby do své historie, nezapamatuje si také vaše vyhledávání a neukládá informace z vyplněných formulářů.

Mapy

Personalizované funkce jsou vytvářeny za pomocí dat v zařízení, ty jsou odeslány a **spojeny s náhodnými identifikátory**, takže ani Apple nemá informace o vašich pohybech a vyhledávání.

Tyto mapy používají **šifrování end-to-end**, což zabraňuje společnosti Apple číst vaše osobní údaje.

Zmatení místa spočívá v tom, že když budete vyhledávat pomocí procesu nazvaného „fuzzing" tak mapy převedou přesné místo vašeho hledání na nepřesné místo, čímž by mohlo dojít k odhalení vaší identity.

Fotky

Pokud se v aplikaci Fotky rozhodnete svou knihovnu fotografií zálohovat na iCloud, tak Apple chrání tyto vaše fotografie šifrováním.

Pokud by aplikace třetí strany vyžadovala přístup uložení fotografie k vašim fotografiím, může požádat pouze o tuto jedinou akci, aniž by mohla vidět vaše ostatní fotografie.

iMessage a Facetime

iMessage je aplikace pro zasílání textů, fotek, videí na jiný iPhone, iPad, iPod nebo Mac.

Pro uskutečňování videohovorů existuje aplikace Facetime.

Taktéž jako fotografie, jsou zprávy a **konverzace šifrovány**, takže je nelze číst, když jsou odesílány mezi zařízeními.

Aplikace iMessage nemá přístup ke skutečným kontaktním informacím účastníků nebo konverzacím, protože iOS poskytuje každé aplikaci **náhodný identifikátor pro každého účastníka** pokaždé, který se při odinstalaci aplikace resetuje.

SMS zprávy a iMessage konverzace jsou zálohovány na iCloud ovšem tuto zálohu lze kdykoli vypnout. Tento obsah není nikdy ukládán na žádné servery.

Siri

Siri je virtuální asistent, který používá hlasové dotazy a uživatelské rozhraní pro zodpovězení na otázky. Je navržen tak aby vaše žádosti a dotazy byly **spojeny s náhodným identifikátorem**.

Apple Pay

Ochrana vašeho soukromí při převádění, odesílání a přijímání peněz, transakcí apod. se provádí pomocí **Apple Cash**. Když do Apple Pay prostřednictvím aplikace Peněženka přidáte svoji kreditní, debetní nebo předplacenou kartu, vaše zařízení odešle bezpečně informace o vaší kartě spolu s dalšími informacemi o vašem účtu a zařízení, ale vaše **skutečná čísla karet se nikdy neukládají** na zařízení ani na servery Apple, místo toho **je vytvořeno jedinečné číslo** účtu zařízení, které je vhodným způsobem **šifrováno**.

V obchodech jsou tedy platby zpracovávány pomocí tohoto jedinečného čísla a bezpečnostního kódu specifického pro transakci.

Karta Apple

Apple Card nám poskytuje užitečné funkce ze kterých můžeme vyčíst např. historii transakcí, souhrny výdajů, a to přímo v aplikaci Peněženka. Toto zabezpečení a ochrana osobních údajů brání společnosti Apple vědět co jste kde nakupovali apod.

Poziční služby

Tak jako u Androidu můžeme **udělovat oprávnění k sledování polohy**, a to jak pouze jednou, tak kdykoli ji budeme používat. Jestliže udělíme aplikaci oprávnění k sledování polohy, tak **budeme dostávat upozornění**, když aplikace bude používat naši polohu na pozadí. Tato upozornění nám také umožní si zobrazit mapu, který zobrazí místa, kde aplikace použila naši polohu.

Přihlášení Apple ID

Pro zjednodušení přihlášení k webům nám může sloužit Apple ID, a pokud nebudeme chtít sdílet svoji e-mailovou adresu s webem můžeme ji skrýt nebo můžeme zvolit, aby nám Apple vytvořil jedinečnou e-mailovou adresu. Pro přihlášení pomocí Apple ID je vyžadována **dvoufázová ověření**, tím je přístup k těmto účtům bezpečnější.

iCloud

iCloud nám slouží k ukládání zálohování našich dat, samozřejmě jsou také šifrovány. Tato data jsou chráněna klíčem, který je jedinečný pro naše zařízení a je kombinován s přístupovým kódem našeho zařízení, které známe pouze my.

Find My

Tato funkce nám **pomůže najít naše zařízení**, pokud se nám ztratilo nebo bylo odcizeno. Je povolena už **automaticky při přihlášení do služby iCloud** na novém zařízení. Další funkcí je také možnost vzdáleně vymazat osobní údaje. (Privacy - Features, 2020)

Dále bude vytvořen check-list s bezpečnostními funkcemi

5.3 Bezpečnostní funkce

Legenda: ✓ - obsahuje funkci (ovšem nemusí být bezpečná na stejné úrovni)

× - neobsahuje funkci (nemusí být bezpečná na stejné úrovni)

Tabulka 1: Bezpečnostní funkce

Funkce	Android	iOS
Ověřený obchod s aplikacemi	✓	✓
Ověření při instalování aplikace	✓	✓
Aplikace pro nalezení ztraceného zařízení	✓	✓
Kontrola udělování oprávnění	✓	✓
Měsíční bezpečnostní aktualizace (záleží na výrobci zařízení)	✓	✓
Šifrování zařízení	✓	✓
Integrovaná antivirová ochrana	✓	×
Touch ID (příp. pro služby)	×	✓
Face ID (příp. pro služby)	×	✓
Autorizace systémového softwaru	×	✓
Cloudové služby pro zálohy	✓	✓
Sandboxing (izolace aplikací)	✓	✓

6 ANALÝZA BEZPEČNOSTI OPERAČNÍCH SYSTÉMŮ ANDROID A IOS S VYUŽITÍM METODY MULTIKRITERIÁLNÍHO HODNOCENÍ

V této kapitole bude provedena analýza operačních systémů Android a iOS z hlediska bezpečnosti, za pomocí předem vybraných kritérií, které by měl splňovat bezpečný operační systém mobilních komunikačních zařízení dle mého názoru, aby byl co nejbezpečnější. Čím vyšší bude výsledná hodnota u operačního systému, tím bezpečnější operační systém je. K porovnání bude sloužit následující multikriteriální hodnocení.

6.1 Multikriteriální analýza

Abychom mohli zjistit, jestli dané kritérium vybraný operační systém splňuje či nikoliv, je nutné pro multikriteriální hodnocení použít následující vzorce:

- vzorec pro výpočet váženého průměru, předpokladem je soubor n hodnot:

$$X = \{x_1, \dots, x_n\}$$

- vzorec pro odpovídající váhu:

$$W = \{\omega_1, \dots, \omega_n\}$$

- kde je následně dán vzorec:

$$\bar{x} = \frac{\sum_{i=1}^{n} \omega_i x_i}{\sum_{i=1}^{n} \omega_i} \quad (1)$$

Jako komparační kritérium budou zvoleny dva nejpoužívanější operační systémy a tím bude Android a iOS.

Pro jednotlivé kritérium což je soubor n hodnot, je přidělena váha (ω), která označuje významnost tohoto kritéria. Čím vyšší bude hodnota, tím je toto kritérium důležitější pro celkovou bezpečnost tohoto operačního systému.

Tabulka 2: Hodnoty vah pro kritéria

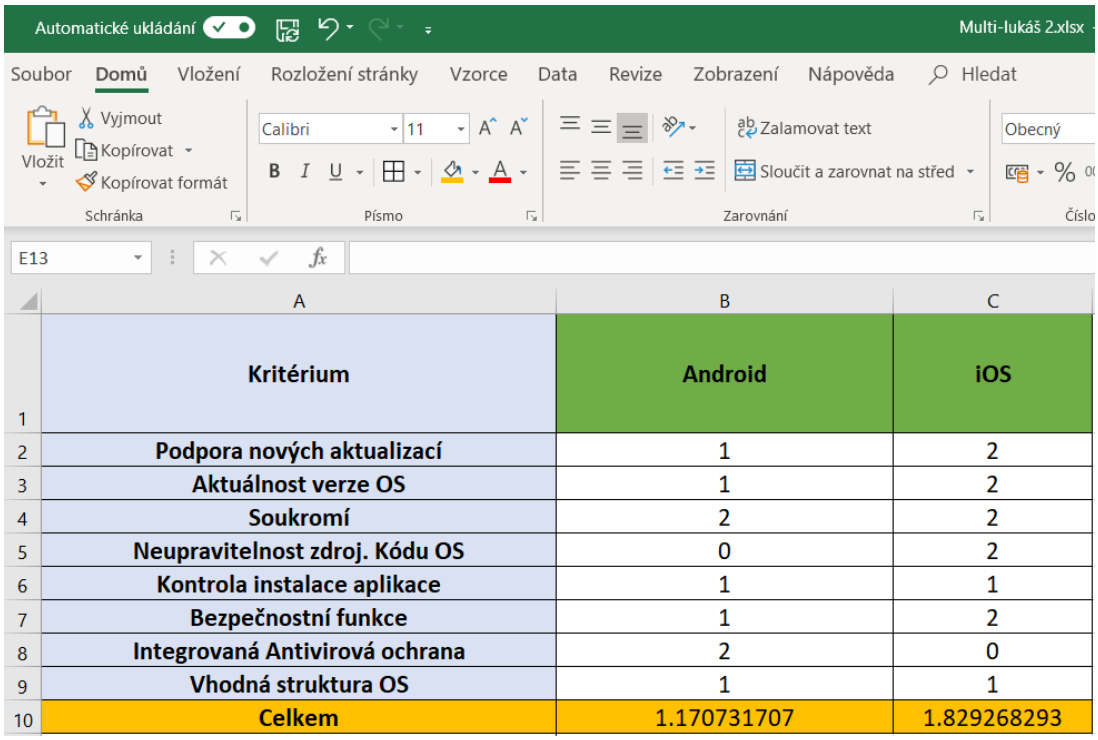
Kritérium	Přiřazená váha (ω)
Podpora nových aktualizací	10
Aktuálnost verze OS	9
Soukromí	8
Neupravitelnost zdroj. kódu OS	6
Kontrola instalace aplikace	4
Bezpečnostní funkce	2
Integrovaná antivirová ochrana	1
Vhodná struktura OS	1

- **Podpora nových aktualizací –** Podpora výrobcem OS, pravděpodobnost získání nové aktualizace OS.
- **Aktuálnost verze OS –** Nejvyšší dostupná verze OS.
- **Soukromí –** Prvky pro udržování soukromí uživatele napříč používáním celého zařízení.
- **Neupravitelnost zdroj. kódu OS –** Úprava zdrojového kódu pouze výrobcem OS nikoliv výrobcem zařízení.
- **Kontrola instalace aplikace –** Kontrola aplikace na přítomnost virů při instalaci do zařízení.
- **Bezpečnostní funkce –** Dostupnost šifrování, možnosti zámku obrazovky, Face ID, Touch ID apod.
- **Integrovaná antivirová ochrana –** Tovární předinstalovaný antivirový software.
- **Vhodná struktura OS –** Zabezpečení na úrovni hardwaru a struktury OS.

Další parametr vzorce pro vážený průměr je x, které značí číselné ohodnocení dané vlastnosti. Tento parametr se pohybuje v rozmezí od hodnoty 0 po hodnotu 2. Hodnota 0 značí že minimální splnění kritéria, 1 částečné splnění kritéria a 2 úplné splnění kritéria.

Pro zajištění přehledného výpočtu této multikriteriální analýzy bude vytvořena tabulka v aplikaci Microsoft Excel.

6.2 Výsledek multikriteriální analýzy



	A	B	C
1	**Kritérium**	**Android**	**iOS**
2	**Podpora nových aktualizací**	1	2
3	**Aktuálnost verze OS**	1	2
4	**Soukromí**	2	2
5	**Neupravitelnost zdroj. Kódu OS**	0	2
6	**Kontrola instalace aplikace**	1	1
7	**Bezpečnostní funkce**	1	2
8	**Integrovaná Antivirová ochrana**	2	0
9	**Vhodná struktura OS**	1	1
10	**Celkem**	1.170731707	1.829268293

Obrázek 14: Výsledek multikriteriální analýzy (zdroj: vlastní)

Pro výpočet celkové hodnoty pro Android byl použit výše zmíněný vzorec (1)

Po dosazení hodnot pro Android výpočet vypadá následovně:

$$\bar{x} = \frac{(1 \times 10) + (1 \times 9) + (2 \times 8) + (0 \times 6) + (1 \times 4) + (1 \times 2) + (2 \times 1) + (1 \times 1)}{41}$$

$$\bar{x} \doteq 1{,}170$$

Po dosazení hodnot pro iOS výpočet vypadá následovně:

$$\bar{x} = \frac{(2 \times 10) + (2 \times 9) + (2 \times 8) + (2 \times 6) + (1 \times 4) + (2 \times 2) + (0 \times 1) + (1 \times 1)}{41}$$

$$\bar{x} \doteq 1{,}829$$

6.2.1 Podpora nových aktualizací

Podpora nových aktualizací operačních systémů se u Androidu a iOS dost významně liší. U Androidu jsou ve většině podporována zařízení, která jsou jedny z těch nejnovějších a běží na nich čistý operační systém Android nebo spadají pod program Android One, kde mají tato zařízení garantována, že v následujících dvou letech budou dostávat aktualizace na nové verze operačního systému a měsíční záplaty bezpečnostních chyb. O něco hůře jsou na tom zařízení, která nemají čistý operační systém, ale mají na něm ještě nabalenou tzv. „nástavbu" kterou vyvíjí samotný výrobce zařízení nikoliv výrobce operačního systému. Tito výrobci jsou v podstatě s novými verzemi operačních systémů a bezpečnostními aktualizacemi neustále pozadu protože implementace nové verze operačního systému na již zmíněnou nadstavbu je poměrně složitá a vyžaduje čas. Tímto se vyznačují levnější zařízení např. od společnosti Huawei, Xiaomi, Honor apod.

Naopak uživatelé zařízení s operačním systémem iOS jsou na tom o výrazně líp. Podpora nových aktualizací operačního systému je u společnosti Apple jednou ze zásadních výhod, protože společnost Apple si zakládá na tom, že je potřeba udržovat a nezapomínat na starší zařízení, která vyžadují v podstatě vyšší péči. Nikoho z majitelů zařízení, na kterých běží operační systém iOS nezaskočí, že i když používá zařízení staré několik let, stále dostává aktualizace na nové verze operačního systému. Důvodem této zvýšené podpory také může být, že operační systém iOS je proprietární, takže ho může vyvíjet pouze Apple a uživatelé nejsou odkázaní na výrobce zařízení. Z tohoto důvodu jsem pro Android zvolil hodnotu 1 a pro iOS hodnotu 2.

6.2.2 Aktuálnost verze OS

Jako jedno z dalších kritérií jsem zvolil aktuálnost verze operačního systému, a to z toho důvodu, že na spousty zařízeních neběží nejaktuálnější verze obzvláště na zařízeních s operačním systémem Android, zastoupení verzí je hodně roztříštěné, naproti tomu zařízení s operačním systémem iOS mají ve většině nejaktuálnější verzi, proto starší verze může mít za následek zvýšení rizika obsahu závažných bezpečnostních trhlin. Toto kritérium je spojeno také s podporou nových aktualizací, a to velmi významně, protože jestli zařízení nedostane aktualizaci na novější verzi operačního systému, nemůže na něm tedy běžet aktuální verze s nejnovějšími opravami a vylepšeními z hlediska bezpečnosti. Proto jsem se rozhodl pro Android zvolit hodnotu 1 a pro iOS hodnotu 2.

6.2.3 Soukromí

Soukromí na obou operační systémech bych považoval za velmi dobré. Jak už bylo výše zmíněno v samostatné kapitole zabezpečení a soukromí, oba operační systémy se opravdu snaží naše data, přístupové údaje, fotky, zprávy chránit před možným vyzrazením nebo odcizením. Oba dva tyto operační systémy samozřejmě šifrují tyto data, protože jsou pro nás velmi důležitá. O jednu výhodu navíc má ovšem operační systém iOS, který používá pro různá přihlášení nebo vyplnění údajů, platebních transakcí službu Apple ID, který funguje na bázi ověření otisku prstu, ovšem oba dva operační systémy si v ochraně soukromí vedou opravdu dobře dle mého názoru. Z tohoto důvodu jsem pro oba operační systémy zvolil hodnotu 2.

6.2.4 Neupravitelnost zdrojového kódu OS

Co se týká neupravitelnosti zdrojového kódu operačních systémů bych zmínil že, tato vlastnost může být přínosem pro vývoj operačního systému v budoucnosti, ale také může být poměrně závažnou bezpečnostní hrozbou pro tyto operační systémy. Dle mého názoru si myslím, že moderní operační systém a jeho zdrojový kód by neměl být upravitelný, protože zde vzniká už zmíněné bezpečnostní riziko. Android má otevřený zdrojový kód a tím pádem ho může kdokoliv upravit např. výrobce zařízení a vytvořit na něj onu nástavbu. Výhoda ovšem může spočívat v tom, že uživatelé nebo různí nadšenci mohou do Androidu naprogramovat nějaké funkce a mohou napovědět oficiálním vývojářům např. jaké funkce by mohli do nové verze operačního systému naprogramovat a tím vylepšit operační systém anebo navrhnout úpravy pro zlepšení bezpečnosti. Horší verze je že, zdrojový kód operačního systému jim poskytne určité vodítko, jak by se dalo zabezpečení operačního systému obejít a napadnout jej. Naproti tomu operační systém iOS má neupravitelný kód, takže tím pádem vývoj se upírá pouze na společnost Apple a nikdo jiný jej nemůže upravovat. Z tohoto důvodu jsem se rozhodl pro razantní hodnocení, a to pro Android hodnotu 0 a pro iOS hodnotu 2.

6.2.5 Kontrola instalace aplikace

Kontrola instalace nových aplikací je už dnes používána oběma operačními systémy. Protože aplikace je jedna z dalších možností, jak do zařízení vpustit infikovaný kód je nutné při instalaci nových aplikací provést kontrolu, zda tato aplikace neobsahuje onen infikovaný kód nebo nebude shromažďovat data pro následný možný únik těchto informací. Oba dva operační systémy mají tyto kontroly implementovány přes vlastní obchody s aplikacemi, takže by se mohlo zdát, že je o bezpečnost nově nainstalované aplikace postaráno. Nemusí tomu být opravdu tak, protože pořád existuje možnost, jak do zařízení nainstalovat aplikaci, která neprošla kontrolou přes ony obchody s aplikacemi. Jak u Androidu, tak i u iOS je možné přes zvláštní povolení instalace neověřených aplikací v nastavení instalovat potenciálně škodlivé aplikace, které neprošly kontrolou. Tyto možnosti by dle mého názoru pro zachování bezpečnosti při instalaci nových aplikací neměly být přístupné, protože by mohlo vzniknout riziko napadení zařízení anebo únik dat. Proto jsem se rozhodl zvolit stejnou hodnotu 1 jak pro Android, tak pro iOS.

6.2.6 Bezpečnostní funkce

Bezpečnostní funkce jsou dle mého názoru na obou operačních systémech velmi podobné a v daných okolnostech poměrně dostačující. Pod bezpečnostní funkce bychom mohli zařadit např. šifrování, dostupné antivirové softwary z obchodu Google Play nebo App Store, cloudová úložiště, aplikace spojené s nalezením ztraceného zařízení apod. Co se týče možností uzamčení obrazovky, jsou na tom oba operační systémy poměrně stejně, protože nabízejí dnes už standardní ověřování otisku prstu anebo ověřování obličeje. Za zmínku ovšem stojí funkce Apple ID – služba pro bezpečnější přihlašování na webu, nakupování aplikací apod., která byla vzpomenuta už výše a kterou nalezneme pouze u operačního systému iOS. Tuto funkci považuji za velmi vhodnou pro udržení soukromí na internetu. Z tohoto důvodu jsem se rozhodl pro Android hodnotu 1 a pro iOS hodnotu 2.

6.2.7 Integrovaná antivirová ochrana

Pouze jeden z těchto operačních systému má většinou integrovanou antivirovou ochranu jako součást aplikace pro správu telefonu a tím je Android. V dnešní době je vhodné, jak na počítačích mít antivirový software, tak i na mobilních zařízeních aspoň ve formě této integrované ochrany součástí aplikace. Virů, které se šíří napříč celým internetem, aplikacemi apod. je celá řada, a proto bych považoval integrovanou antivirovou ochranu za další možnost, jak se proti těmto nectnostem chránit, ovšem pro zvýšení zabezpečení zařízení bych doporučoval nainstalovat ještě plnohodnotnou antivirovou aplikaci z obchodů s aplikacemi. Tato integrovaná antivirová ochrana je základem pro zvýšení zabezpečení zařízení a dle mého názoru by měla být součástí moderních operačních systémů. Operační systém iOS tuto integrovanou ochranu nemá, ale stále mají možnost uživatelé si nainstalovat samotnou antivirovou aplikaci. Z tohoto důvodu jsem se rozhodl Androidu udělit hodnotu 2 a iOS hodnotu 0.

6.2.8 Vhodná struktura OS

Dnešní operační systémy mobilních komunikačních zařízení mají integrovaná opatření pro zvýšení bezpečnosti pomocí hardwaru už v samotné struktuře operačního systému. Bohužel pokud se v samotné struktuře operačního systému nebo v určitém kusu hardwaru nachází bezpečnostní chyba, pravděpodobnost, že se tato chyba podaří opravit je prakticky nulová. Chyba např. v čipu by se dala opravit pouze výměnou onoho čipu zařízení. Tato možnost je prakticky k ničemu, takže pokud má zařízení bezpečnostní chybu už v tomto čipu je vysoce pravděpodobné, že k její opravě nikdy nedojde, pouze onou výměnou celého zařízení. Tento problém by se dal vyřešit tím, že by se daly určité části hardwaru snadno vyměnit, což by mohlo být ale složité, časově náročné a drahé. Proto jsem se z tohoto důvodu rozhodl pro oba operační systémy zvolit hodnotu 1.

6.3 Shrnutí multikriteriální analýzy

Z výzkumu můžeme dojít k závěru, že celková bezpečnost operačních systémů Android a iOS je do určité míry rozdílná.

Základ bezpečnosti operačního systému musí tvořit samotný vývojář operačního systému, dalším článkem pak až samotný uživatel. Nic nemění na tom, že oba dva operační systémy jsou vhodně vyvíjeny směrem kupředu co se týče podpory nových aktualizací a aktuálnosti verze operačního systému, ale v tomto ohledu si přece jen o kousek vede firma Apple a její operační systém iOS opravdu lépe, a to konkrétně ve větší podpoře starších zařízení.

V dnešní době je velká část bezpečnosti také věnována tématu Soukromí uživatelů při používání jakéhokoliv zařízení. V oblasti soukromí si oba dva operační systémy vedou poměrně dobře že šifrují naše data, aby nedošlo k nechtěnému úniku našich citlivých informací, ovšem zde si o něco lépe vede opět operační systém iOS, a to konkrétně službou Apple ID, která se používá centrálně v celém operačním systému pro chránění našich dat.

Dalším tématem byla neupravitelnost zdrojového kódu, kde Android je open-source operační systém, což může mít své výhody ale také nevýhody z hlediska bezpečnosti. Naopak operační systém iOS je uzavřený a vyvíjet a upravovat ho může pouze samotná firma Apple.

Následující kritérium byla kontrola při instalaci nových aplikací. Tato kontrola je opravdu vhodná, protože neustále na svá zařízení instalujeme další nové aplikace, a i ty je potřeba nejprve zkontrolovat. Ovšem oba dva systémy umožňují při poměrně malém zásahu do nastavení nainstalovat i aplikace z neověřených zdrojů, což není zrovna bezpečné.

Bezpečnostních funkcí pro oba systémy je celá řada (šifrování, antivirové softwary, cloudová úložiště aj.), ale bezpečnostních funkcí není nikdy dostatek. V této části si celkově vedl zase iOS, ačkoliv nedisponuje integrovanou antivirovou ochranou Androidu.

Poslední částí analýzy byla vhodná struktura operačních systémů, která se týká např. integrovaných bezpečnostních opatření už v samotném hardwaru zařízení. I v této oblasti stále vývojáři neví, jak přesně tyto opatření nejvhodněji zavádět do zařízení, přičemž aby byly co nejjednodušší a nejlevnější, ale stále kvalitní.

7 ZÁKLADNÍ MOŽNOSTI ZABEZPEČENÍ ZAŘÍZENÍ

V dnešní době narůstá počet hackerských útoků a mobilní zařízení jsou zranitelná než kdy dřív. Zajištění zabezpečení mobilního zařízení můžeme rozdělit na dvě úrovně. První úroveň zabezpečení zařízení vytváří už samotní vývojáři operačního systému, kteří integrují do svého hardwaru a operačního systému řadu ochran pro bezpečnost. Tato úroveň byla popsána už výše, a nyní je čas zmínit některé možnosti které už závisí pouze na uživateli, zda je aplikuje nebo je bude používat a sníží tak pravděpodobnost úniku citlivých dat a informací.

7.1 Aktualizace aplikací a systému

Aktualizace aplikací je tou jednodušší částí tou získáme jak nové funkce, ale hlavně že aplikace bude více „bezpečnější“. Aplikace se aktualizují buď automaticky nebo po udělení souhlasu. Na Androidu se aplikace aktualizují přes Google Play a na iOS přes App Store. Každou další verzí aplikace se vývojáři snaží opravit objevené chyby, bezpečnostní trhliny apod.

Aktualizace systému je bezpochyby tou důležitější částí. Každý výrobce operačního systému či mobilního zařízení přistupuje k aktualizacím jinak. Existují dva způsoby, jak docílit nejaktuálnějšího a více bezpečnější verze operačního systému:

- **Tzv. over the air (OTA)** (vzduchem) – Tento způsob je nejpoužívanější a funguje tak že, jakmile je dostupná nová verze operačního zařízení vám automaticky stáhne a nainstaluje novou verzi operačního systému. Pokud tomu tak není tak je potřeba jít do nastavení telefonu či zařízení a pod položkou Systém zvolit Aktualizace softwaru ručně.
- **Kabelem** – V tomto případě se operační systém neaktualizuje sám a je zapotřebí ho připojit USB kabelem např. do počítače a přes výrobcem určený program nebo aplikaci ručně novou aktualizaci stáhnout a nainstalovat. Tento způsob výrobci zařízení postupně opouští.

Problém v těchto aktualizacích spočívá v tom, že nevíte, kdy a jakou aktualizaci vaše zařízení dostane. Toto ovlivňují pouze výrobci vašeho zařízení nikoliv operačního systému, jak je tomu u dražších telefonech. Nejvíce dlouhodobá podpora je zaručena pro zařízení vyráběná přímo společností, která vyvíjí i onen operační systém.

Další možností, jak mít větší šanci, že vaše zařízení dostane novou aktualizaci operačního systému je zakoupit telefon z některých programů jakým je např. **Android One**. Horší situace je pak u zařízeních, které běží na tzv. nástavbě na operačním systému např. MIUI (Xiaomi), EMUI (Huawei) a jim podobné, kde doba pro vydání nové aktualizace operačního systému je o hodně delší než u telefonů s čistým operačním systémem. (Jak aktualizovat Android, 2020)

Anroid One je označení pro zařízení, kde **výrobce garantuje, že zařízení bude dostávat nové aktualizace operačního systému po dobu dvou let a měsíční bezpečnostní aktualizace po dobu tří let.** Zařízení spadající do programu Android One používají čistý operační systém. Heslo programu Android One zní: „Bezpečnost, aktuálnost a jednoduchost používání“. (Android One: Secure, up-to-date and easy to use, 2020)

7.2 Cloudové nástroje

Cloudové služby nebo nástroje využívají tzv. cloud computing, což jsou v podstatě jsou servery, úložiště, služby a aplikace dostupné uživateli vzdáleně na síti a nezabírají nám paměť v zařízení. Důležitou výhodou těchto služeb a nástrojů je, že si můžeme vybrat jaká data budeme na Cloud zálohovat. Kdyby totiž došlo k ztrátě nebo odcizení zařízení nebo i napadení zařízení útočníky, tak tyto data máme uložená na Cloudu. K těmto datům ale může mít přístup třetí strana.

Pro využívání některých cloudových služeb není ani zapotřebí instalace nějaké aplikace, stačí když se uživatel do nich přihlásí skrze klientské prostředí na internetu a automaticky dostane omezenou velikost prostoru pro nahrání svých dat. Mezi nejznámější Cloudové nástroje patří: Microsoft Onedrive, Google Drive, iCloud, Dropbox. (Cloudové služby, 2013-2017)

7.3 Šifrování dat

Šifrování v mobilních zařízení je integrované už v operačních systémech, funguje tak, že jakmile se telefon uzamkne, dojde k zašifrování dat. Při odemknutí zařízení musíme zadat PIN nebo otisk prstu, tím dojde k dešifrování. Znemožní odemknutí zařízení při jeho případné ztrátě nebo krádeži.

Na zařízení s Androidem je v nastavení sekci Osobní zabezpečení možnost šifrovat zařízení. Při tomto procesu je nutné připojit nabíječku. Poté budete vyzváni k zvolení hesla,

bezpečnostního gesta nebo PIN kódu pro dešifrování. Po tomto procesu se dešifrovací klíč bezpečně uloží v Androidu. Možné je také zašifrovat i SD kartu v telefonu.

Pro zašifrování zařízení s iOS v nastavení slouží položka Touch ID a Face ID, dále přístupový kód, následně musíme zadat silné heslo skládající se z písmen, číslic, popř. symbolů.

Šifrování konverzací v aplikacích např. Messenger, WhatsApp nebo Viber nebo i iMessage využívá end-to-end šifrování, takže riziko zde vzniká to, že nevíme, kdo má k dispozici klíče pro dešifrování a ten by popř. byl ochotný tyto klíče předat nějaké např. vládní organizaci.

Toto šifrování běží neustále na pozadí, takže se šifrují i nové a aktuálně používané soubory. (Šifrování dat, c2015-2020)

7.4 Antivirus

V prvé řadě je potřeba si uvědomit, že v dnešní době nejsou telefony už jen na telefonování a posílání SMS zpráv, ale většina uživatelů zde může ukládat důležitá data, fotky, nebo např. využívat přístupu do svého účtu skrz internetové bankovnictví nebo přes mobilní aplikace. Všechny tyto data mohou útočníky lákat na získání těchto dat pomocí nějakého útoku. Na to, aby se nám do telefonu dostal virus mohou stačit i pouhé každodenní aktivity, surfování na internetu, stahování aplikací, otevírání e-mailových příloh apod. Nejčastěji se do telefonu dostane virus skrz kliknutí na reklamu nebo infikovaný odkaz např. v e-mailu nebo v SMS zprávě. Další možností, jak se může virus do zařízení dostat jsou bezpečnostní chyby v operačních systémech. Některá tzv. „zadní dvířka“, která výrobci nechávají v operačních systémech záměrně mohou také sloužit k obejití zabezpečení zařízení, pokud o nich kdokoliv ví. Různé obchody a platformy které nabízejí aplikace pro Android, tak mají právě méně odpovědný proces schvalování nových aplikací, a právě tím se zde mohou dostat potenciálně infikované aplikace, které mohou obsahovat viry.

Naopak iOS má bezpečnější schvalování nových aplikací díky přísnějším pravidlům pro ověření nových aplikací – bezpečnostním aplikacím umožňují pouze omezené skenování, např. jen příloh e-mailů nebo jednoho určitého souboru. Mezi nejpoužívanější antivirové softwary patří např. Avast, Avira, ESET nebo Kaspersky. (Je potřeba Antivirus i na telefon?, c2011-2020)

Legenda: ✓ - dostupný pro daný operační systém

× - nedostupný pro daný operační systém

Tabulka 3: Dostupné antivirové softwary

Název	Android	iOS
AVG	✓	✓
Avast	✓	✓
ESET	✓	×
Kaspersky	✓	×
Avira	✓	✓
McAfee	✓	✓
Norton	✓	✓

Zde je výčet nejpoužívanějších a nejznámějších dostupných antivirových softwarů pro operační systémy Android a iOS.[1]

[1] zdroj: Google Play, (Je potřeba Antivirus i na telefon?, c2011-2020) (Petřík, 2020) (5 nejlepších (OPRAVDU BEZPLATNÝCH) antivirových aplikací pro iPhone a iPad 2020, 2020) [1]

ZÁVĚR

V dnešní době má každý z nás mobilní zařízení a jeho součástí je také operační systém. Na mobilech a jiných zařízeních máme uložená různá citlivá data jakými jsou např. přihlašovací údaje, telefonní čísla, přihlašovací kódy k internetovému bankovnictví, ale také fotografie apod.

Z tohoto důvodu je také nutné tyto mobilní zařízení chránit a snažit se udržovat tyto naše data bezpečně uložená. Hlavním článkem ochrany a zabezpečení našeho zařízení je operační systém. Ten by měl vytvořit jakýsi základ kvalitní ochrany našich dat.

Dnešní mobilní operační systémy mají celou řadu bezpečnostních funkcí, ale vzhledem k tomu že čas je neúprosný, tak i útočníci hledají další a další slabá místa našich zařízení jak nás o naše drahocenná data, dokonce finanční prostředky připravit.

Proto je tedy nutné, když to jenom jde neustále se snažit udržovat naše mobilní telefony a jiná zařízení bezpečné a zvyšovat jejich zabezpečení. K tomu nám mohou dopomoct různé antivirové softwary či další z mnoha služeb pro zvýšení zabezpečení zařízení.

Byla zpracována rešerše a definice základních pojmů a legislativa týkající se předmětné problematiky. Dalšími cíli byla dále identifikace současných operačních systémů mobilních komunikačních zařízení, následně analýza struktury vybraných operačních systémů a pojednání o jejich zranitelnostech. Posledním cílem byla komparace bezpečnosti vybraných operačních systémů s za pomocí multikriteriální analýzy a specifikace opatření pro zvýšení celkové bezpečnosti.

Na základě těchto informací docházíme k závěru, že nejbezpečnější operační systém mobilních komunikačních zařízení je operační systém iOS vyvíjený společností Apple. Operační systém iOS si vede ve většině kritérií bezpečnosti velmi dobře a to např. v podpoře nových aktualizací, udržování soukromí uživatelů a v neposlední řadě bezpečnostních funkcích, i za cenu vyšších pořizovacích nákladů na zařízení s tímto operačním systémem.

Jako vhodným doplněním pro zvýšení celkové bezpečnosti zařízení bych zvolil jeden z dostupných antivirových softwarů např. Avast. Velká odpovědnost na bezpečnosti našich mobilních zařízení stále zůstává na výrobcích těchto operačních systémů a ti by se měli snažit celkovou bezpečnost operačního systému neustále zlepšovat.

Cíle bakalářské práce byly splněny.

SEZNAM POUŽITÉ LITERATURY

5 nejlepších (OPRAVDU BEZPLATNÝCH) antivirových aplikací pro iPhone a iPad 2020, 2020. *Cs.safetydetectives.com* [online]. [cit. 2020-04-02]. Dostupné z: https://cs.safetydetectives.com/blog/nejlepsich-opravdu-zdarma-antiviru-pro-ios/

Android One: Secure, up-to-date and easy to use, 2020. *Android* [online]. Google LLC. [cit. 2020-03-29]. Dostupné z: https://www.android.com/one/

Apple Platform Security, 2019. *Apple* [online]. California, USA: Apple Inc. [cit. 2020-01-02]. Dostupné z: https://support.apple.com/cs-cz/guide/security/welcome/web

ARMIN, 2019. New Logo and Identity for Android. In: *Brand New* [online]. Bloomington: UnderConsideration LLC [cit. 2019-11-08]. Dostupné z: https://www.underconsideration.com/brandnew/archives/new_logo_and_identity_for_android_by_huge.php

Autentizace, ověření, identifikace (Authentication) [online], 2018. Wilmington: Magementmania.com [cit. 2019-11-21]. Dostupné z: https://managementmania.com/cs/autentizace-identifikace

Authentication [online], 2018. Sharpened Productions [cit. 2019-11-21]. Dostupné z: https://techterms.com/definition/authentication

Autorizace, oprávnění (Authorization) [online], 2017. Wilmington: Managementmania.com [cit. 2019-11-21]. Dostupné z: https://managementmania.com/cs/autorizace

BEAL, Vangie, 2011. Mobile Operating Systems (Mobile OS) Explained. *Webopedia.com* [online]. Foster City: QuinStreet, Inc. [cit. 2019-11-08]. Dostupné z: https://www.webopedia.com/DidYouKnow/Hardware_Software/mobile-operating-systems-mobile-os-explained.html

Cloudové služby, 2013-2017. *Wikisofia* [online]. Praha: Wikisofia.cz [cit. 2020-02-22]. Dostupné z: https://wikisofia.cz/wiki/Cloudov%C3%A9_slu%C5%BEby

ČERMÁK, Miroslav, 2011. Informační bezpečnost. *Cleverandsmart Management Consulting* [online]. Miroslav Čermák [cit. 2019-11-21]. Dostupné z: https://www.cleverandsmart.cz/informacni-bezpecnost/

ČÍŽEK, Jakub, 2019. Nejděravější firmy a programy roku 2019: Android, Debian a Windows. *Živě.cz* [online]. Praha: CZECH NEWS CENTER a.s. [cit. 2020-03-06].

Dostupné z: https://www.zive.cz/clanky/nejderavejsi-firmy-a-programy-roku-2019-android-debian-a-windows/sc-3-a-202743/default.aspx

Google zjistil obří bezpečnostní chybu v Androidu z roku 2017. Využívala ji izraelská organizace, 2019. *Gamebro.cz* [online]. Praha: Gamebro [cit. 2020-01-31]. Dostupné z: https://www.gamebro.cz/google-zjistil-obri-bezpecnostni-chybu-v-androidu-z-roku-2017-vyuzivala-ji-izraelska-organizace/

HÁK, Igor, 2018. Kauza QRecorder, milióny Kč pryč. Na co si dát příště pozor?. *VIRY.CZ* [online]. Praha [cit. 2020-03-29]. Dostupné z: https://www.viry.cz/kauza-qrecorder-miliony-kc-pryc-na-co-si-dat-priste-pozor/

CHAU, Melissa a Ryan REITH, 2020. Smartphone Market Share: OS Data Overview. *IDC.com* [online]. Framingham: IDC [cit. 2019-11-21]. Dostupné z: https://www.idc.com/promo/smartphone-market-share/os

IOS Apple, c1999–2019. *Aktuálně.cz* [online]. Praha: Economia, a.s. [cit. 2019-12-07]. Dostupné z: https://www.aktualne.cz/wiki/veda-a-technika/ios-apple/r~i:wiki:1558/

IOS logo, c2016-2019. In: *1000 Logos - The Famous Brands and Company Logos in the World* [online]. 1000logos.net [cit. 2019-11-21]. Dostupné z: https://1000logos.net/ios-logo/

Jak aktualizovat Android, 2020. *Radírna.cz* [online]. Radírna - Internetová online poradna [cit. 2020-02-22]. Dostupné z: https://www.radirna.cz/mobily/jak-aktualizovat-android.html

Jak vypadá Android uvnitř?, 2011. *Androidmarket.cz* [online]. [cit. 2019-11-23]. Dostupné z: https://androidmarket.cz/android/jak-vypada-android-uvnitr-aneb-co-je-rom-kernel-bootloader-a-dalsi/

Je potřeba Antivirus i na telefon?, c2011-2020. *Letem světem Applem* [online]. Brno: Text Factory s. r. o. [cit. 2020-02-28]. Dostupné z: https://www.letemsvetemapplem.eu/2017/07/03/potrebuji-antivirus-telefon/

JIRÁSEK, Petr, Luděk NOVÁK a Josef POŽÁR, 2015. *Výkladový slovník kybernetické bezpečnosti: Cyber security glossary*. Třetí aktualizované vydání. Praha: Policejní akademie ČR v Praze. ISBN 978-80-7251-436-6.

KLUSKA, Vladislav, 2019. Android obsahoval chybu, kvůli které šel napadnout PNG obrázkem. *Živě.cz* [online]. Praha: CZECH NEWS CENTER a.s. [cit. 2020-01-31]. Dostupné z: https://www.zive.cz/clanky/android-obsahoval-chybu-kvuli-ktere-sel-napadnout-png-obrazkem/sc-3-a-197134/default.aspx

KOLOUCH, Jan, 2016. *CyberCrime*. 1. vydání. Praha: CZ.NIC, z.s.p.o. CZ.NIC. ISBN 978-80-88168-15-7.

KOLOUCH, Jan a Pavel BAŠTA, 2019. *CyberSecurity*. Praha: CZ.NIC, z.s.p.o. CZ.NIC. ISBN 978-80-88168-31-7.

LUCIDEUS, 2019. Understanding the Structure of an iOS Application. In: *Medium - Get smarter about what matters to you* [online]. A Medium Corporation [cit. 2019-12-07]. Dostupné z: https://medium.com/@lucideus/understanding-the-structure-of-an-ios-application-a3144f1140d4

PALYZA, Jiří, 2018. Nezáplatovatelná zranitelnost: ohrožuje miliony smartphonů Apple. *Chip.cz* [online]. Praha: Burda International CZ s.r.o. [cit. 2020-01-31]. Dostupné z: https://www.chip.cz/novinky/nezaplatovatelna-zranitelnost-ohrozuje-miliony-smartphonu-apple/

PETŘÍK, Jiří, 2020. Pozor na malware a antivirový software na iOS. *Be Apple Pro* [online]. Praha: Be Apple Pro [cit. 2020-04-02]. Dostupné z: https://www.beapple.pro/aplikace/pozor-na-malware-a-antivirovy-software-na-ios/

Privacy - Features, 2020. *Apple* [online]. California, USA: Apple Inc. [cit. 2020-01-28]. Dostupné z: https://www.apple.com/privacy/features/

Privacy best practises, 2019. *Android Developers* [online]. [cit. 2020-01-28]. Dostupné z: https://developer.android.com/privacy/best-practices#pay_attention_to_permissions

REMAKER, Phillip, 2018. How different are MacOS and Darwin OS?. *Quora - A place to share knowledge and better understand the world* [online]. © Quora Inc. 2019 [cit. 2019-12-07]. Dostupné z: https://www.quora.com/How-different-are-MacOS-and-Darwin-OS

Secure an Android Device, 2020. *Android Open Source Project* [online]. [cit. 2019-11-23]. Dostupné z: https://source.android.com/security

Security, 2020. *Apple Developer* [online]. California, USA: Apple Inc. [cit. 2020-03-29]. Dostupné z: https://developer.apple.com/documentation/security

SMITH, David, 2020. IOS Version Stats. *David Smith, Independent iOS Developer* [online]. Virginia, USA: David Smith [cit. 2019-12-07]. Dostupné z: https://david-smith.org/iosversionstats/

Stovky milionů mobilů v ohrožení. Oprava nebezpečné trhliny chybí, 2019. *Novinky.cz* [online]. Praha: Borgis a.s. [cit. 2020-01-31]. Dostupné z: https://www.novinky.cz/internet-a-pc/bezpecnost/clanek/stovky-milionu-mobilu-v-ohrozeni-oprava-nebezpecne-trhliny-chybi-40299023

StrandHogg: Serious Android vulnerability leaves most apps vulnerable to attacks, 2006. *Promon* [online]. Norsko: Promon AS [cit. 2020-01-31]. Dostupné z: https://promon.co/security-news/strandhogg/

Šifrování dat, c2015-2020. *Advokta* [online]. Brno: Advokta [cit. 2020-02-22]. Dostupné z: https://www.advokta.cz/blog/navod-jak-nastavit-sifrovani-dat-v-mobilu/

ŠKORNIČKOVÁ, Eva, 2018. Citlivé osobní údaje. *GDPR | Obecné nařízení o ochraně údajů - prakticky* [online]. GDPR.cz [cit. 2019-11-21]. Dostupné z: https://www.gdpr.cz/gdpr/heslo/citlive-osobni-udaje/

ŠKORNIČKOVÁ, Eva, 2018. Osobní údaje. *GDPR | Obecné nařízení o ochraně údajů - prakticky* [online]. GDPR.cz [cit. 2019-11-21]. Dostupné z: https://www.gdpr.cz/gdpr/heslo/osobni-udaje/

ŠKUTA, Petr, 2018. Chyby v iOS umožnily hacknout iPhone jen přes webovou stránku. Odhalil je až Google. *Jablíčkář.cz* [online]. Brno: Text Factory s. r. o. [cit. 2020-01-31]. Dostupné z: https://jablickar.cz/chyby-v-ios-umoznily-hacknout-iphone-jen-pres-webovou-stranku-namisto-applu-je-odhalil-google/

Top 7 Mobile Security Threats: Smart Phones, Tablets, & Mobile Internet Devices – What the Future has in Store, 2020. *Kaspersky* [online]. Moskva, Rusko: AO Kaspersky Lab. [cit. 2020-02-22]. Dostupné z: https://www.kaspersky.com/resource-center/threats/top-seven-mobile-security-threats-smart-phones-tablets-and-mobile-internet-devices-what-the-future-has-in-store

Understanding Xamarin iOS - Build Native iOS App, 2019. *Dot Net Tricks* [online]. Indie: Dot Net Tricks Innovation [cit. 2019-12-07]. Dostupné z: https://www.dotnettricks.com/learn/xamarin/understanding-xamarin-ios-build-native-ios-app

VÁCLAVÍK, Lukáš, 2020. Android 10 má 8% podíl, „devítka“ okupuje třetinu zařízení. *Cnews.cz | Od tranzistorů až po PC sestavy* [online]. Praha: Mladá fronta a. s. [cit. 2020-04-15]. Dostupné z: https://www.cnews.cz/android-statistiky-duben-2020

VACULÍK, Přemysl, 2010. Android má závažnou chybu v multitaskingu, útočníci mohou odcizit cokoliv. *Dotekománie.cz* [online]. [cit. 2020-01-31]. Dostupné z: https://dotekomanie.cz/2019/12/android-ma-zavaznou-chybu-v-multitaskingu-utocnici-mohou-odcizit-cokoliv/

Vulnerabilities and threats in mobile applications, c2002-2020. *Positive Technologies* [online]. Londýn, UK: Positive Technologies [cit. 2020-02-22]. Dostupné z: https://www.ptsecurity.com/ww-en/analytics/mobile-application-security-threats-and-vulnerabilities-2019/

SEZNAM POUŽITÝCH SYMBOLŮ A ZKRATEK

GDPR Obecné nařízení o ochraně osobních údajů (General Data Protection Regulation)

IT Informační technologie (Information Technologies)

IDC Mezinárodní datová společnost (International Data Corporation)

OS Operační systém (Operating System)

SEZNAM OBRÁZKŮ

SEZNAM TABULEK