Bezpečnost mobilních zařízení z pohledu uživatele

Ondřej Kubáček

Bakalářská práce
2018

Univerzita Tomáše Bati ve Zlíně
Fakulta aplikované informatiky

Univerzita Tomáše Bati ve Zlíně
Fakulta aplikované informatiky
akademický rok: 2017/2018

ZADÁNÍ BAKALÁŘSKÉ PRÁCE
(PROJEKTU, UMĚLECKÉHO DÍLA, UMĚLECKÉHO VÝKONU)

Jméno a příjmení:	**Ondřej Kubáček**
Osobní číslo:	**A14252**
Studijní program:	**B3902 Inženýrská informatika**
Studijní obor:	**Informační technologie v administrativě**
Forma studia:	**prezenční**
Téma práce:	**Bezpečnost mobilních zařízení z pohledu uživatele**
Téma anglicky:	**The Security of Mobile Devices from the User's Perspective**

Zásady pro vypracování:

1. **Seznamte se s OS Android a jeho historií.**
2. **Popište nejčastější hrozby a rizika z pohledu uživatele OS Android.**
3. **Analyzujte chování uživatelů při práci s OS Android.**
4. **Proveďte analýzu dostupných aplikací ve službě Google Play a požadovaných oprávnění se zaměřením na potenciální zneužití.**
5. **K analýze využijte běžně dostupné nástroje.**
6. **Navrhněte stručnou metodiku jak se účinně bránit a chovat při práci s OS Android.**

Rozsah bakalářské práce:

Rozsah příloh:

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

Seznam odborné literatury:

1. **UJBÁNYAI, Miroslav. Programujeme pro Android. Praha: Grada, 2012. Průvodce (Grada). ISBN 978-80-247-3995-3.**
2. **HERODEK, Martin. 333 tipů a triků pro Android: [sbírka nejužitečnějších postupů a řešení]. Brno: Computer Press, 2014. ISBN 978-80-251-4310-0.**
3. **MAN Ho. Raymond Choo. Mobile security and privacy: advances, challenges and future research directions. Syngress, 2016 ISBN 978-01-280-4746-0**
4. **MISRA Anmol and Abhishek DUBEY. Android security: attacks and defenses. Boca Raton, Fla: CRC Press, 2013. ISBN 1439896461.**
5. **SUJITHRA M. and Padmavathi G. Mobile Device Security: A Survey on Mobile Device Threats, Vulnerabilities and their Defensive Mechanism. International Journal of Computer Applications [online]. 2012-10-20, vol. 56, issue 14, s. 24-29 [cit. 2017-01-31]. Dostupné z: http://research.ijcaonline.org/volume56/number14/pxc3883163.pdf**

Vedoucí bakalářské práce: **Ing. Lukáš Králík**
Ústav počítačových a komunikačních systémů

Datum zadání bakalářské práce: **1. prosince 2017**

Termín odevzdání bakalářské práce: **25. května 2018**

Ve Zlíně dne 14. prosince 2017

doc. Mgr. Milan Adámek, Ph.D.
děkan

L.S.

UNIVERZITA TOMÁŠE BATI VE ZLÍNĚ
Fakulta aplikované informatiky

doc. Ing. Martin Sysel, Ph.D.
garant oboru

Jméno, příjmení: Ondřej Kubáček

Název bakalářské práce: Bezpečnost mobilních zařízení z pohledu uživatele

Prohlašuji, že

- beru na vědomí, že odevzdáním bakalářské práce souhlasím se zveřejněním své práce podle zákona č. 111/1998 Sb. o vysokých školách a o změně a doplnění dalších zákonů (zákon o vysokých školách), ve znění pozdějších právních předpisů, bez ohledu na výsledek obhajoby;
- beru na vědomí, že bakalářská práce bude uložena v elektronické podobě v univerzitním informačním systému dostupná k prezenčnímu nahlédnutí, že jeden výtisk bakalářské práce bude uložen v příruční knihovně Fakulty aplikované informatiky Univerzity Tomáše Bati ve Zlíně a jeden výtisk bude uložen u vedoucího práce;
- byl/a jsem seznámen/a s tím, že 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;
- beru na vědomí, že podle § 60 odst. 1 autorského zákona má UTB ve Zlíně právo na uzavření licenční smlouvy o užití školního díla v rozsahu § 12 odst. 4 autorského zákona;
- beru na vědomí, že podle § 60 odst. 2 a 3 autorského zákona mohu užít své dílo – diplomovou/bakalářskou práci nebo poskytnout licenci k jejímu využití jen připouští-li tak licenční smlouva uzavřená mezi mnou a Univerzitou Tomáše Bati ve Zlíně s tím, že vyrovnání případného přiměřeného příspěvku na úhradu nákladů, které byly Univerzitou Tomáše Bati ve Zlíně na vytvoření díla vynaloženy (až do jejich skutečné výše) bude rovněž předmětem této licenční smlouvy;
- beru na vědomí, že pokud bylo k vypracování bakalářské práce využito softwaru poskytnutého Univerzitou Tomáše Bati ve Zlíně nebo jinými subjekty pouze ke studijním a výzkumným účelům (tedy pouze k nekomerčnímu využití), nelze výsledky bakalářské práce využít ke komerčním účelům;
- beru na vědomí, že 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 totožné.

Ve Zlíně, dne 23.5.2018

Kubáček

.....

podpis diplomanta

ABSTRAKT

Abstrakt česky

Cílem práce je poskytnout uživatelům mobilních zařízení přehled současných hrozeb, před kterými se mohou sami aktivně bránit. Teoretická část je v úvodu zaměřena na historii a vývoj operačního systému Android. Následně postupně přechází k otázce bezpečnosti a výčtu jednotlivých hrozeb a rizik, které může uživatel sám ovlivnit svým chováním. V praktické části je provedena analýza bezpečného chování uživatelů za použití dotazníkového šetření. Výsledky dotazníkového šetření jsou doplněny o analýzu aplikací dostupný na Google Play. Analýza je zaměřena na potenciální zneužití aplikace. K tomu budou využity běžně dostupné nástroje, jako jsou například antivirové aplikace pro Android.

Klíčová slova: Android, aplikace, Google Play, bezpečnostní hrozby, prevence

ABSTRACT

Abstrakt ve světovém jazyce

The aim of the work is to provide mobile users with an overview of the current threats that they can defend themselves against. The theoretical part is focused on the introduction to the history and development of the Android operating system. Subsequently gradually becomes a safety issue and a list of individual threats and risks, which the user can influence their behavior. In the practical part is an analysis of safe user behavior using questionnaires. The results of the questionnaire survey are complemented by app analysis available on Google Play. The analysis focuses on potential abuse of the application. This will be used commonly available tools, such as antivirus app for Android.

Keywords: Android, apps, Google Play, security threats, prevention

Chtěl bych poděkovat panu Ing. Lukáši Králíkovi, za odbornou pomoc při vedení práce a také cenné rady, díky kterým se mi podařilo tuto práci dokončit. Dále bych chtěl poděkovat tvůrcům serveru vyplňto.cz, za možnost bezplatného využití jejich serveru k dotazníkovému šetření v práci.

OBSAH

ÚVOD

Tato bakalářská práce je zaměřena na operační systém Android, dále jen OS, obchod Google Play a bezpečnostní hrozby, v největší míře malware. Cílem této práce je poukázat na současné hrozby a rizika ukázat jim jak se před těmito riziky bránit.

Teoretická část je v úvodu zaměřena na historii a vývoj operačního systému Android. Popisuje počátek operačního systému Android a odkoupení Firmou Google, která započala jeho další vývoj. Dále se zabývá otázkou jednotlivých verzí, postupně od té nejstarší až po tu současnou. Poté čtenářům ukáže architekturu OS Android, její části a také základní části aplikace a aplikační Sandbox. Jako poslední je ze serveru Android developers ukázán podíl mezi uživateli v jednotlivých verzích Android.

Druhá kapitola se zaměřuje na Obchod Play, na historii obchodu, na vzhled prostředí, jeho funkce, popis instalace aplikace, podmínky pro používání obchodu např. pro platby. Poslední podkapitola se zabývá nebezpečnými oprávněními.

Následně v třetí kapitole jsou postupně představeny jednotlivé hrozby, především jednotlivé základní a populární typy malwaru, phishing, spam a útoky prostřednictvím wifi.

V praktické části je provedena analýza bezpečného chování uživatelů za použití dotazníkového šetření. Dotazník má celkem 22 otázek a vyplnilo ho 175 respondentů, otázky se týkají hlavně chování uživatelů na OS Android, různých bezpečnostních prvků v systému, názorů na jednotlivé pojmy. Jsou zde vyhodnoceny navržené hypotézy a zodpovězené hlavní a dílčí cíle.

V další kapitole je praktická část doplněna o analýzu aplikací dostupných na Google Play, s potencionálním zneužitím uživatele. Jsou vybrány jednotlivé typy aplikací, které jsou následně testovány a monitorovány běžně dostupnými nástroji, které může použít běžný uživatel. Jedná se např. o antivirové aplikace, monitoring toku dat, sledování spotřeby baterie a vyhledávání hrozeb aplikací na webových databázích s hrozbami.

Závěrem se tato práce věnuje různým technikám, jak se účinně bránit proti bezpečnostním hrozbám. Vychází se především ze zkušeností samotných uživatelů s tímto OS. Jedná se o všední věci, které zvládnou běžní uživatelé.

I. TEORETICKÁ ČÁST

1 OPERAČNÍ SYSTÉM ANDROID

Android je open-source mobilní operační systém (dále jen OS), ale tento název slouží i pro open-source vývojářskou platformu. Ta slouží k vytváření mobilních aplikací pro OS Android. Dnes se tento systém rozvinul natolik, že kromě mobilních telefonů se používá také v tabletech, televizích, chytrých hodinkách apod.

1.1 Historie společnosti Android

Android původně nezaložila společnost Google. V roce 2003 založili tuto společnost Andy Rubin, Rich Miner, Nick Sears a Chris White a její původní jméno nese název Android Inc. V srpnu roku 2005 přišel Google Inc. s nabídkou pro odkoupení a ze společnosti nakonec udělal svojí dceřinou firmu. [1]

I po tom, co Google společnost koupil, byl do vedení dosazen jeden ze zakladatelů Andy Rubin. Tento člověk také zahájil vývoj systému. V roce 2007 si začal Google patentovat první věci týkajících se mobilních zařízení. Tímto Google vyvolal ve světě první spekulace o jeho vstupu na trh chytrých mobilních telefonů. [1]

Pro společnost Android byl velice významný den 5. listopadu roku 2007. Nastal totiž jeden z největších kroků v historii společnosti. Byla vytvořena tzv. „Open Handset Alliance“. Šlo o hromadné seskupení firem, které vyrábějí mobilní telefony. Za cíl si tato aliance kladla vyvinout standard pro mobilní zařízení. Dnešními členy jsou například: Google, Intel, Samsung, HTC, LG, NVIDIA, Qualcomm, Sony, Dell, Telefónica, T-Mobile, eBay a asi dalších 70 společností z celého světa. [1]

Ihned poté Google vydal prohlášení o první verzi mobilního operačního systému Android. Všem společnostem bylo ihned jasné, že s Androidem má společnost Google na trhu s smartphony velké ambice. První telefon s Androidem byl představen rok po prvním představení OS Android. Výrobcem tohoto telefonu byla společnost HTC a jmenoval se Dream. V některých zemích ho uživatelé mohli spatřit také s jiným názvem - T-Mobile G1. V České Republice se poprvé objevil počátkem roku 2009. [1]

1.2 Historie jednotlivých verzí OS Android

Pod tímto textem je přehled jednotlivých verzí Android s roky vydání každé prvotní jednotlivé verze (Tab. 1.). Dále je u každé verze číselné označení jednotlivého typu OS.

Tab. 1. Přehled verzí OS Android a jejich rok vydání prvotní verze [4]

Verze	Jméno verze	Rok vydání	Verze	Jméno verze	Rok vydání
1.0	Apple pie	2008	4.0 - 4.0.4	Ice cream sandwich	2011
1.1	Banana bread	2009	4.1 - 4.3	Jelly Bean	2012
1.5	Cup cake	2009	4.4 - 4.4.4	Kitkat	2013
1.6	Donut	2009	5.0 - 5.1.1	Lollipop	2014
2.0 - 2.1	Eclair	2009	6.0 - 6.0.1	Marshmallow	2015
2.2	Froyo	2010	7.0 - 7.1.2	Nougat	2016
2.3. - 2.3.7	Gingerbread	2010	8.0 - 8.1	Oreo	2017

První verze operačního systému Android byla představena společně s telefonem T-mobile G1. Tato verze umožňovala používat webový prohlížeč, multimediální přehrávač, nebo hlasové vytáčení hovoru. V první verzi se vývojáři věnovali podpoře základních aplikací od Google jako např. poštovní služba Gmail, obchod s aplikacemi Android market, komunikační aplikace Google Talks, Mapy Google, nebo přehrávání videí z portálu Youtube. Verze běžela na linuxovém jádře 2.6.25. Zásadní je podpora základních tzv. widgetů na domovské obrazovce. Půl roku poté byla představena verze 1.1, která nic zásadního nepřinesla. Opravovala však první nalezené chyby. Tato verze poskytovala zobrazení a skrytí číselníku a zkracovala interval vypnutí obrazovky při příchozím hovoru. [2] [4]

Nejzásadnější funkce v další verzi s názvem 1.5 Cupcake jsou natáčení a následné přehrávání videa. V Cupcake se objevila první softwarová klávesnice. Uživatelé již mohou přiřazovat obrázky či fotografie ke svým kontaktům, nebo jsou schopni také nahrávat pořízené snímky a videa na Youtube a Picasa. Widgety je možné upravovat. [2] [3]

Vylepšení následující verze 1.6 Donut spočívá hlavně v kompatibilitě s jinými typy telefonů a s rozlišením obrazovek. Přinesl nový vyhledávací panel, který uměl vyhledávat v kontaktech, záložkách, nebo historii webového prohlížeče. Dále byl využit rychlejší klient pro aplikaci Android market a struktura tohoto obchodu se stala přehlednější. [2] [5]

Ve verzi Eclair se poprvé objevila synchronizace aplikace Facebook společně s kontakty ze zařízení. OS již podporuje více účtů v zařízení najednou. Dále byl přidán převod textu na mluvenou řeč. [2] [4]

Verze Froyo se zlepšila v celkovém zrychlení a zjednodušil se systém díky optimalizaci procesů a uživatelského rozhraní. Uživatelé mají možnost vytvořit z telefonu wifi hotspot, který umožňuje sdílení internetu pro další zařízení v okolí. Dále je možné instalovat aplikace na paměťovou kartu. [2] [6]

Ve verzi Gingerbread byla upravena softwarová klávesnice, vylepšen správce stahování a přidána podpora fotoaparátů na čelní straně zařízení. Byla přidána podpora displejů s vysokým rozlišením (WXGA a vyšší), a také podpora technologie NFC, která umožňuje přenos mezi zařízeními na krátkou vzdálenost. [2] [7]

Verze Ice Cream Sandwich navázala na Android Honeycomb, který v této práci není uveden, protože byl vytvořen jen pro tablety. Měl dobrý základ funkcí a vylepšení, které bylo ale potřeba aplikovat i na klasické smartphony. Většina zařízení proto z verze Gingerbread přecházela rovnou na Ice Cream Sandwich. Celkově se zlepšila aplikace fotoaparátu a zkrátila se také jeho prodleva. Dále se objevila možnost natáčet časosběrná videa, režim panoramatického snímku a možnost přibližování během natáčení. Verze 4.0 do sebe integrovala jednoduchý editor na úpravu fotografií. Nahrávání videí je již možné i v rozlišení 1080p. Konečně se uživatelé také dočkali převodu z mluvené řeči na text a kontroly využívání dat aplikacemi. Vylepšení zasáhlo také internetový prohlížeč, kalendář a e-mailového klienta. Nově byla představena funkce Android Beam, která umožňuje velice rychlou výměnu dat na krátkou vzdálenost přes NFC. Provádí se přímým dotykem zadních částí dvou zařízení. [2] [8]

Ve verzi Androidu Jelly Beam se Google soustředil hlavně na design a vylepšení vyplývající z uživatelských zkušeností. Google v této verzi použil tzv. „Projekt Butter“. Tak se nazývá skupina různých aktualizací, s cílem snížit prodlevy systému a zrychlit jeho celkovou odezvu. V těchto verzích zlepšení spočívalo především v optimalizaci práce s obnovovací frekvencí displeje, časování v-sync nebo použití vyrovnávací paměti u grafického čipu. Systém již nepůsobil tak trhaně, nebo zpomaleně jako v přechozích verzích, zlepšila se celková plynulost a rychlost. [2] [9]

V Android Kitkat proběhla změna v plynulosti a rychlosti prostředí především u slabších zařízeních s menší RAM. KitKat by tak měl fungovat i na zařízeních s 340 MB RAM. Dále přináší podporu pro ART runtime, který je náhradou za původní systém Dalvik. Díky ART se celkově zlepšila plynulost aplikací, aplikace se rychleji spouští a zlepšil se výkon baterie. Díky KitKatu uživatelé mohou používat bezkontaktní platby, bezdrátový tisk, nebo

si nahrávat dění na obrazovce telefonu a další. I vzhled se změnil, celkově prostředí působí velice propracovaně. [2] [10]

Největší změnou ve verzi Lollipop bylo zjednodušení vzhledu uživatelského rozhraní označené jako Material design. Dále se aktualizace zaměřila na větší plynulost systému. Verze nabízela vytvoření více profilů více uživatelům, mezi kterými je možno kdykoliv přepínat. Dále mohou uživatelé nastavovat omezení pro oznámení, nebo příchozí hovory v daném čase - například při spánku. Celková práce s notifikacemi byla vylepšena. V odemykací obrazovce uživatelé mohou vidět pro lepší identifikaci rozšířená oznámení. V sekci nastavení baterie je k dispozici funkce spořič baterie, jejímž cílem je prodloužení výdrže baterie v přístroji až o 90 minut. Omezuje proto běžné funkce telefonu, až na ty základní jako telefonování. Uživatel může sám nastavovat tato omezení. [4] [11]

Mezi základní novinky ve verzi Marshmallow patří podpora čteček otisků prstů, nebo zlepšená verze kopírování a vložení, kdy místo v horní liště se zobrazí tyto funkce přímo nad kopírovaným textem. V této verzi se poprvé setkáváme s dodatečným schvalováním přístupu funkcí aplikací. Ve starších verzích systému všechny aplikace požadovaly před instalací oprávnění přístupu k jednotlivým funkcím telefonu. V praxi to v minulosti fungovalo tak, že mnoho aplikací zbytečně žádalo přístup k citlivým datům, aniž by to ke svému chodu nějak výrazně potřebovaly. Mnohdy šlo o účelové sbírání osobních dat uživatelů. Teď je konečně vše jinak a nová verze umožňuje nakládat s oprávněním aplikací dle svého uvážení. Pokud aplikace zrovna požaduje příslušné povolení, tak se vás přímo při využívání sama zeptá, jestli jí danou funkci povolíte. Nová aplikace Doze se stará o chod aplikací a šetří energii vypínáním při jejich nepoužívání. Jedinou nevýhodou je delší opětovné spuštění aplikace. Za to ale zařízení vydrží delší dobu v pohotovostním režimu. Nově Android podporuje USB Type-C. [4] [12]

Další verzí je Nougat. Dostal zcela nový grafický subsystém. Jmenuje se Vulkan a je náhradou za původní OpenGL. Díky tomuto systému můžeme pozorovat vylepšené efekty v různých aplikacích nebo hrách. Samotné aplikace budou více spolupracovat s GPU, než s ovladači. Jejich role je nyní omezená. Díky tomu se celkově sníží zatížení CPU/RAM. Užitečnou novinkou je nastavení tzv. zobrazované velikosti. U ovládacích prvků a textu si uživatel může libovolně změnit velikost v pěti krocích. Dále se Google zaměřil na používání tzv. split screen, neboli používání více oken najednou. V této aktualizaci Google zapracoval na rozšíření úsporného režimu Doze. Tento režim bude nově fungovat, pokud máte telefon v kapse. Když bude mít zařízení delší dobu zhasnutý displej,

samo přejde do hlubšího spánku. Nakonec také byla uvedena funkce úspory dat**.** Funguje na principu zákazu využívání mobilního připojení aplikacím na pozadí. [4] [13]

Android Oreo je zatím poslední vydaná verze OS Android. Google v této verzi slibuje především rychlejší zavádění systému. Jako v každé z posledních verzí se vývojáři snažili o snížení spotřeby energie. V tomto případě vsadili na umělé ukončování aplikací na pozadí Wise limits, které ukončuje dlouho nepoužívané aplikace. Díky tzv. oznamovacím kanálům může uživatel sám přizpůsobovat upozornění od jednotlivých aplikací. Jednoduše tak každý odstraní vše nepotřebné a ponechá jen to nejdůležitější. V této verzi se nachází tzv. predikce označeného textu. Pokud uživatel např. označí křestní jméno, systém automaticky označí i příjmení. Obraz v obraze je další novinkou. Jakmile uživatel bude přehrávat video na youtube a bude potřebovat se podívat např. na email, stiskne tlačítko domů a video se automaticky přesune do malého okna, které je možno libovolně přesouvat, nebo ukončovat. [4] [14]

1.3 Architektura OS Android

Android je OS, který využívá jádro Linux. V jeho architektuře můžeme nalézt 5 vrstev. Tyto vrstvy si kladou za cíl co nejvíce optimalizovat vývoj aplikací. Pro vývoj aplikací se využívá nástroj Android SDK, který používá další nástroje a API, aby dosáhl požadované funkčnosti a maximální bezpečnosti. Architekturu rozdělujeme dle hlavních komponentů takto: [1]

Linux Kernel neboli linuxové jádro je nejnižší vrstvou architektury a tvoří úplný základ operačního systému. Stará se především o komunikaci mezi hardwarem a softwarem, která je zajištěna pomocí driverů - ovladačů. Dále poskytuje služby jako zabezpečení, správu paměti a správu procesů Android. [1]

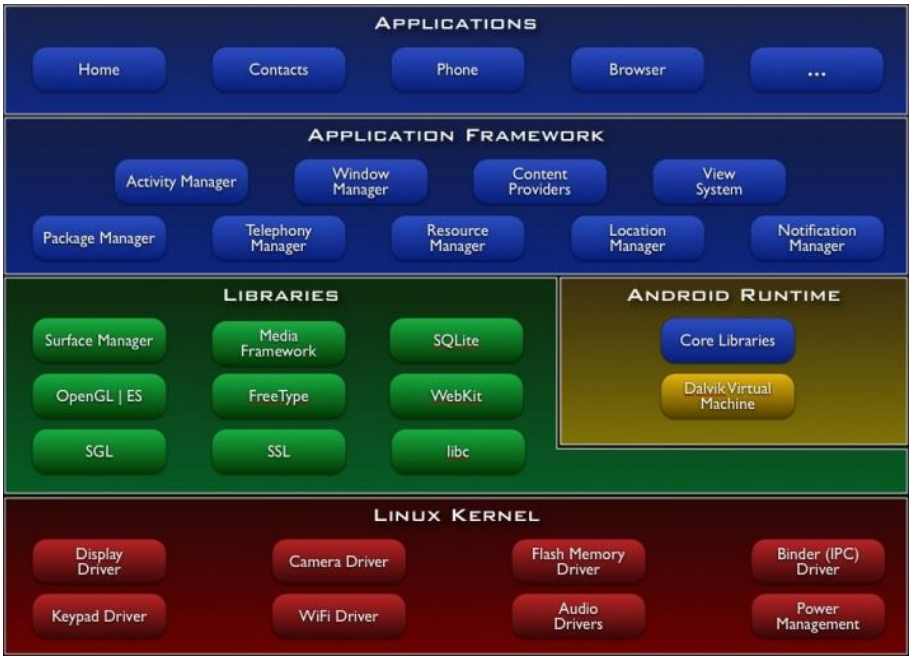
Libraries znamenají v překladu knihovny. Knihovny jsou psány v programovacím jazyce C/C++ a jejich úkolem je zajišťovat chod základních funkcí systému. Knihovny OpenGL/ES a SGL slouží k vykreslování grafiky, SSL umožňuje šifrování, Media Framework zase práci s mediálními soubory. [1]

Android Runtime je vrstva, která zabezpečuje fungování správného běhu aplikací a obsahuje knihovny programovacího jazyka Java. Java není nativním jazykem OS Android, je proto nezbytné použít virtuální stroj, který aplikaci překládá. To právě

zajišťuje tato vrstva. V dřívějších verzích systému Android používal virtuální stroj Dalvik Virtual Machine, avšak od verze 4.4 Kitkat byl u Androidu použit nový stroj ART (Android Runtime). [1]

Application Framework neboli aplikační rámce jsou považovány za nejdůležitější vrstvu pro programátory a programování aplikací. Obsahuje další užitečné knihovny, které již jsou napsané v Javě. Vývojáři Androidu se díky poskytování otevřené developerské platformy snaží o zvýšení bohatosti systému jako celku. Android povoluje plný přístup k API rámcům, které využívají funkce běžící v jádře. Díky tomu aplikace může zažádat o použití všech dostupných položek (např. upozornění, lišta), které poskytuje systém Android. API lze označit jako sadu nástrojů a protokolů, díky kterým se vytváří aplikace, usnadňují práci programátorovi. API poskytované na této vrstvě jsou celkem 4. Úkol obsahového manažera spočívá ve sdílení dat mezi různými aplikacemi. Manažer oznámení poskytuje zobrazování alarmů v liště notifikací. Zdrojový manažer umožňuje přístup k nekódovaným zdrojům. Manažer aktivit se stará o životnost aplikací. [1]

Application je nejvyšší vrstva. Obsahuje jednotlivé aplikace. Mezi nejzákladnější aplikace patří emailový klient, kalendář, prohlížeč a kontakty. Tyto aplikace jsou předinstalované. Uživatel má také možnost stahovat další typy aplikací, které jsou dostupné v obchodě Google Play. Na obrázku 1 pod textem lze vidět prostředí architektury OS Android.[1]



Obr. 1. Prostředí architektury OS Android [1]

1.4 Aplikace v OS android

Mobilní aplikace je softwarový nástroj vytvořený pro mobilní chytré telefony. Ze začátku vzniku tzv. smartphonů sloužili první aplikace hlavně k prezentování základních funkcí - prohlížení emailu, počasí a dalších. Postupem času se do chytrých telefonů dostali aplikace mnoha druhů a v dnešní době se hodně vývojářů předhání o to, jaký nový typ aplikace někdo představí jako první. V další podkapitole se nachází základní přehled komponent aplikace.

1.4.1 Základní části aplikace

Základ aplikací Android rozdělujeme do 4 částí. Jsou to komponenty activity, které reprezentují obrazovku, service poskytuje provádění akce na pozadí, content providers umožňuje přístup uživateli k datům a broadcast reciever reaguje na příchozí oznámení. Tyto komponenty můžeme najít a definovat v souboru AndroidManifest.xml, který je uložen v kořenovém adresáři. Ještě navíc mohou komponenty mezi sebou spolupracovat pomocí zpráv, tzv. intentů. [15]

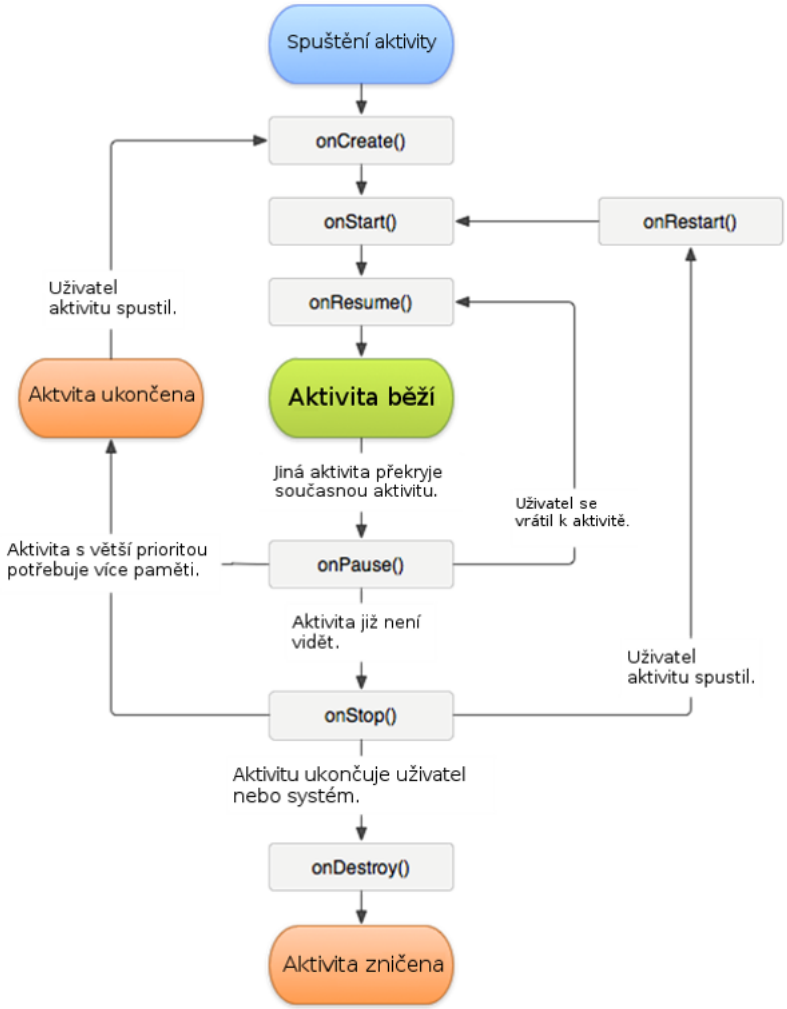
Aktivita je jedna obrazovka, která v sobě skrývá grafické uživatelské rozhraní, díky kterému může provádět interakci s uživatelem. Jedna aplikace má v sobě často více aktivit. Uživatel má možnost mezi nimi přepínat a přitom si aktivity mezi sebou mohou předávat informace. Zahájení aktivity probíhá v několika krocích. Nejdříve je potřeba utvořit nový proces, dále musí proběhnout alokace paměti, která náleží objektům uživatelských rozhraní, které se rozloží do layoutu obrazovky a na připravenou obrazovku vyvolají zobrazení. Pro ochranu proti plýtvání výpočetních prostředků např. při vzniku, zániku a opětovného vzniku aktivity se využívá Activity Manager, který má odpovědnost za vytváření, zrušení a celkovou správu životního cyklu aktivity. Activity Manager obsahuje zásobník. V tomto zásobníku se uchovávají informace o spuštěných aktivitách. [15]

Životní cyklus aktivity se dělí do následujících stavů:

- Activity starts - Začátek inicializace aktivity.
- Activity is running - Probíhá zobrazování aktivity na displeji. Zde může docházet k interakci s uživatelem. Jediná aktivita v jednom okamžiku se může nacházet v tomto stavu.

- Process is killed - Activity Manager zrušil aktivitu z důvodu nedostatku paměti. K této akci může dojít, pokud aktivita není viditelná. Další možnost není tak obvyklá - aktivita je viditelné, ale uživatel s ní nemůže navázat interakci.
- Activity is shut down - Activity Manager skončil aktivitu - není již nevyužívána žádná paměť. [15] [16]

Životní cyklus běžné aktivity je zachycen na pod tímto textem (Obr. 2.).



Obr. 2. Životní cyklus aktivity [16]

1.5 Aplikační sandbox

Díky linuxovému jádru má OS Android výhody v identifikaci a izolaci nástrojů aplikací. Aplikace je spouštěna jako samostatný proces s jedinečným ID, které je přiřazováno OS Android. Na tomto principu funguje pouze tento OS. Aplikační sandbox pracuje na úrovni

jádra. Jádro se stará o bezpečnost aplikací spolu se systémem na procesní úrovni, jednotlivým aplikacím jsou přidělena různá ID, díky kterým získají aplikace svolení přístupu k různým operacím. Většinou aplikace mají zákaz spolu spolupracovat, pokud nedostanou povolení a do operačního systému mohou zasahovat jen omezeně. Mimo jádro se aplikační sandbox objevuje i v nativním kódu a v aplikacích. Veškerý software pracující nad Linuxovým jádrem začíná pracovat pomocí Aplikačního sandboxu. Jestliže se v jiných OS setkáme s porušením integrity paměti, v zásadě je ohrožena bezpečnost. V OS Android to tak není, protože veškeré aplikace se na úrovni operačního systému sledují prostřednictvím aplikačního sandboxu. Jako i další bezpečnostní prvky tohoto OS lze sandbox obelstít. Pokud se tak opravdu stane, muselo proběhnout narušení bezpečnosti Linuxového jádra. [17]

1.6 Oprávnění aplikací

Oprávnění systému dle serveru Android developer rozdělujeme do několika úrovní ochrany. Nejdůležitější jsou však dvě základní. Říká se jim normální a nebezpečné oprávnění. [18]

Normální oprávnění se týkají pole působností, kde potřebují aplikace přístup k datům nebo zdroje mimo bezpečnostní mechanismus aplikace. Zjednodušeně řečeno přesně tam, kde je minimální riziko pro porušení soukromí uživatele nebo pro přerušení provozu dalších aplikací. Mezi normální povolení se řadí například nastavení časového pásma. Pokud aplikace vyžaduje normální oprávnění, systém jí tato oprávnění přidělí sám. [18]

Nebezpečné oprávnění uživatelé spatří tam, kde aplikace požaduje data nebo prostředky, které se týkají výhradně zásahu do soukromých záležitostí uživatele, provozu jiných aplikací, nebo například ovlivňují uložená data uživatele. Mezi tato oprávnění patří například čtení zpráv. Pokud aplikace potřebuje nebezpečné povolení, ve verzi OS Android 5.1 a nižší musí uživatel sám ručně udělit oprávnění aplikaci při její instalaci. Platí zde, že systém sdělí uživateli příslušnou skupinu povolení aplikace, kterou vyžaduje, nikoliv jednotlivé oprávnění. Když například aplikace dostane povolení číst v kontaktech, tak to znamená, že kontakty může i zadávat. [18]

U verze OS Android 6.0 a vyšší fungují nebezpečná oprávnění jen na základě souhlasu uživatele. V praxi to znamená, když aplikace zrovna požaduje přístup k fotoaparátu, tak se vás na to jednoduše zeptá před použitím. Každý má možnost dané oprávnění zakázat

buď v nastavení telefonu ve složce aplikace, nebo před použitím daného oprávnění. Každé nebezpečné oprávnění opět patří do určité skupiny, na kterou se vás systém předem ptá. Jakékoliv povolení může patřit do skupiny oprávnění, i včetně běžných povolení a oprávnění definovaných vaší aplikací. Dá se říci, že skupina povolení má vliv pouze na uživatelský komfort pouze tehdy, když povolení patří do skupiny nebezpečných. Pokud se jedná pouze o skupinu s normálním oprávněním, není třeba jí věnovat takovou pozornost. Pod textem se nachází tabulka s nebezpečnými oprávněními dle serveru Android developers. [18]

Tab. 2. Přehled nebezpečných oprávnění ze serveru Android Developers [18]

Skupiny oprávnění	Oprávnění
Kalendář	• READ_CALENDAR • WRITE_CALENDAR
Kamera	• CAMERA
Kontakty	• READ_CONTACTS • WRITE_CONTACTS • GET_ACCOUNTS
Geolokace	• ACCESS_FINE_LOCATION • ACCESS_COARSE_LOCATION
Mikrofon	• RECORD_AUDIO
Telefon a Volání	• READ_PHONE_STATE • CALL_PHONE • READ_CALL_LOG • WRITE_CALL_LOG • ADD_VOICEMAIL • USE_SIP • PROCESS_OUTGOING_CALLS
Senzory	• BODY_SENSORS
SMS	• SEND_SMS • RECEIVE_SMS • READ_SMS • RECEIVE_WAP_PUSH • RECEIVE_MMS
Úložiště	• READ_EXTERNAL_STORAGE • WRITE_EXTERNAL_STORAGE

1.7 Podíl verzí Androidu mezi uživateli

Na stránce Android developers můžeme vidět, kolik uživatelů používá různé verze systému Android. Výzkum Android provádí za pomocí aplikace Google Play. Aplikace analyzuje návštěvnost uživatelů na zařízeních s různými verzemi OS Android a data zapisuje. V tabulce 3 pod tímto textem jsou data z období od 1. do 7. května 2018. V tabulce nejsou obsaženy verze s podílem menším než 0,1%. Nejpoužívanější verzí systému je Android 6.0 Marchmallow s podílem 25,5%, následovaný verzí 7.0 Nougat s podílem 22,9%. [19]

Tab. 3. Přehled využití verzí OS Android uživateli v procentech [19]

Verze	Název	Distribuce
2.3.3 - 2.3.7	Gingerbread	0.3%
4.0.3 - 4.0.4	Ice Cream Sandwich	0.4%
4.1.x	Jelly Bean	1.5%
4.2.x		2.2%
4.3		0.6%
4.4	KitKat	10.3%
5.0	Lollipop	4.8%
5.1		17.6%
6.0	Marshmallow	25.5%
7.0	Nougat	22.9%
7.1		8.2%
8.0	Oreo	4.9%
8.1		0.8%

2 OBCHOD GOOGLE PLAY

Google play je oficiální internetový obchod společnosti Google, který shromažďuje aplikace pro Android a je základním kamenem pro jejich stahování. Díky tomu uživatelé mohou přistupovat k milionům nejnovějších aplikací pro Android, ale také her, hudby, filmů, televizních pořadů, knih, časopisů a dalšího obsahu.

2.1 Historie Obchodu

Vznik Google Play obchodu s původním názvem Android Market se datuje do října roku 2008. Obchod s aplikacemi byl uveden spolu s prvním telefonem s OS Android. [48]

Vedle obchodu s aplikacemi ve stejné době vzniká také služba Google Music. Dle zjištění bylo shledáno, že tyto dvě služby ztrácí na přehlednosti a jejich prostředí pro uživatele není příliš intuitivní. Kvůli tomu Google, tak trochu po vzoru iStore od Applu, dne 6. března 2012 zveřejnil jednotný obchod s názvem Google Play. [48]

2.2 Platby v obchodě

V obchodě se nacházejí aplikace zdarma, nebo aplikace vyžadující platbu k jejich zakoupení.

2.2.1 Aplikace zdarma

Google umožnuje stahovat bezplatně volně dostupný obsah obchodu. Všechny podmínky, které se vztahují k placeným aplikacím, jsou stejné i u volného obsahu, kromě všech skutečností souvisejících s platbou. [20]

2.2.2 Zpoplatněné aplikace

Pro zakoupení obsahu v obchodě musí uživatel souhlasit s platebními podmínkami služby Google. Smlouva o koupi a používání obsahu bude dokončena, pokud uživatel obdrží e-mail potvrzující nákup obsahu. Poté začíná plnění této smlouvy. Platby v obchodě lze realizovat pomocí služby Google Payments. Některé nákupy však vyžadují přímou interakci s poskytovatelem produktu. V tomto případě se může stát, že vaše osobní údaje Google bude sdílet přímo s poskytovatelem. Uživatelé mají kromě této techniky k dispozici různé způsoby zpracování plateb pro snadnější nákup v obchodě. Samozřejmě musí být dodrženy všechny podmínky nebo právní dohody, ať už u Google nebo třetí strany, která řídí používání dané metody zpracování plateb. Google může přidat,

nebo odebrat metody zpracování plateb na základě vlastního uvážení a bez upozornění. [20]

Pokud máte zřízenou svou rodinnou skupinu pro jednotnou platbu za účelem zakupování aplikací, tak šéf této skupiny neboli rodinný manažer musí nastavit platné metody pro rodinnou platbu. Poté je všichni členové rodinné skupiny můžou použít k nákupu obsahu a i v rámci aplikací. Od této chvíle je rodinný manažer zodpovědný za všechny platby svých rodinných příslušníků. [20]

2.3 Podmínky pro využívání obchodu

Pokud se chystáte z obchodu cokoliv stahovat, jako první si musíte založit nebo se přihlásit pomocí Google účtu. Obchod s aplikacemi totiž funguje jen s přihlášením, jakožto i ostatní služby Googlu. Chcete-li Google Play používat, budete potřebovat zařízení, které splňuje požadavky na systém a kompatibilitu pro příslušný obsah, což se může čas od času změnit. Dále je potřeba přístup k internetu a kompatibilní software. Další pravidlo, které si uživatel musí zapamatovat je, že každá aplikace v obchodě nefunguje na každém typu zařízení. Různé typy aplikací fungují např. jen od určité verze OS Android a vyšší. Pokud aplikace nepodporuje vaše zařízení, nezobrazí se vám ve výčtu aplikací, které můžete stáhnout. Dále jsou uživatelé zodpovědní za odvádění poplatků za internet třetím stranám, např. poskytovateli internetu, nebo mobilnímu operátorovi. Vaše schopnost používat tuto službu může být ovlivněna jedním z těchto faktorů. [20]

Google vydává aktualizace, které se mohou týkat např. opravy bezpečnostních chyb, vylepšení některých funkcí, chybějících zásuvných modulů nebo vzhledu obchodu. Také po uživatelích vyžaduje, aby souhlasili s automatickými aktualizacemi systému. Dále je možnost pravidelně automaticky stahovat aktualizace aplikací. Uživatel může také nastavit, kdy se tyto aplikace můžou stahovat – např. jen při používání wifi sítě nebo i mobilních dat od operátora. Google může automaticky bez souhlasu instalovat aktualizace aplikacím, které obsahují kritické chyby zabezpečení a ohrozily by tím bezpečnost vašeho mobilního zařízení. [20]

Pokud jste členové rodiny a rádi využíváte Obchod Play, Google nabízí využívání tzv. rodinné skupiny. V rámci této skupiny budou moci vaši rodinní příslušníci vidět určité informace o vás. V čele rodinné skupiny stojí rodinný manažer, který může zvát další členy do skupiny. Všichni členové skupiny mezi sebou vidí uživatelské informace jako např.

jméno, email či fotografii. Rodinný manažer si také může zobrazit detailnější informace jako věk a uvidí záznamy o všech nákupech rodinných členů, včetně popisu zakoupeného obsahu. S tímto souvisí rodinné platby a rodinné předplatné, které jdou v rámci skupiny nastavit. Některý obsah obchodu může podporovat rodinné sdílení. Pokud ano, pak všichni členové rodiny budou mít přístup k obsahu a také uvidí, kdo daný obsah zakoupil. Google tímto chce zamezit hlavně používání jednoho účtu více lidmi. Uživatele také nabádá, aby udržovali své osobní údaje v bezpečí a nesdíleli je s jinými uživateli. Má to hned několik důvodů. Např. pokud máte k účtu připojenou platební kartu, může být kýmkoliv zneužita. Může dojít i ke zneužití osobních údajů uživatele, nebo rodinné skupiny. Pokud uživatel poruší obchodní podmínky, může mu být zakázán přístup přes Google účet k obchodu a jakýmkoliv aplikacím, které do obchodu patří. Zákaz přístupu rodinným manažerům nebo členům skupiny může ovlivnit také další členy skupiny, kteří tak mohou ztratit přístup k rodinným funkcím, jako je například metoda rodinné platby, rodinné předplatné nebo sdílení obsahu. [20]

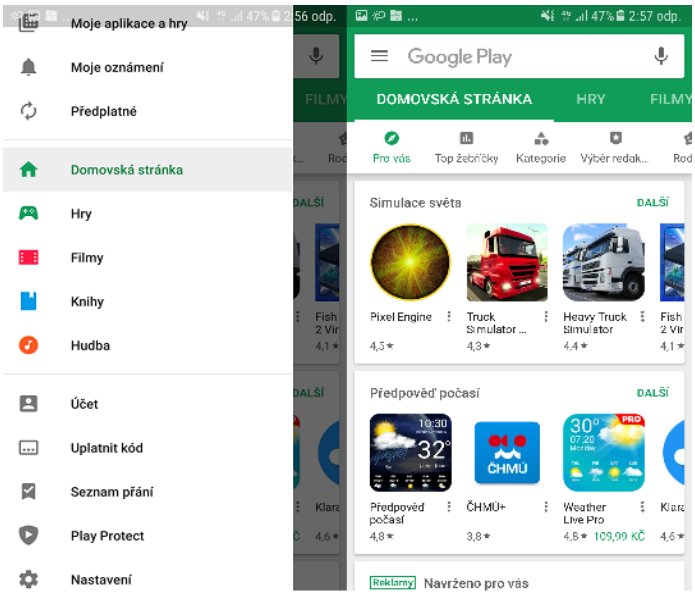
V obchodě je využívána malware ochrana, která chrání před škodlivým softwarem třetích stran a před dalšími problémy se zabezpečením. Google tak může získávat informace o síťovém připojení zařízení, operačním systému a aplikacích třetích stran. Může vás varovat, pokud se domnívá, že aplikace může být nebezpečná. Dokonce může pomocí správce zařízení a Google Play odstranit nebo zablokovat instalaci aplikace v zařízení, pokud se ukáže, že je aplikace škodlivá. Tato ochrana lze vypnout v nastavení telefonu. Rozhodně to ale není doporučováno. [20]

2.4 Popis prostředí

V březnu 2012 se Android Market změnil a přejmenoval na Google Play. Došlo k tomu zejména díky sjednocení všech obchodních aplikací do jednoho celku. Android Market se tedy rozšířil o nabídku hudby, elektronických knih, nebo filmů. Celé prostředí Google Play je v češtině a i ceny aplikací se zobrazují v tuzemské měně. Tato aplikace se pořád vyvíjí a podle počtu přibývajících aplikací dochází čas od času ke změnám vzhledu a struktury aplikace. V této podkapitole budu popisovat nejnovější verzi 9.8.30, kterou používám na svém telefonu Samsung Galaxy A5 2017 společně s OS Android 7.0.

Při spuštění aplikace Obchod Play se nám zobrazí úvodní obrazovka. Nahoře se nachází vyhledávací řádek, díky kterému uživatelé mohou najít aplikace podle jména. Po pravé straně v tomto řádku se nachází mikrofon, který se používá k hlasovému zadávání. Vlevo

se po stisknutí na tlačítko tří čar pod sebou vysune z levého okraje displeje nabídka, kde je vidět nyní přihlášený účet Google, tlačítko nabídky Moje aplikace a hry, moje oznámení a předplatné, dále domovská stránka, tlačítko nabídky her, filmů, hudby a knih. Pod nimi se nachází nabídka účet, kde se nastavují platební metody, poté jsou zde odběry hudby či aplikací, vyzvednutí odměn, nebo historie objednávek. Druhé tlačítko se nazývá Uplatnit kód, kde ho uživatelé mohou uplatnit na obsah různého charakteru např. pro koupi hry. Další nabídka se jmenuje Seznam přání a funguje tak, jako záložky na počítači. Každý si zde může uložit vybraný obsah pro pozdější stažení. Poté zde uživatelé najdou tlačítko Play Protect. Jedná se o vylepšenou ochranu proti škodlivým aplikacím z Google Play. Díky této ochraně můžete pravidelně kontrolovat aktivitu aplikací a zjišťovat jejich stav. Dále v tlačítku nastavení, které je poslední v této nabídce, uživatelé mohou nastavovat např. automatické stahování aktualizací systému a samotných aplikací, vypnutí či zapnutí rodičovské kontroly, požadování ověření při nákupu, nebo vymazání místní historie vyhledávání. V nabídce, která je na obrázku 4 pod textem lze nalézt aktuální verzi Obchodu Play, podrobnosti o open source licenci, nebo certifikace zařízení.



Obr. 3. Ukázka prostředí nabídky obchodu

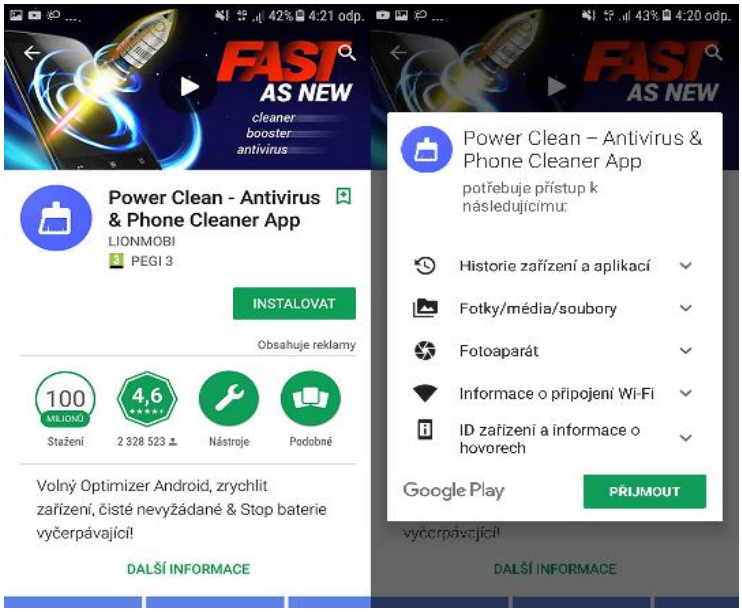
Pod vyhledávacím řádkem se vyskytují 2 nabídky. První rozděluje obsah na domovskou stánku, hry, filmy, hudbu a knihy. Pod ní druhá nabídka je podrobnější. Lze v ní nalézt nabídku pro vás, která intuitivně nabízí aplikace dle vašich stahování, žebříčky nejlepších aplikací, ve které můžeme vyhledat aplikace dle oblíbenosti, zisku, popularity, nebo prodejnosti. Dále zde můžeme nalézt položku Kategorie, ve které funguje vyhledávání aplikací dle různých kategorií jako například cestování a doprava, byznys,

finance, fotografie a další. V této nabídce je také nabídka rodina, výběr nejlepších aplikací redakce, nebo předběžný přístup, do kterého patří aplikace před vydáním. Pod těmito nabídkami se dají nalézt výběry aplikací z různých kategorií. Potáhnutím doleva se zobrazí další aplikace z vybrané kategorie.

2.5 Popis instalace Aplikace

Instalace obsahu z obchodu play probíhá velice jednoduchým způsobem. Na rozdíl od počítače s operačním systémem Windows nemusí uživatel zadávat, do jaké složky se aplikace má uložit. Google se postará prakticky o vše. Obchod potřebuje ke svému fungování jakékoliv připojení k internetu.

Po nalezení příslušné aplikace se zobrazí stránka, kde se nachází v pravém horním rohu tlačítko instalovat. Po kliknutí se zobrazí výčet oprávnění, které aplikace potřebuje ke svému chodu a správnému fungování. Je třeba přemýšlet nad tím, která aplikace opravdu potřebuje daná oprávnění. Mnoho aplikací totiž po uživatelích často zbytečně vyžaduje oprávnění, která jim vlastně nepřísluší. Proto se musí uživatel nad nimi zamyslet a logickým uvažováním popřemýšlet. Pokud aplikace vyžaduje něco víc než ve skutečnosti má, může se jednat o škodlivou aplikaci. Po zanalyzování oprávnění stačí poklepnout na tlačítko přijmout. Tato nabídka a stránka s aplikací jsou vidět na obrázku 5 pod tímto textem. Aplikace se stáhne do zařízení a sama nainstaluje. Po instalaci se na dané stránce s aplikací vedle sebe zobrazí tlačítko otevřít a odinstalovat.



Obr. 4. Ukázka instalace aplikace

V prostředí stránek jednotlivých aplikací v obchodě můžeme nalézt velmi podobnou strukturu nabízených aplikací. Jak je vidět na obrázku nad textem, Obchod Play zobrazuje o aplikaci základní informace, jako například kolik lidí si danou aplikaci stáhlo, nebo ohodnotilo a také do které skupiny aplikací patří. Dále je zde uveden krátký popis, který se po kliknutí zvětší o detailnější popis produktu. Uživatel zde najde také obrázky přímo z aplikace, aby mohl prozkoumat její prostředí ještě před stažením. Následující důležitou skutečností je hodnocení samotných uživatelů, kteří daný produkt používají. Podle jejich zpětné vazby a zkušeností může uživatel sám odhalit škodlivou, nebo nefunkční aplikaci, nebo jen její verzi, ještě před jejím stažením. Pod recenzemi uživatelé najdou různé nabídky jako další aplikace od stejného vývojáře, funkčně podobné aplikace nebo mohlo by se vám líbit. Jako poslední se zde nachází informace o vývojářích, zahrnující odkaz na jejich webové stránky včetně možnosti posílání emailu, zásady ochrany soukromí, nebo podrobnosti o oprávněních, která daná aplikace využívá v nejnovější verzi. Úplně na konci stránky je odkaz na pravidla pro vrácení peněz v obchodě a pod ním tlačítko nahlásit jako nevhodné, kde uživatel může podat sám zpětnou vazbu o aplikaci na oddělení Googlu, které spravuje tento obchod.

2.6 Google Bouncer a Play Protect

Bouncer je testovací program, který je používán v obchodě play společností Google za účelem automatické kontroly všech aplikací. Tento skener každý den testuje aplikace, jestli mají známky jakékoliv anomálie, díky které může označit aplikaci jako škodlivý program. Takové aplikace z obchodu rovnou vylučuje. Tento program také kontroluje nové vývojářské účty a snaží se vyhledávat vývojáře, kteří se již v minulosti provinili tvorbou škodlivých aplikací a takovéto účty mazat. [21]

Pro uživatele zřídil Google v rámci obchodu Play službu s názvem Play Protect. Každý uživatel může tento nástroj používat pro každodenní kontrolu aplikací po aktualizacích, nebo při instalaci nových. Play Protect kontroluje v aplikacích hlavně malware.

3 BEZPEČNOSTNÍ HROZBY

Tato kapitola se zprvu zaměřuje na mobilní malware, jeho základní typy a také populární typy posledních let. Dále se zaměřuje na problematiku spamu, phishingu a útoků při používání wifi.

3.1 Mobilní malware

Za mobilní malware se považuje škodlivý software, který se zaměřuje na mobilní zařízení. V důsledku útoku může tento software způsobit zhroucení systému, nebo ztrátu či únik důvěrných informací. Vzhledem k tomu, že se platforma Android používá u mnoha značek a na více typech zařízení, jako jsou chytré hodinky, nebo televizory, je pro vývojáře stále obtížnější zajistit jejich bezpečnost před elektronickými útoky v podobě virů nebo jiného malwaru. Navíc se hackeři zaměřují na platformu Android díky jejímu obrovskému rozšíření a špatné ochraně hlavně u starších verzí, které stále používá dost lidí. Celosvětově je Android jednoznačně nejpoužívanější OS pro mobilní zařízení, takže není divu, že se stává stále častějším cílem útočníků. Ti to zkouší nejrůznějšími cestami.

Malware se řadí do jednotlivých kategorií. Tyto kategorie se označují jako tzv. rodiny. Rodiny udávají základní charakteristiku malwaru. Když bude vytvořen nový škodlivý software, tak díky jeho rodině poznáme, jak se bude daný program chovat. Při vytváření nového malwaru většinou jen vývojáři upravují některý z existujících kódů. V dalším odstavci se nacházejí nejznámější typy malware útoků.

3.1.1 Základní typy

V této podkapitole je definováno základní rozdělení malwaru, tedy škodlivého kódu, který je rozšířen i v jiných OS. Nejdříve byl rozšířen např. u Windows, ale s příchodem chytrých telefonů se začal velice rozšiřovat i na zařízení s OS Android.

3.1.1.1 Vir

V některých ohledech se chová jako biologický vir. Tento program se dokáže sám volně šířit mezi zařízeními a může poškozovat hardware i software. Do zařízení se dostane nevědomě jako součást nějakého programu či dokumentu. [22]

3.1.1.2 Červ

Tento typ je označován za modifikaci viru. Dokáže se pohybovat po síti prostřednictvím škodlivých dokumentů nebo paketů počítačové sítě. Také se dokáže volně šířit a nakazit tak další zařízení prostřednictvím kopií. Vir a červ se liší od sebe v tom, že červ se umí rozšiřovat sám bez přítomnosti hostitele. [22]

3.1.1.3 Trojský kůň

Trojský kůň je typ nástroje, který se tváří při instalaci jako užitečný, ale poté mnohdy způsobuje škody. Tento typ se sám nedokáže šířit. Po instalaci do zařízení začne provozovat jiné škodlivé aktivity, než pro které byl určen. [22]

3.1.1.4 Rootkit

Rootkit je soustava prostředků, díky kterým lze skrývat přítomnost infikovaných programů, například virů, trojských koní, adwaru a podobně. Aby nedošlo k odhalení, tento nástroj schovává vybrané složky adresáře např. do registrů. Existují i legitimní rootkity, proto uživateli při každém styku s ním nemusí ihned hrozit nebezpečí. [23]

3.1.1.5 Exploit

Označuje se tak speciální nástroj využívající programátorské chyby v systému pro jeho úplnou kontrolu nebo za účelem instalace jiného infikovaného prostředku. Tuto chybu je třeba odstranit pomocí aktualizací. [24]

3.1.2 Populární typy

V této podkapitole se objevují nejpopulárnější vybrané formy malwaru posledních let dle internetového serveru společnosti Kaspersky. V dalších podkapitolách je přehled nejpopulárnějších forem malwaru posledních let. [27]

3.1.2.1 Bankovní malware

Bankovní malware se objevuje v posledních letech čím dál častěji. U hackerů je hodně oblíbený a cílí hlavně na uživatele, kteří upřednostňují veškerou svou činnost včetně převodů peněz a plateb z mobilních zařízení. Tento typ hrozby nashromáždí potřebná data k přihlášení do internetového bankovnictví, které následně odešle zpět na odesílatelův server. Je to jedna z nejrychleji rostoucích hrozeb pro mobilní zařízení za poslední roky. [26]

Jeden z nejznámějších bankovních malwarů současnosti se nazývá Bankbot. Tento trojský kůň zasáhl několik významných světových bank. Jeho nová verze letos několikrát překonala ochranu Google Play Bouncer a v několika aplikacích se dostala do obchodu. Bohužel to pocítily i české banky na vlastní kůži, a to AirBank, ČSOB a Sberbank. Tuto informaci zveřejnil server Avast. Na Google Play se postupně objevily útoky, kdy se daný malware nacházel ve funkčních aplikacích a hrách. Například se nacházel ve svítilně, ve hře Solitaire anebo v aplikaci pro čištění telefonu. [25]

3.1.2.2 Ransomware

Ransomware je velice rozšířený typ malwaru a bránit se proti hackerům, kteří ho používají, je velice složité. Obsahuje škodlivý kód šířící se pomocí e-mailových příloh, nebo jako součást programů a nedůvěryhodných stránek. Jakmile se dostane do zařízení, zablokuje důležitá uživatelská data disku, jako jsou dokumenty, fotografie a videa, a následně tyto informace zašifruje. Poté většinou po poškozeném požaduje peníze pro jeho vývojáře za odblokování. Pokud daný uživatel nezaplatí včas, soubory zůstanou uzamčené nebo budou smazány.

Ransomware se ve světě také velice rozšiřuje, přičemž jeho objem mezi uživateli se během prvních měsíců roku 2017 zvýšil více než trojnásobně. Tato skutečnost je zaznamená v Malware Report společnosti Kaspersky Lab. Jedná se o zprávu za první čtvrtletí roku 2017. Součet zjištěných mobilních případů s nákazou ransomware soubory dosáhly v průběhu čtvrtletí 218 625 v porovnání s 61 832 v předchozím čtvrtletím, přičemž rodina Conguru představovala více než 86 %. Jen za první čtvrtletí bylo zaznamenáno 11 nových kryptografických rodin a 55 679 nových modifikací stávajícího malwaru. [28]

3.1.2.3 Spyware

Odhalení spywaru nebývá vůbec jednoduché. Skrytě hledá jakékoliv informace o vašem chování na internetu, např. záložky, historii prohlížených stránek a jiné. Poté tyto informace sdílí přes internet třetím stranám. Tento typ malware je načten jako program do vašeho zařízení, snaží se monitorovat vaši polohu, zaznamenává vaše aktivity a sbírá důležité informace, jako jsou uživatelská jména a hesla pro e-mailové účty nebo stránky elektronického bankovnictví. Občas je také přibalen s jiným zdánlivě neškodným softwarem a tiše pracuje na pozadí. Většina běžných uživatelů si jeho přítomnosti

ani nevšimne, dokud neudělají test nějakým antimalwarovým softwarem, nebo např. klesne výkon mobilního zařízení. [29]

Někteří vývojáři spywaru tvrdí, že jejich program odesílá veškeré informace jen z důvodu pochopení potřeb nebo zájmů uživatele a využií pro zacílenou reklamu. Tento typ spywaru je legální. Toto je samozřejmě možné, ale pořád jsou tu i spyware odesílající hesla a čísla kreditních karet. Bohužel uživatel těžko pozná, z jaké kategorie spyware pochází. [29]

Jedna z nejznámějších legálních spyware aplikací se jmenuje mSpy. Tato aplikace je forma rodičovské kontroly. Monitoruje a zaznamenává aktivitu uživatele na zařízení. Rodiče mohou sledovat celou řadu aktivit, které jejich děti na mobilu dělají, od sledování polohy zařízení až po historii prohlížeče, videa, obrázky, e-maily, texty a další.

3.1.2.4 Adware

Tento typ malwaru se objevuje přímo v prohlížeči, ve vyskakovacích oknech, v panelech nástrojů. V některých oblastech se podobá spywaru. Tvůrci prostřednictvím adwaru mohou vydělávat v závislosti na počtu kliknutí na daný odkaz. Většina těchto reklam pouze obtěžuje, ale nepředstavuje velké riziko. Některé programy však představují riziko skrze shromažďování osobních informací. Nejčastěji se nachází v aplikacích, které jsou zdarma. Jakmile nainstalujeme danou aplikaci, souhlasíme s licenčním ujednáním, adware se tak v pohodě dostane do zařízení. [30]

Adware může také obtěžovat pomocí vyskakovacích oken, kterým se říká pop-up. Pokud klikneme na obsah okna, vystavujeme se riziku nainstalování dalšího škodlivého softwaru do zařízení. Tato okna se zobrazují při prohlížení stránek, nejčastěji těch nedůvěryhodných. Můžou lákat na soutěže a také často zobrazí, že uživatel vyhrál nějakou cenu např. za 1000. návštěvníka na dané stránce. Mezi spyware a adware může probíhat spolupráce. Spyware má za úkol monitorovat činnost uživatele, obsah pak pošle adwaru, který zacílí reklamu přesně podle potřeb uživatele. [30]

Typickým příkladem zákeřného Adwaru je Hummingbad z rodiny Shedun. Tento malware se objevil poprvé v únoru 2016. Při prohlížení webových stránek vyskočí reklama, kterou nelze zavřít, dokud to neudělá sama. Při zobrazení této reklamy se nainstalují zadní vrátka, které následně umožní používat rootkit za účelem naprosté kontroly nad zařízením. Za tímto malwarem stojí čínská společnost Yingmob. Objevil se hlavně Číně a v Indii, ale v menších rozměrech i po celém světě. [31]

3.1.2.5 SMS trojské koně

SMS trojský kůň se může dostat do telefonu v nějaké aplikaci. Tento typ trojského koně způsobuje uživatelům finanční potíže tím, že posílá SMS zprávy na čísla s prémiovými sazbami a zvyšuje jejich účty za telefon. Dále také může zprávy zachycovat, např. informace o finančních transakcích a kopii těchto zpráv dál šířit po síti. Už při instalaci a následném spuštění aplikace s nebezpečným kódem dochází k infekci. Uživatel se většinou tuto skutečnost dozví až z výpisu účtu za telefon. [27] [32]

3.2 Spam

Jako spam označujeme nevyžádanou elektronickou poštu. Tyto maily jsou rozesílány tzv. spammery na obrovský počet emailových adres. V tomto případě nejde o reklamu mířenou na určitou skupinu lidí, ale o posílání zpráv naprosto komukoliv. Adresa odesílatele bývá falešná. Je to z důvodu krytí spammerů, dalo by se je jinak snadno identifikovat. Tato adresa bývá většinou neexistujícím odesílatelem nebo nahrazena e-mailem příjemce. Posílání nevyžádané pošty je považováno za obtěžování, proto kdyby spamy odesílali ze svých e-mailových adres, bylo by snadné je dohledat a odpojit od internetu. Dříve byl spam rozšířen jen pomocí e-mailu, dnes je rozšířený na celém internetu. Tento nevyžádaný obsah nyní je součástí diskusních skupin, instant messagingu, blogů, návštěvních knih a na fór. Nejnovější typ je SMS spam. Dle serveru bezpecnyinternet.cz je denně odesláno 107 miliard spamu a více jak 99% je psáno v anglickém jazyce. [33]

3.3 Phishing

Phishing je jedna z technik sociálního inženýrství, díky které můžou uživatelé být okradeni o svá osobní data a údaje (přihlašovací údaje, hesla). Pomocí věrohodných emailových zpráv či webových adres se snaží hackeři z lidí vytáhnout důležité údaje - čísla kreditních karet, heslo k bankovnímu účtu. Emailová zpráva může na první pohled vypadat dost podobně té originální např. od banky. Většinou odkazuje na externí web. Tady jsou základní pravidla rozeznání phishingu. Jako první na webové stránce bývá formulář, který nutí uživatele vyplnit své důležité osobní údaje. Je třeba si všímat různých detailů, které se mohou lišit od originální verze webu, za který se podvrh vydává. Dále webová adresa se většinou snaží napodobit tu originální co nejvíce – změnou jednoho písmena či webové domény na jinou. Komunikace se mnohdy provozuje po nezabezpečeném

protokolu (adresa začíná http://). Velkou hrozbou phishingu je bohužel to, že infikované webové stránky bývají těžko rozeznatelné od originálních. Z toho důvodu je nutné vědět, jak phishing poznat a předcházet mu. [34]

3.4 Hrozby při používání WIFI sítí

Útočníci mohou využívat k útokům také wifi sítě. V dnešní době, kdy mnoho lidí na veřejných místech používá nezabezpečené wifi sítě, se to stává čím dál častěji. Lidé si často ani neuvědomují, jaké hrozby jim hrozí. Přes takovou to síť můžou hackeři např. krást osobní data, nebo zařízení odposlouchávat. Jedna z možností jak tuto hrozbu eliminovat je využití nástroje VPN - virtual private network. Mezi zařízením a VPN bránou se vytvoří šifrované spojení. Pokud by hacker prolomil síť wifi, k šifrovaným datům ze zařízení stejně nebude mít přístup. Tento software slouží především jako prevence proti hackerům, kteří se mohou snažit zachytit spojení a zařízeni třeba odposlouchávat. VPN servery mohou být umístěny po celém světě. Server odesílá data prostřednictvím IP adresy daného serveru, takže to navenek vypadá tak, jako by uživatel u něj byl fyzicky. Při výběru vhodného serveru je třeba ověřit, zda je důvěryhodný. Jinak se jednoduše může stát, že místo hackera vás bude odposlouchávat poskytovatel VPN serveru. [35] [36]

V poslední době se také začaly objevovat útoky na prolomení protokolu WPA a i WPA2. Nejznámější je nejspíše Krack, který se objevil v druhé polovině minulého roku. Díky této chybě se mohou útočníci dostat k šifrované komunikaci na bezdrátových sítích, které jsou zabezpečovány standardem IEEE 802.11. Útok probíhá při komunikaci potřebné k proběhnutí spojení při přihlašování klientské stanice k přístupovému bodu. Daná komunikace se nazývá 4-way handshake. Jmenuje se podle výměny čtyř paketů, které jsou potřebné k určení pravosti hesla k bezdrátové síti a sestavení šifrovacích klíčů pro další komunikaci. Tyto útoky podmiňuje, že jeho odesílatel musí být v okolí signálu dané wifi sítě. Jen změna hesla wifi bohužel nepostačí k vyřešení této hrozby. Vše může vyřešit aktualizace zařízení, která chybu napraví. Tyto útoky zasáhly především OS Linux a Android. Tímto útokem se především potvrdil fakt, že i zdánlivě neprolomitelný protokol WPA2 může být pro každého uživatele velkou hrozbou. [37] [38]

II. PRAKTICKÁ ČÁST

4 DOTAZNÍK

Součástí tohoto dotazníkového šetření jsou cíle analýzy, včetně hlavního a dílčích cílů, dále hypotézy. Jsou zde popsány sběr, zdroje dat a také jejich kontrola. Poté jsou popsány výsledky jednotlivých otázek s verifikací hypotéz a splnění hlavního a dílčích cílů.

Hlavním cílem tohoto průzkumu je definovat a také poukázat na bezpečnostní hrozby při používání OS Android běžnými uživateli.

Dílčí cíle:

- Zjistit, jestli uživatelé používají antivirové aplikace.
- Prozkoumat, kolik uživatelů bylo napadeno nějakým typem mobilního malwaru a ověřit, zda uživatelé využívají různé typy prevence.
- Potvrdit, že uživatelé instalují aktualizace aplikací.
- Zjistit, v jaké míře uživatelé používají nejnovější verze OS Android.
- Ověřit znalost potencionálně nebezpečných oprávnění.

Hypotézy

- Více než 80 % uživatelů čte alespoň občas recenze uživatelů před instalací aplikací.
- Více než 90 % uživatelů ví co je to phishing.
- Více než 50 % uživatelů kontroluje oprávnění a ovlivňuje to jejich rozhodnutí.
- Méně než 10 % uživatelů neinstaluje aktualizace.
- Více než 35 % odpovědí uživatelů se týkají napadení některým z typů mobilního malwaru.
- Více než 50 % respondentů používá mobilní antivirový program.

4.1 Sběr a zdroje dat

Sběr respondentů probíhal převážně na sociální síti Facebook v různých skupinách s tématikou OS Android a Google Play. Dále jsem oslovil i své známé. Celkově bylo vyplněno 175 dotazníků. Návratnost dotazníků byla dobrá, v několika případech se ale stalo, že uživatel předčasně ukončil vyplňování bez odeslání odpovědí. Jelikož se ale nejednalo o vícenásobné ukončení dotazníku na jedné otázce, nebylo třeba se zabývat, jestli některá z otázek dělá respondentům problém při vyplňování.

Pokud někdo z oslovených dané otázce nerozuměl, mohl požádat zadavatele dotazníku pomocí formuláře na úvodní stránce o vysvětlení.

4.2 Kontrola dat

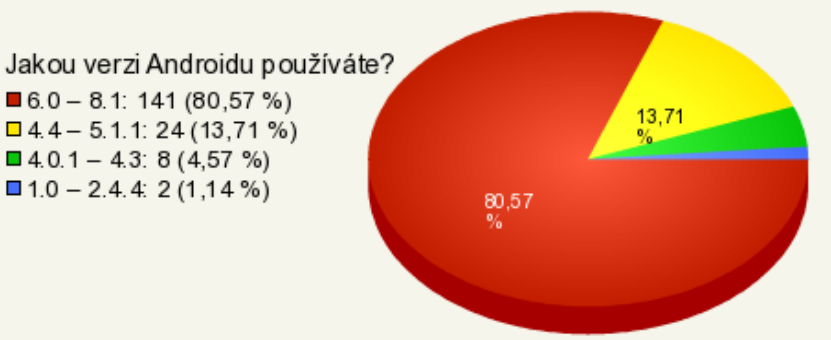
Při tomto průzkumu je použita teoretická kvantitativní analýza dat, která se provádí pomocí internetového dotazníkového šetření. Dotazník je vytvořen v rámci webové služby vyplnto.cz, která svým jednoduchým rozhraním plně vyhovuje potřebám tohoto průzkumu. Zároveň je možné získat respondenty pomocí zveřejnění daného dotazníku na různých serverech za účelem jeho vyplnění, což značně usnadní hledání potencionálních respondentů s OS Android.

V elektronickém formuláři na serveru vyplnto.cz se nachází doplňky pro přidávání obrázků či videí (např. z YouTube), nebo pro vytvoření propracovaného formuláře s větvením a logickým přeskakováním otázek. Pro tuto analýzu stačí jen klasické výběry z jedné, či více možností prostřednictvím zatrhávání, nebo odškrtávání odpovědí. Jediná otázka č. 14 v dotazníku je nepovinná, protože se váže na odpověď z předchozí otázky.

Data z vyplněných dotazníků se na serveru zpracují a generují do různých grafů s výsledky průzkumu každé z otázek. Grafy jsou jednoduché, ale velice přehledné, proto jsem si tuto internetovou službu vybral pro svou práci.

4.3 Výsledky dotazníkového šetření

Dotazník vyplnilo 175 respondentů. Po zpracování odpovědí se objevily následující výsledky.

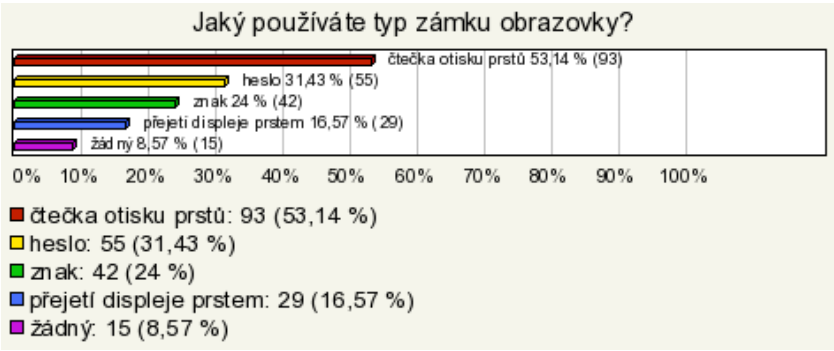


Obr. 5. Používané verze OS Android uživateli

Nejvíce respondentů uvedlo, že používají verzi 6.0 - 8.1, celkem 81% (Obr. 6.). Z toho lze předpokládat, že většina respondentů si v posledních letech koupila nový chytrý telefon. Následovaly odpovědi 4.4 – 5.1.1 (13,71 %), 4.0.1 – 4.3 (4,57 %), a 1.0 – 2.4.4 (1,14 %).

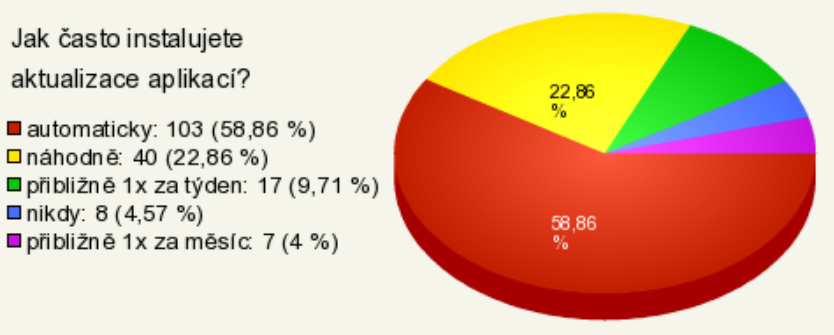
Obr. 6. Počet používaných znaků v heslech uživateli

V heslech při přihlašování respondenti používají nejčastěji 11 a více znaků - 66 osob (37,71 %), v dalším pořadí se sestupně nachází 9-10 znaků, 6-8 znaků a 0-5 znaků jako poslední. Znamená to tak, že větší polovina vyplňujících používá silnější hesla (Obr. 7.).



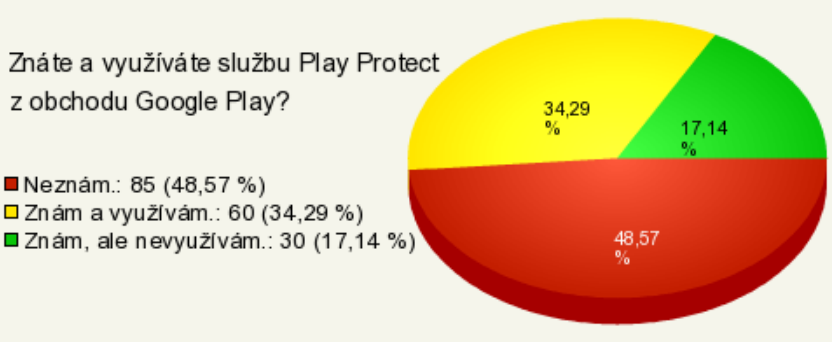
Obr. 7. Používané typy zámku obrazovky

53,14 % respondentů používá čtečku otisků prstů. Tato odpověď je nejčastější. 31,43 % z dotázaných používá heslo, 24 % znak, 16,57 % přejetí displeje prstem. Celkově 15 uživatelů ze 175 nepoužívá žádný ochranný prvek pro odemčení obrazovky (Obr. 8.).



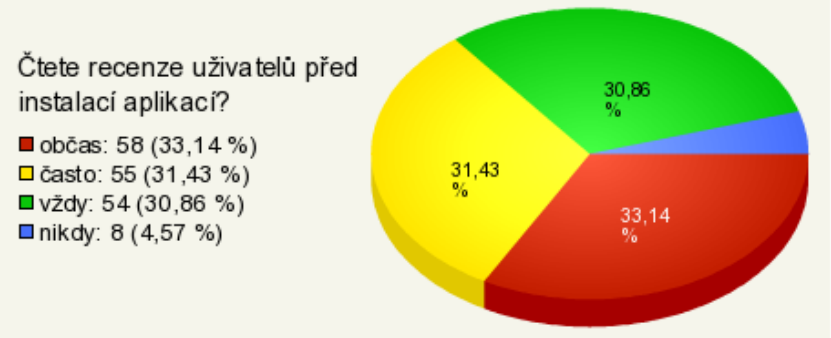
Obr. 8. Časové rozmezí aktualizací aplikací

103 dotazovaných instaluje aktualizace aplikací automaticky. 40 z nich je naopak stahuje a nahrává v náhodných intervalech svépomocí, další využívají aktualizace v menších intervalech. Celkem 8 lidí odpovědělo, že neinstaluje aktualizace (Obr. 9.).



Obr. 9. Znalost služby Play Protect

Službu Play Protect z Google Play nezná 85 respondentů, tedy necelá polovina dotázaných. Větší polovina z nich službu zná, ale celkově ji využívá jen 60 uživatelů (Obr. 10.)

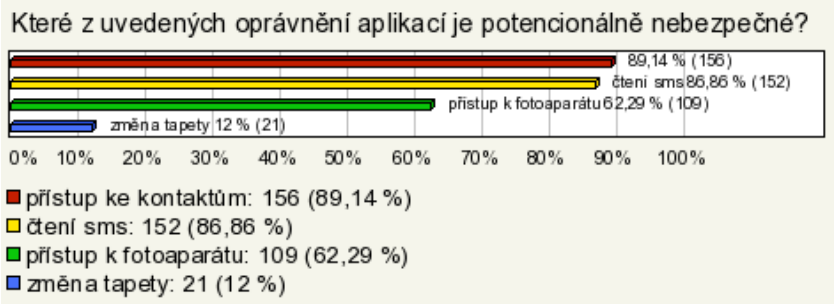


Obr. 10. Čtení recenzí uživatelů aplikací

K této otázce se nachází tři velmi vyrovnané odpovědi. 58 osob čte recenze před instalací občas, 55 často a 54 vždy. Jen 8 uživatelů nikdy před instalací aplikace nečte recenze (Obr. 11.).

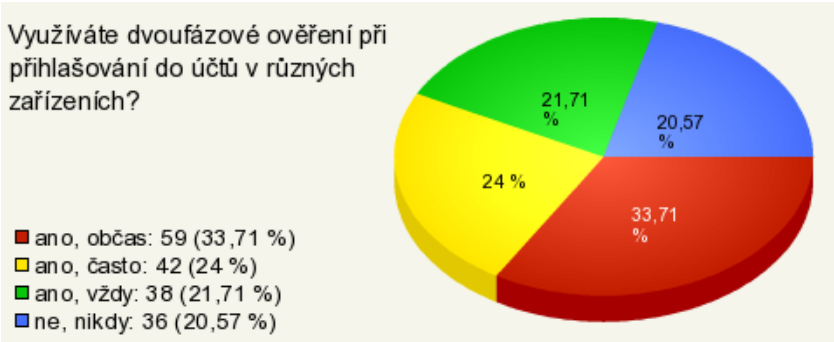
Obr. 11. Sledování požadovaných oprávnění aplikací

Oprávnění aplikací při instalaci čte většina dotázaných, celkově okolo 82 %. Celkem u 92 respondentů čtení oprávnění ovlivňuje jejich rozhodnutí, jestli danou aplikaci nainstalovat. 30 uživatelů nečte oprávnění vůbec (Obr. 12.).



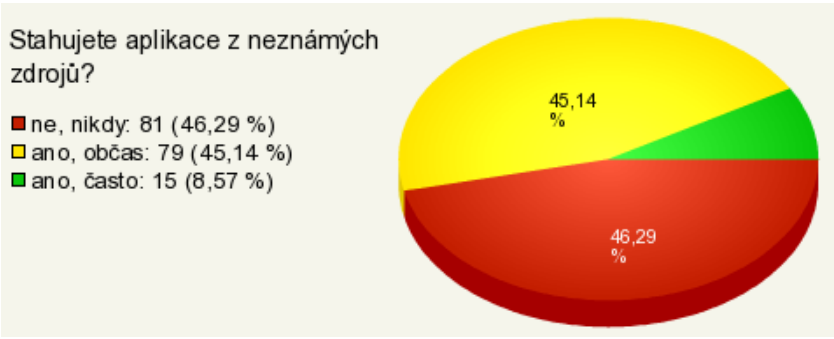
Obr. 12. Označení správných nebezpečných oprávnění

V této otázce jsou správné první 3 odpovědi, takže většina respondentů dokázala poznat alespoň některé z nich. Každý měl možnosti až 4 odpovědí, přičemž změnu tapety jako potencionálně nebezpečnou označilo 21 lidí, i když tato odpověď je nesprávná (Obr. 13.).



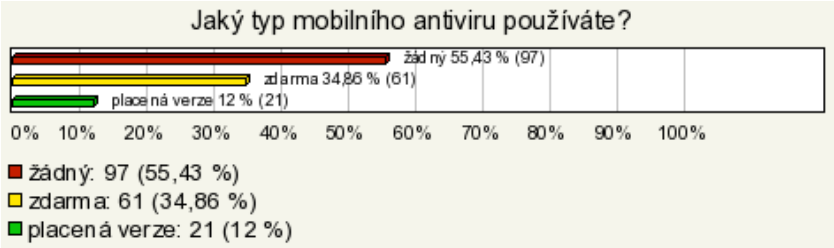
Obr. 13. Využívání dvoufázového ověření k přihlašování

Dvoufázové ověření při přihlašování k účtům používá okolo 80 % dotazovaných, z toho 59 respondentů jej používá občas, 42 často, 38 vždy. 36 osob vypovědělo, že toto ověření nepoužívají. (Obr. 14.).



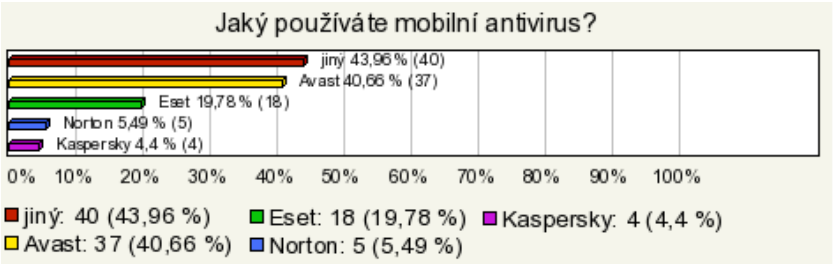
Obr. 14. Stahování aplikací z neznámých zdrojů

Více jak polovina lidí využívá stahování aplikací z neznámých zdrojů, 79 dotázaných občas a 15 často. Naopak 81 z nich nikdy neznámé zdroje nepoužívá (Obr. 15.).



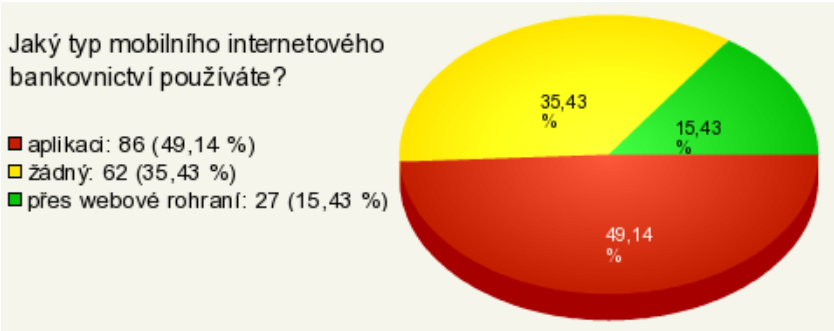
Obr. 15. Používání mobilního antiviru

Mobilní antivirus není ve více jak polovině zařízení respondentů (97). Možná je to zapříčiněno zlepšenou systémovou bezpečností v nových verzích OS Android. 82 osob antivirus používá, z nich 21 placenou verzi (Obr. 16.).



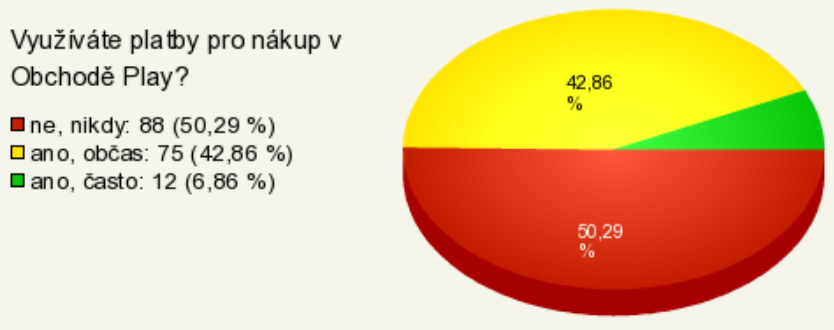
Obr. 16. Používané značky mobilních antivirů

Tato otázka byla nepovinná, jelikož úzce navazovala na otázku předchozí. Pokud někdo z dotázaných nepoužívá antivir, nemusel na tuto otázku odpovídat. Nejoblíbenější mobilní antivir je Avast, následovaný aplikací společnosti Eset. Méně uživatelů pak používá Norton, nebo Kaspersky. Okolo 44 % odpovídajících používá aplikaci od jiných vývojářů. (Obr. 17.).



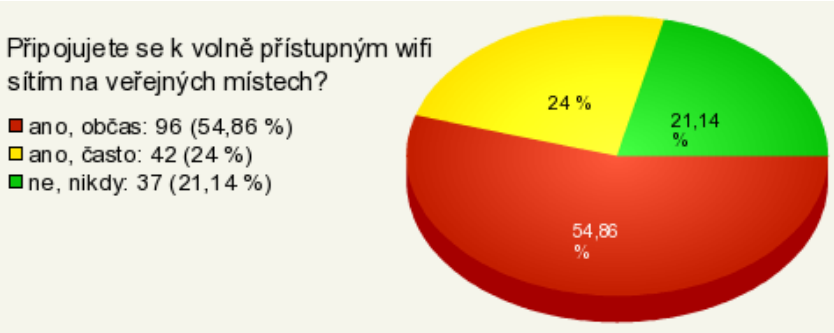
Obr. 17. Používání mobilního bankovnictví

Celkem 115 uživatelů OS Android používá mobilní bankovnictví přes webové rozhraní nebo aplikaci. Naopak 62 z dotázaných internetové bankovnictví nemá (Obr. 18.).



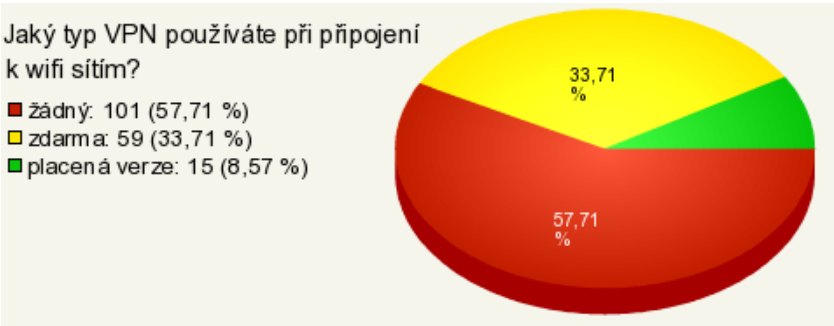
Obr. 18. Využívání plateb v Obchodě Play

V otázce využívání plateb v Obchodě Play jsou velice vyrovnané výsledky. 88 lidí tyto služby nevyužívá a 87 využívá – 75 občas a 12 často. Polovina lidí tedy utrácí za placené služby v obchodě, ať už jde o aplikace, hry, knihy, nebo hudbu (Obr. 19.).



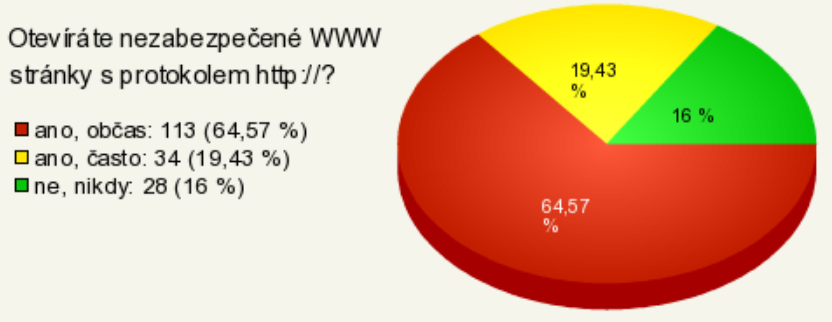
Obr. 19. Připojování k volně přistůpným wifi sítím

Přes tři čtvrtiny uživatelů používá volně přístupné wifi sítě na veřejných místech – celkem 138 uživatelů. Není to vůbec překvapivé, dost uživatelů dává přednost jakékoliv wifi před čerpáním omezeného množství mobilních dat (Obr. 20.).



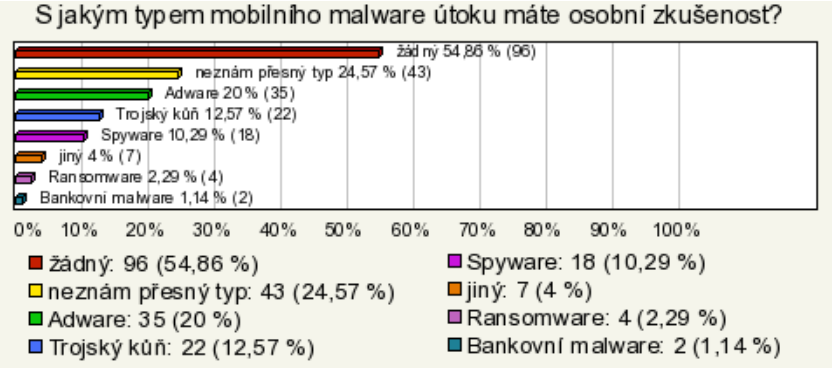
Obr. 20. Používání VPN pro připojení k wifi sítím

Menší polovina respondentů používá VPN při připojování k wifi sítím – 74, z toho 59 ve verzi zdarma. VPN bývá i součástí prohlížečů, jako např. v prohlížeči Opera (Obr. 21.).



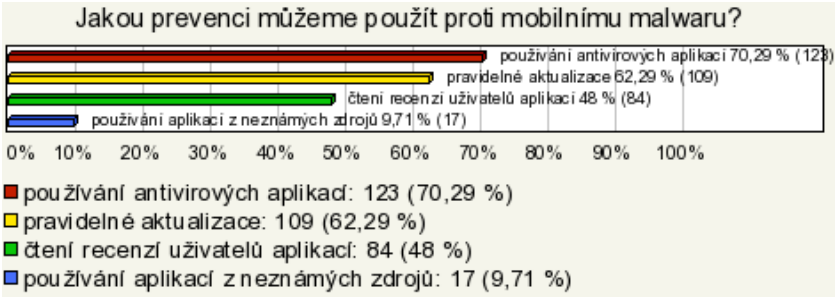
Obr. 21. Návštěva nezabezpečených webových stránek

Většina uživatelů otevírá stránky s nezabezpečeným protokolem http://, celkově 84 %. Jen 16 % dotázaných nezabezpečené stránky neotevírá a nevystavuje se útokům (Obr. 22.).



Obr. 22. Zkušenosti s mobilním malwarem

Více jak polovina respondentů (96) nepřišla do osobního styku s mobilním malwarem. Dalších 43 uživatelů nezná přesný typ mobilního malwaru, kterým byli napadeni. Nejvíce osob bylo napadeno Adwarem (35), Trojským koněm (22), Spywarem (18). 7 dotázaných napadl jiný typ malware útoku, 4 Ransomware a 2 bankovní malware (Obr. 23.).

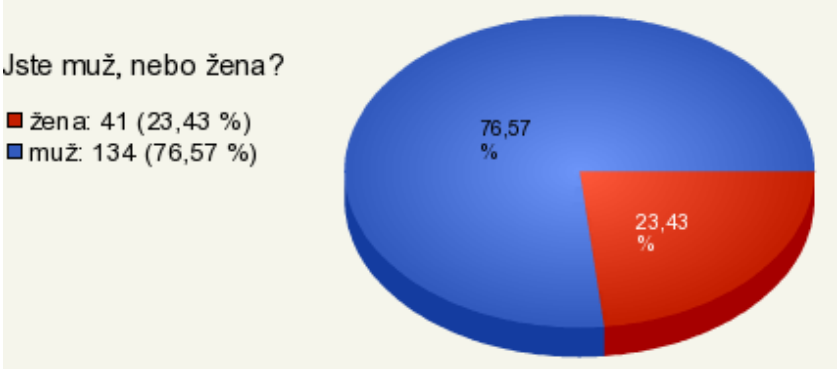


Obr. 23.. Označení správné prevence proti mobilnímu malwaru

Jako správné odpovědi na otázku prevence proti mobilnímu malwaru označuji první tři ve výběru. Většina z uživatelů uvedla, alespoň 1 správnou odpověď, každý mohl označit až 4 odpovědi. Jen 17 uživatelů označilo špatnou odpověď, a to sice stahování aplikací z neznámých zdrojů (Obr. 24.).

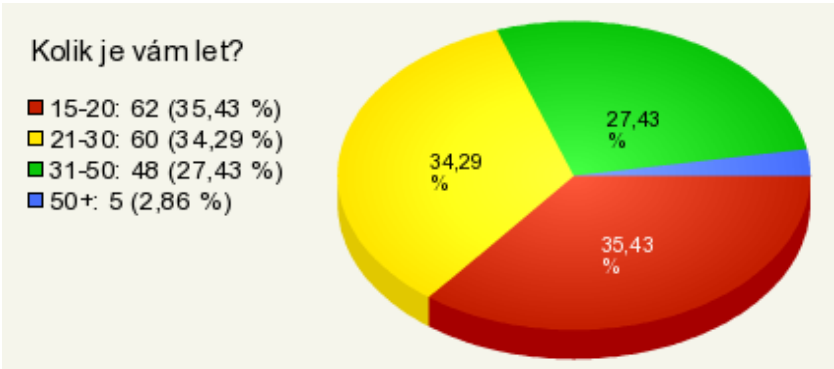
Obr. 24. Znalost pojmu Phishing

Drtivá většina respondentů odpověděla správně na otázku co je to Phishing. Je to podvodná technika k získávání hesel a například také čísel bankovního účtu. Celkově 29 uživatelů odpovědělo špatně (Obr. 25.).



Obr. 25. Pohlaví respondentů

Tento dotazník vyplňovalo přes dvě třetiny mužů. Jen v jedné třetině odevzdaly odpovědi dotazníku ženy (Obr. 26.).



Obr. 26. Věk respondentů

Nejvíce dotázaných odpovídalo ve věku 15-20 let (62), následování věkem respondentů 21-30 let (60), dále věkem 31-50 let (48) a jako poslední 50+ let (5), (Obr. 27.).

4.4 Verifikace hypotéz

První hypotéza uvádí, že více než 80 % uživatelů čte alespoň občas recenze uživatelů před instalací aplikací. To se potvrdilo, jelikož celkem čte recenze uživatelů okolo 95 % respondentů.

Druhá hypotéza uvádí, že více než 90 % uživatelů ví co je to phishing. Tato hypotéza se nepotvrdila, jelikož co toto slovo znamená, vědělo okolo 83 % dotazovaných. I přes nepotvrzení této hypotézy pořád více jak tři čtvrtiny uživatelů, ví co je to phishing, což lze považovat za úspěch.

Třetí hypotéza uvádí, že více než 50 % uživatelů kontroluje oprávnění a ovlivňuje to jejich rozhodnutí. Celkem okolo 52 % dotázaných uvedlo tuto odpověď, takže se hypotéza potvrdila.

Čtvrtá hypotéza uvádí, že méně než 10 % uživatelů neinstaluje aktualizace. Tato hypotéza se také potvrdila, jelikož aktualizace neinstaluje jen okolo 5 % respondentů.

Pátá hypotéza uvádí, že více než 35 % odpovědí uživatelů se týkají napadení některým z typů mobilního malwaru. Celkem okolo 45 % odpovědí je spojeno s některým typem malwaru, tato hypotéza je potvrzena. 103 uživatelů stahuje aktualizace automaticky, 40 náhodně, 17 přibližně jednou za týden a 7 přibližně 1 za měsíc. 7 uživatelů neinstaluje nikdy.

Šestá hypotéza uvádí, že více než 50 % respondentů používá mobilní antivirový program. Tato hypotéza se potvrdila, jelikož okolo 55 % nemá ve svém mobilním zařízení žádný antivirový program.

4.5 Zodpovězení hlavního a dílčích cílů

Hlavním cílem tohoto průzkumu bylo definovat a také poukázat na bezpečnostní hrozby a rizika při používání OS Android běžnými uživateli. To se díky zodpovězeným otázkám podařilo. Identifikoval jsem nejčastější malware útoky na běžné uživatele. Dále jsem ověřil, jak často používají uživatelé různé druhy ochrany jako prevenci. Také mi průzkum ukázal, že většina uživatelů už používá nejnovější verze Androidu 6.0+. Podařilo se mi zjistit, jak často respondenti instalují aktualizace aplikací a také to, že jen zlomek z nich aktualizace nestahuje. Větší polovina uživatelů nepoužívá žádnou antivirovou aplikaci. Děje se tak nejspíše z důvodu zlepšených integrovaných prvků v systému Android

u nejnovějších verzí, které většina respondentů používá. Drtivá většina uživatelů instaluje aktualizace aplikací buď automaticky, nebo v různých časových intervalech. Většina dotázaných poznala alespoň jedno ze tří správných nebezpečných oprávnění, které měli na výběr v poslední otázce.

5 TESTOVÁNÍ APLIKACÍ Z GOOGLE PLAY

Tato kapitola je rozdělena do dvou částí. První část se zaměřuje na analýzu dostupných aplikací na Google Play. Celkem bylo vybráno 8 typů aplikací. Hlavní důvod výběru jednoho z těchto typů je buď časté používání aplikací mezi uživateli v obchodě, nebo výzkumy, které v minulosti upozornily na malware a jiné hrozby v tomto typu aplikace. V druhé části proběhne samotná analýza dostupných aplikací jednotlivých typů z Obchodu Play.

5.1 Analýza dostupných aplikací na Google Play

V analýze jsou vybrány aplikace různých zaměření. V této kapitole jednak můžou uživatelé narazit na nejpoužívanější typy aplikací samotnými uživateli, ale také na potencionálně nebezpečné typy aplikací, na které bylo upozorněno na internetu v rámci různých výzkumů, či článků. Všechny zkoumané aplikace jsou dostupné v Obchodu Play volně ke stažení zdarma. U každého zaměření aplikací je zmíněn důvod použití v této práci a také seznam nejnutnějších oprávnění, které aplikace potřebují k naplnění své funkce.

Svítilny

Často se jedná o velice jednoduchou aplikaci, pomocí které uživatel jen zapíná světlo na zadní straně telefonu. Podle toho by měla vypadat i oprávnění potřebná pro její provoz. V dnešní době se stále více začínají objevovat aplikace, kde je svítilna pouze součást většího celku funkcí. Já se v této práci zaměřím pouze na fungování svítilny, bez jakýchkoliv dalších funkcí. Tento typ byl k testování vybrán pro častý výskyt malwaru v posledních měsících na Google Play, konkrétně v lednu 2018 se na tuto problematiku zaměřil výzkum na internetovém serveru Check Point. Celkem bylo z obchodu Play vyřazeno 22 potencionálně nebezpečných aplikací s malwarem nazývaným LightsOut. Celkově si malware stáhlo od 1,5 do 7,5 milionu běžných uživatelů. Mezi požadovaná oprávnění tohoto typu aplikace patří rozhodně přístup k fotoaparátu, konkrétně ovládání světla diody blesku. Další oprávnění k normálnímu chodu tento typ aplikace nepotřebuje. [39]

VPN aplikace pro Android

Dalším vybraným typem pro tuto analýzu jsou VPN aplikace. Vybral jsem si je z důvodu častého výskytu Adwaru, Spywaru, nebo například trojských koní v těchto typech aplikací. Na tuto problematiku se v roce 2017 zaměřil výzkum prováděný skupinou CSIRO´s Data

61, univerzity v Novém Jižním Walesu a UC Barkley. Po prozkoumání 283 Android aplikací došli k následujícím závěrům. Ve 43 % aplikací se objevil Adware, ve 29 % Trojský kůň a v 5 % Spyware. Z toho také 18 % aplikací s VPN používá tunelovací protokoly bez šifrování, a to i když primárně slibují online anonymitu a bezpečnost uživatelů. VPN aplikace využívají ke svému chodu hlavně oprávnění související se sítí, jako je např. úplný přístup k Internetu. Pokud se bavíme o běžných VPN klientech bez dalších funkcí, tak je to jediný druh oprávnění, které by měla aplikace požadovat. [40]

Antivirové aplikace

Tento typ byl vybrán z důvodu vysokého potencionálního zneužití aplikacemi od neznámých nových vývojářů, které mohou představovat pro uživatele určité riziko oproti řešení od známých firem typu Kaspersky, Eset, Avast, Norton, nebo AVG. V dubnu 2018 se na toto téma zaměřila společnost ESET a ve svém výzkumu označila celkem 35 antivirových aplikací jako potencionálně nechtěné. Z vybraných aplikací 3 z nich mají více jak milion stažení. Jedná se o Super Antivirus & Virus Cleaner,Virus Cleaner Antivirus 2017, nebo hAntivirus – Security. Zde je třeba říci, že se opravdu vyplatí používat osvědčené varianty, které si stáhly desítky milionů uživatelů. Antivirové aplikace mohou mít požadovaná oprávnění více typů, jelikož se aplikace ve vysoké míře nezaměřují jen na čtení dat a kontrolu systému, ale třeba i čištění disku od nepotřebných souborů a další možné funkce. Při kontrole oprávnění je tedy do těch bezpečných nutno zahrnout veškerou možnou aktivitu určité aplikace. [41]

Webový prohlížeče

Jednoznačně jeden z nejpoužívanějších typů aplikací na mobilních telefonech. Díky přístupu k webovým stránkám, který má v dnešní době každý chytrý telefon. Kvůli webovým aplikacím a různým podvodným technikám a webům bývají prohlížeče častým terčem útoků. Typickým příkladem je prohlížeč Google Chrome. Na serveru CVEdetails je archivováno celkem 1545 útoků na tuto službu napříč všemi platformami. Tento prohlížeč je vývojáři často aktualizován, jsou opravovány chyby, avšak pro svou popularitu je oblíbený mezi různými útočníky. Z tohoto důvodu byl tento typ aplikace vybrán do analýzy. Některé, často neznámé prohlížeče dokážou být pro uživatele také hrozbou. [50]

Aplikace pro čištění úložiště

Důvod proč testovat tento typ aplikace je podobný jako u různých antivirů. Tyto nástroje mohou v sobě skrývat např. nebezpečná oprávnění. Takovéto nástroje mohou být v některých případech součástí např. antivirové aplikace. Už v minulosti v roce 2013 se v obchodě od společnosti Google objevily falešné aplikace, které na první pohled vypadaly zcela normálně, zastíraly svou opravdovou činnost. V některých se například nacházel phishing. Pomocí velice identického formuláře pro přihlášení k účtu Android získali mnoho uživatelských účtů a hesel. [42]

Čtečky QR kódů

Tyto aplikace slouží k rozpoznání QR kódů zobrazených na různých výrobcích, nebo službách. QR kódy v poslední době začínají mít široké využití, uplatňují se např. v marketingu, nebo na vizitkách pro nahrání kontaktních informací dané osoby. Do tohoto kódu se dají zašifrovat jakékoliv textové zprávy, nebo např. může být použit pro odkaz na webové stránky určitého výrobku. Není proto divu, že se v obchodě Play tyto aplikace velice rozšířily. V březnu roku 2018 společnost SophosLab zpozorovala na serveru Google Play 6 aplikací QR čteček, které v sobě skrývaly stejný malware označený jako Andr/HiddnAd-AJ. Po instalaci uživatelem tento škodlivý software začne pracovat až za 6 hodin - konkrétně pracuje s Adwarem, zaplavuje uživatele reklamami na celé obrazovce, otevírá inzeráty na webových stránkách a odesílá různá oznámení obsahující odkazy na reklamu. Celkově si jednu z těchto aplikací stáhlo kolem půl milionu lidí. [45]

Aplikace pro natáčení a fotografování

Dalším zvoleným typem jsou tzv. kamery. Tyto aplikace umožňují primárně fotografování a natáčení videí, dále se mohou zaměřovat na jejich úpravu a zapisování dat na disk a sdílení mezi dalšími aplikacemi. Funkce použití tohoto typu aplikace se považuje za jednu z nejzákladnějších na Androidu vůbec. V roce 2017 byly zpozorovány společností Check Point nebezpečné kamery ukrývající malware HummingWhale. Je to modifikace ransomwaru HummingBad. Všechny aplikace byly nahrané pod jmény falešných čínských vývojářů. Kromě infikovaných aplikací fotoaparátu vědci identifikovali 16 dalších aplikací jiného typu se stejným malware. Nejprve server poskytuje falešné reklamy a nainstalovaný malware v aplikaci. Jakmile se uživatel pokusí zavřít reklamu, aplikace, kterou stáhne malware, se nahraje a je spuštěna v zařízení. Poté se generuje falešný identifikátor odkazu, který malware používá k vytváření příjmů pro pachatele. Tento škodlivý kód se zaměřuje také na zobrazování škodlivé reklamy a skrytí

původní aplikace po instalaci. Dokonce dokáže přidávat recenze a hodnocení aplikací uživateli v Google Play. Tento typ aplikací je lehce zneužitelný, pokud má aplikace oprávnění přístupu k fotoaparátu a zároveň k síti, může se jednoduše stát, že bude bez vědomí natáčet, nebo fotografovat a následně data odesílat. Proto v tomto případě je důležité také sledovat datový tok aplikací. [43]

Hry

Jeden z nejpočetnějších typů aplikací v Obchodě Play jsou hry, to byl jeden z důvodů při výběru k této analýze. Díky placenému obsahu uvnitř vývojáři často generují ohromné zisky. Některé hry v sobě však také mohou skrývat hrozby ať už v podobě Spywaru, phishingu, či Ransomwaru. Při instalaci je důležité sledovat oprávnění, hry by neměly nijak zasahovat oprávněními do systémového chodu telefonu. Je třeba dávat pozor, zda aplikace používá zbytečná oprávnění, které přímo nesouvisí s funkcemi dané aplikace. Pokud aplikace využívá placený obsah, může požadovat přístup k platebnímu styku. V obchodě jsou také rozšířeny aplikace s návody pro různé hry. V dubnu 2017 výzkum společnosti Checkpoint ukázal, že 40 aplikací v Google Play bylo napadeno malwarem Falseguide
a poté byly z obchodu vyřazeny. Většina z nich byly návody na různé hry. Tyto typy aplikací jsou v poslední době velmi populární. FalseGuide požaduje neobvyklé oprávnění už při instalaci - oprávnění správce zařízení. Malware používá oprávnění administrátora, aby se vyhnul vymazání uživatele, což je akce, která normálně naznačuje škodlivý záměr. [44]

5.2 Testování aplikací pomocí běžně dostupných nástrojů

V této kapitole otestuji aplikace vybraných typů z předchozí kapitoly běžně dostupnými prostředky, kterými se každý běžný uživatel může bránit. K tomu budou použity následující nástroje.

5.2.1 Použité běžně dostupné nástroje a techniky

Antivirové programy - celkem bylo použito 5 antivirových programů značek Avast, Eset, Norton, Kaspersky, AVG.

Ochrana obchodu Play - Google Play Protect zmíněno již v 2. kapitole teoretické části.

Webové databáze bezpečnostních hrozeb - CVE details a Exploit-DB.

Monitorování datového toku aplikací - Systémová aplikace Android + aplikace My data manager.

Sledování datového toku každého typu aplikací bude probíhat několik dní s ohledem na možné pozdější zahájení nebezpečné aktivity jednotlivých aplikací. Dále se u každé aplikace tato část práce zaměřuje na její požadovaná oprávnění, popis jednotlivých žádoucích a nežádoucích oprávnění. Součástí analýzy oprávnění jsou nebezpečná oprávnění z tabulky 2 strana 28, zaměřuji se na jejich počet a důvod použití u jednotlivých aplikací. Tato oprávnění může každý uživatel s verzí Android 6.0 a vyšší libovolně udělovat při dotazování aplikace, pokud si v nastavení sám nezvolí, že oprávnění bude mít produkt dlouhodobě. Tato analýza se zaměřuje jen na bezpečnost, ne na funkcionalitu aplikací. Použité nástroje musí dokázat pochopit běžný uživatel používající OS Android, to je hlavní cíl této práce. Od každého vybraného typu budou otestovány 2 aplikace. Tato varianta je vybrána z důvodu porovnání příbuzných aplikací.

5.2.2 Parametry hodnocení

Každá aplikace bude hodnocena podle stupnice hodnocení 1 až 5, přičemž jedna je nejlepší hodnocení a pět nejhorší. Celkové hodnocení každé aplikace bude záviset na několika kritériích. Každá z aplikací bude ohodnocena buď 0 body, nebo 1 bodem, podle splnění podmínky v kritériu hodnocení.

Jednotlivá kritéria pro hodnocení

- analýza požadovaných oprávnění aplikace, zaměření na nebezpečná oprávnění
- detekce malwaru běžně dostupnými antivirovými nástroji
- sledování datového toku, denní spotřeby dat aplikace
- sledování stavu hrozeb aplikace na webu CVEdetails a Exploit-DB
- sledování spotřeby baterie aplikacemi

Jednotlivé výsledky hodnocení

- známka 1 - doporučuji ke stažení, aplikace ve všech ohledech bezpečná
- známka 2 - doporučuji ke stažení, aplikace s drobnými nedostatky
- známka 3 - nedostatky středního rozsahu, doporučení sledování chodu aplikace

- známka 4 - nedoporučuji, hrubé nedostatky v bezpečnosti aplikace
- známka 5 - škodlivá aplikace s účelem útoku na uživatele

5.2.3 Představení aplikací a jejich oprávnění

V každém typu jsou nejprve představena jména použitých aplikací (Obr. 28.), jejich přibližný počet stažení, celkové hodnocení uživateli ve hvězdičkách dle obchodu Play. Posledním ve výčtu údajů je použitá verze dané aplikace. Dále je zde věnována pozornost jednotlivým oprávněním, rozdělení na nebezpečná a ostatní oprávnění i s komentářem možnosti využití nebezpečných oprávnění aplikacemi.

Obr. 27. Seznam aplikací

5.2.3.1 Svítilny

Svítilna od Zerone Mobile Inc. s hodnocením uživatelů 4 hvězdičky, stažením přes 10 miliónů uživatelů, verze 1.3.7.

Jednoduchá svítilna od YoonSoft s názvem WoW FlashLight, celkem přes půl milionů stažení, verze 4.1.

WoW Flash Light požaduje 3 oprávnění - úplný přístup k síti a zobrazování síťových připojení, pořizování fotografií a videí. Jen poslední jmenované oprávnění je nutné pro chod aplikace, bez něj hlavní funkce nebude fungovat. Oprávnění úplný přístup k síti a zobrazování síťových připojení je relevantní jen v případě nutného spouštění aktualizace. Svítilna od Zerone Mobile Inc. mimo tři již zmíněná oprávnění žádá uživatele o povolení bránění přechodu do režimu spánku, přijímání dat z internetu a zobrazení připojení Wifi.

Tato oprávnění nejsou pro uživatele velkou hrozbou, ale mohou způsobit například vysokou spotřebu dat nebo energie v baterii. Je třeba uvažovat nad počtem oprávnění jako takových, protože čím víc oprávnění aplikace má, tím více si může dovolit.

5.2.3.2 VPN aplikace pro Android

Turbo VPN od VPN proxy master s celkovým stažením 10 tisíc uživatelů, hodnocení aplikace 4,5 hvězdičky, verze 1.4.

Secure VPN od Signal lab se stažením přes půl milionu uživatelů, hodnocení 4,8 hvězdičky, verze 1.0.5.

Turbo VPN požaduje přístup k vyhledávání účtů v zařízení a čtení, upravení, nebo odstranění souborů na SD kartě. Po zamítnutí těchto oprávnění se zobrazí hláška, že aplikace byla vytvořena pro starší verze Android. Tato oprávnění rozhodně nejsou bezpečná, zvláště vyhledávání účtů může vést ke ztrátě osobních údajů. Aplikace společně vyžadují zobrazování síťových připojení a také wifi, přijímání dat z internetu, úplný přístup k síti, bránění přechodu do režimu spánku. Tato oprávnění se zdají oprávněná, protože souvisí s chodem tohoto typu aplikace, omezení režimu spánku však může znamenat větší spotřebu baterie. Turbo VPN dále požaduje rozpoznávání aktivity, což je zásah do soukromí z důvodu sledování polohy. Secure VPN chce ke svému chodu párování se zařízeními bluetooth - dle popisu aplikace v obchodě jsem neshledal žádnou funkci, která by toto oprávnění měla požadovat a dále povolení zavřít ostatní aplikace, z důvodu bezpečnostních chyb.

5.2.3.3 Antivirové aplikace

Antivirus scanner od JESKO, přes 10 tisíc stažení, 4,4 hvězdičky, verze 1.7

Security Antivirus Android od CA Uber Apps, 1 milion stažení, 4,2 hvězdičky, verze 1.1.3

Antivirus scanner si žádá od uživatele přístup k přibližné a přesné poloze a čtení, úpravě a odstraňování obsahu SD karty. První oprávnění znamenají omezení ochrany jejich soukromí, údaje o poloze tato aplikace ke svému chodu rozhodně nepotřebuje. Mezi ostatní požadovaná oprávnění patří výpočet místa pro ukládání aplikace, umožňuje načtení svého kódu, dat a velikosti mezipaměti, úplný přístup k síti a zobrazování síťových připojení. Security antivirus Android chce přístup ke stejným oprávněním, kromě přístupu k přesné a přibližné poloze.

5.2.3.4 Webové prohlížeče

Turbo VPN browser od Abdul Apps, přes 1 tisíc stažení, 3,6 hvězdičky, verze 1.0.8

Puffin Web browser od CloudMosa, Inc., přes 10 miliónů stažení, 4,3 hvězdičky, verze 7.5.0.20369

Turbo VPN browser chce z nebezpečných oprávnění povolit přístup k přesné poloze zařízení a ke čtení, úpravě a odstraňování obsahu SD karty. První oprávnění teoreticky může potřebovat například z důvodu lokalizace polohy na webovém serveru s mapami, druhé například k zápisu záložek či dat o prohlížení na disk. Nedoporučuji však tato oprávnění povolovat automaticky. Z dalších oprávnění vyžaduje úplný přístup k síti, zobrazování síťových připojení a instalace zástupců. Toto poslední oprávnění, kdy aplikace může bezdůvodně umisťovat zástupce na plochu, je pro chod aplikace zbytečné. Puffin má ve výběru obdobná oprávnění, ve výčtu nebezpečných ještě přidává nahrávání zvuku a pořizování fotografií a videí, což pro normálně fungující prohlížeč jsou nepotřebná oprávnění, proto by je uživatel neměl povolovat automaticky, ale jen při oprávněné potřebě např. při video hovoru přes webovou aplikaci. Z ostatních požadavků ještě vyžaduje bránění přechodu telefonu do režimu spánku a přijímání dat z internetu.

5.2.3.5 Aplikace pro čištění úložiště

Smart Cleaner od SUVsoft Inc., přes 500 tisíc stažení, 4.1 hvězdičky, verze 1.4

Cleaner od AM project, přes 10 tisíc stažení, 4 hvězdičky, verze 1.0.1

Smart Cleaner používá z nebezpečných oprávnění čtení, úpravu či odstraňování obsahu SD karty například z důvodu čištění dat a z dalších oprávnění zavření ostatních aplikací kvůli zrychlení systému, zobrazování síťových připojení, úplný přístup k síti. Cleaner od AM projekt navíc požaduje načtení spuštěných aplikací pro odhalení informací o používaných aplikacích, výpočet místa pro ukládání aplikace.

5.2.3.6 Čtečky QR a čárových kódů

QR & Barcode Scanner od sartajapp, přes 10 tisíc stažení, 4,8 hvězdičky, verze 1.0

Barcode Scanner & QR Code Reader od MoZah, 500 stažení, 4 hvězdičky, verze 1.0.

QR & Barcode Scanner požaduje oprávnění k pořizování fotografií a videí, čtení, úpravu a odstraňování obsahu na SD kartě. Druhé jmenované úplně nesouvisí s chodem aplikace, čtení obsahu aplikace teoreticky potřebuje, ale ne úpravu a odstraňování. Z ostatních

požadavků na systém vyžaduje ovládání vibrací, zobrazování síťových připojení, úplný přístup k síti. Barcode Scanner & QR Code Reader od MoZah ještě navíc k už jmenovaným oprávněním přidává bránění přechodu do režimu spánku, což aplikaci rozhodně neslouží k plnění funkce a dále přijímání dat z internetu, které musí vyžadovat pro svůj chod.

5.2.3.7 Aplikace pro natáčení a fotografování

HD Camera+ od Best App - Top Droid Team, přes 100 tisíc stažení, 4,4 hvezdičky, verze 1.2

Camera FV-5 Lite od FGAE, přes 10 miliónů stažení, 4 hvězdičky verze 3.31.4

První jmenovaná aplikace vyžaduje určování přibližné a přesné polohy pomocí GPS a sítě, čtení, úpravu a odstraňování obsahu SD karty, pořizování fotografií a videa, nahrávání zvuku bez svolení uživatele, úplný přístup k síti, bránění přechodu do režimu spánku, zobrazování síťových připojení, zobrazení připojení wifi a připojení a odpojení od wifi. Nahrávání zvuku bez svolení a poslední tři funkce související se sítí nejsou zcela oprávněné. Další oprávnění aplikace k chodu potřebuje, údaje o přesné poloze potřebují tyto dvě aplikace jen z důvodu zadání zeměpisných souřadnic k fotografiím. Camera FV - 5 lite nepotřebuje nahrávání zvuku, zobrazení, připojení a odpojení od wifi a zobrazení síťových připojení, avšak navíc přidává vyhledávání účtů v zařízení a kontrolu licence ve službě Play. Vyhledávání účtů může znamenat krádež osobních údajů.

5.2.3.8 Hry

Truck simulator 2014 Free od Thetis Games and Flight Simulator, přes 1 milion stažení, 3,6 hvězdičky, verze 1.5

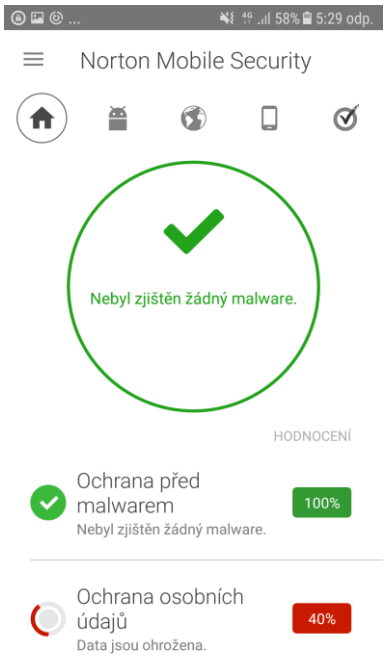
Cheat and Guide for GTA 5 free od Free grand V, přes 1 milion stažení, 3,7 hvězdičky, verze 1.0.8

Truck simulator 2014 Free požaduje více nebezpečných oprávnění, než opravdu potřebuje. Mimo fakturační služby Play, kterou může využít k placenému obsahu, jsou další nebezpečná oprávnění jistě neoprávněná. Jedná se o čtení, úpravu a odstraňování obsahu SD karty a čtení stavu a identity telefonu. Je zde možnost společného zneužití v souvislosti úplného přístupu k síti a zobrazení připojení síťových připojení a wifi. Hry a podobné aplikace by měly požadovat minimum nebezpečných oprávnění ke svému chodu. Aplikace Cheat and Guide vyžaduje přístup k přibližné poloze pomocí sítě a čtení, úpravu,

nebo odstraňování obsahu SD karty. Z ostatních vyžaduje úplný přístup k síti a zobrazování síťových připojení. Tato oprávnění se zdají být velice podezřelá z důvodu zasahování do osobního soukromí. Aplikace nemá žádnou funkci, jak by toto oprávnění využila.

5.2.4 Analýza pomocí antivirových nástrojů

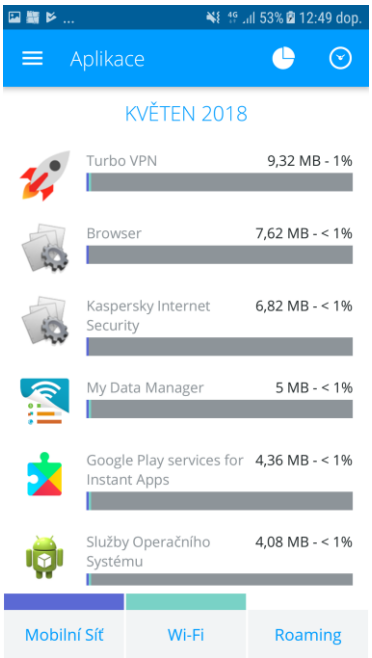
Nejprve aplikace procházely testem Google Play Protect, nedošlo k detekci jakéhokoliv škodlivého softwaru. Při testování antivirovými nástroji jsem použil mobilní aplikace z Obchodu Play od značek Avast verze 6.10.7, Eset 4.0.41.0, Norton 4.1.1.4117, Kaspersky 11.16.4.589 a AVG 6.9.3. Jsou to jedny z nejstahovanějších antivirových nástrojů v obchodě. Ani jeden z programů nedetekoval uvnitř 16 aplikací žádný škodlivý software. Příklad takového testu je vidět na obrázku 29. V obchodě je dle údaje z prosince 2017 webovým serverem statista.com celkem přes 3,5 milionu aplikací, Google zpřísnil kontrolu malwaru a aplikace odstraňuje. I díky těmto důvodům výsledek není nijak překvapivý. Testování proběhlo po nainstalování všech aplikací souhrnnými testy antivirových aplikací. Antiviry byly nainstalovány postupně do zařízení, avšak každý až po odinstalování předchozího použitého z důvodu možného nesouladu programů s antivirovou funkcí. Záměrně jsem se náhodně snažil vybrat i nové, nebo méně stahované aplikace s horším hodnocením, aby byla větší šance na nalezení problému, ale nestalo se tak. Lze tak říct, že použité aplikace v této části obstály úspěšně bez výjimky. [46]



Obr. 28. Test aplikací

5.2.5 Monitorování datového toku aplikací

Monitorování datového toku zajistily dva nástroje. Systémová aplikace v nastavení telefonu a pro porovnání My data manager. Celkově byly aplikace monitorovány 5 dní za účelem podrobnějšího zkoumání. Aplikace byly zapnuty jednou, ihned po instalaci. Zde jsou výsledky. Aplikace Turbo VPN za 5 dní v telefonu spotřebovala přes 9,32 MB (Obr. 30.), z toho první den 2 MB, přes mobilní data a wifi. Tato zvýšená datová aktivita byla zjištěna už první den antivirovým programem Norton. Jinak při monitorování nebyl zpozorován podezřelý zvýšený tok dat. Aplikace odesílaly data maximálně v řádech několika stovek kilobajtů denně. V prvním dni sledování aplikace přesáhla spotřebu dat přes 1 MB aplikace Turbo VPN browser, celkem cca 1,9 MB a Puffin cca 1,2 MB z důvodu zkoušky těchto prohlížečů. Při jejich nepoužívání datová aktivita klesla na minimum. V pátém dni žádný testovaný objekt nevyužíval už více než 0,1 MB za den.

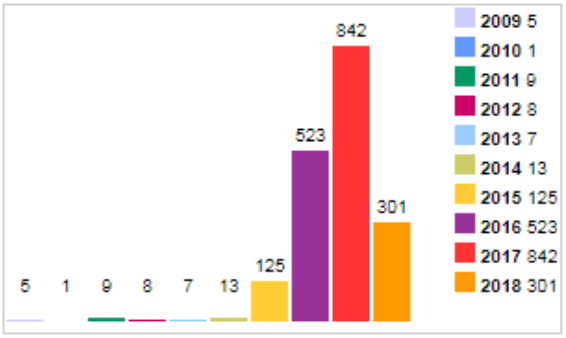


Obr. 29. Spotřeba dat testovaných aplikací

5.2.6 Sledování hrozeb na serveru CVEdetails a Exploit-DB

Tyto webové servery se nacházejí na stránkách https://www.cvedetails.com/ a https://www.exploit-db.com/. Slouží k vyhledávání bezpečnostních hrozeb na různých platformách. Do jejich vyhledávačů byly postupně zaneseny jména všech analyzovaných aplikací. Jinak lze vyhledávat např. dle produktu, nebo platformy. Na obou serverech se neobjevily žádné výsledky vyhledaných hrozeb na tyto konkrétní aplikace. Server

CVEdetails archivuje celkově 1834 všech typů útoků na platformu Android od Google k datu 15. května 2018. Na obrázku 31 pod textem je graf počtu hrozeb v jednotlivých letech. Dle současného vývoje lze předpokládat zvýšení počtu hrozeb na tento OS.



Obr. 30. Graf hrozeb OS Android na webu CVEdetails [49]

5.2.7 Sledování spotřeby baterie

Poslední kontrola aplikací je zaměřena na spotřebu baterie. Všechny aplikace jsem spustil a v nastavení spotřeby baterie sledoval jejich reálnou spotřebu energie. Nejvíce energie využívala aplikace Svítilna již hodinu po instalaci, jednalo se o odběr cca 2,19 % za hodinu (Obr. 32.). Zbylé aplikace využívají zanedbatelnou část energie z baterie.

Obr. 31. Zvýšená spotřeba baterie testovaných aplikací

5.2.8 Hodnocení testovaných aplikací

Svítilna dostává známku 3 za zvýšený počet oprávnění a zvýšenou spotřebu baterie. Jednoduchá svítilna známku 2 za menší počet oprávnění, a spotřebu baterie.

Turbo VPN získává známku 4 za zvýšený počet oprávnění, možnost zneužití osobních údajů díky vyhledávání účtů, zvýšený datový tok aplikace při jejím nepoužívání. Secure VPN dostává známku 3 za zvýšený počet oprávnění, neoprávněný požadavek přístupu k bluetooth.

Antivirus scanner od JESKO dostává známku 2 za nepotřebný přístup k přibližné a přesné poloze. Security Antivirus Android od CA Uber Apps 1. Žádná oprávnění nebyla shledána jako nebezpečná.

Turbo VPN browser od Abdul Apps získává známku 2 za neobvyklá oprávnění. Puffin Web browser od CloudMosa dostává známku 3 za vysoký počet nebezpečných oprávnění včetně určování přesné a přibližné polohy a bezdůvodného nahrávání zvuku.

Smart Cleaner od SUVsoft Inc. dostává známku 1, nebyla nalezena žádná podezřelá aktivita, ani oprávnění. Cleaner od AM project dostává známku 2 za zvýšený počet oprávnění.

QR & Barcode Scanner od sartajapp získává známku 2 za nepotřebné oprávnění úpravy a odstraňování obsahu karty SD. Barcode Scanner & QR Code Reader od MoZah dostává známku 3 za nepotřebná oprávnění s úpravou a odstraňováním obsahu karty SD a bránění přechodu do režimu spánku, které dlouhodobě může způsobovat zvýšenou spotřebu baterie.

HD Camera+ od Best App od Top Droid Team za vysoký počet nebezpečných oprávnění včetně nahrávání zvuku bez svolení uživatele dostává známku 3. Camera FV-5 Lite od FGAE za vysoký počet oprávnění dostává známku 2.

Truck simulator 2014 Free od Thetis Games and Flight Simulator si vysloužil známku 3 za neoprávněná nebezpečná oprávnění zejména čtení stavu a identity telefonu. Může docházet ke ztrátě osobních údajů. Cheat and Guide for GTA 5 free od Free grand V si vysloužila známku 3 za vysoký počet oprávnění pro aplikaci, která je rozhodně nepotřebuje.

5.2.9 Hodnocení testovaných typů aplikací

Je důležité zhodnotit také typy testovaných aplikací. Z osmi testovaných typů nejlépe dopadly antivirové aplikace a nástroje na čištění disku. Stalo se tak především z důvodu nízkého počtu nežádoucích oprávnění u těchto aplikací. Aplikace tohoto typu běžně požadují k povolení daleko více, celkově s více jak 20 oprávněními už mohou být pro uživatele větší hrozbou. V principu toto platí pro všechny typy testovaných aplikací. Každé oprávnění může znamenat funkci navíc, ale taky hrozbu, proto je důležité zhodnotit všechny funkce aplikace a dle toho zhodnotit dané nebezpečné oprávnění. Dle zmíněných výzkumů a mých závěrů z analýzy spíše nedoporučuji stahovat neznámé VPN aplikace. Co se týče VPN aplikací, doporučuji stáhnout spíše aplikace od známých vývojářů, např. typu Kaspersky. Nelze vyvodit podrobné závěry, který typ aplikace doporučit stahovat či ne, protože jsem od každého typu vyzkoušel jen dvě aplikace. Pro detailnější analýzu jednotlivých typů bych se musel zaměřit na větší počet testovaných aplikací jednoho druhu. Všechny typy aplikací, i ostatní, které jsem v této podkapitole nejmenoval, doporučuji stahovat s obezřetností se zaměřením na analýzu použitých oprávnění, testování na přítomnost malwaru, monitorování toku dat a spotřeby baterie, analýzu hrozeb v internetových databázích. Jen tak si běžný uživatel může být jistý, že si nestáhl žádnou škodlivou aplikaci. V neposlední řadě je dobré číst hodnocení a recenze uživatelů, to taky pomůže pomoci odhalit hrozbu předem. U recenzí je nutné brát v potaz zaujatost uživatele, proto je dobré skutečnosti ověřovat pomocí nástrojů, nebo hledat další recenze stejného typu.

6 PREVENCE

V této kapitole je popsána stručná prevence proti mobilním hrozbám a hlavně malwaru. Tyto jednotlivé podkapitoly mohou sloužit jako přehled základních doporučených pravidel pro běžného uživatele při chování s OS Android. Inspirací při tvorbě této kapitoly jsou také zkušenosti samotných uživatelů.

6.1 Udržování systému a aplikací v co nejnovější verzi OS Android

Přestože se nové aktualizace Androidu pro starší telefony bohužel neobjevují tak pravidelně jako pro telefony s novou verzí OS Android, je vždy vhodné nainstalovat jakékoliv aktualizace, jakmile jsou v nabídce. Může se jednat pouze o opravení bezpečnostních chyb na dané verzi OS, nebo také o celkově přepracované prostředí novější verze. Vzhledem k tomu, že společnost Google začala poskytovat měsíční bezpečnostní aktualizace pro systém Android u nejnovějších verzí, ochrana proti škodlivému zneužití se hodně zlepšila a má smysl udržovat zařízení v aktuální verzi, aby se zvýšila bezpečnost vašeho systému. To samé platí i o aktualizacích aplikací. Např. starší verze bankovní aplikace může být napadena škodlivým kódem, proto je nutno stále aktualizovat. U telefonů se starším OS než 6.0 je potřeba zapřemýšlet nad pořízením novějšího, protože z hlediska bezpečnostních chyb, které nebudou opraveny žádnou aktualizací systému, si uživatelé často neuvědomují, jakým hrozbám jsou vystaveni. [47]

6.2 Dvoustupňová autentizace

V různých účtech v aplikacích nebo na webu je využíváno dvoustupňové ověření, které nejenže vyžaduje vytvoření hesla uživatelem, ale zároveň propojí účet s telefonním číslem, e-mailovou adresou nebo další účelovou aplikací. Jakmile se kdokoliv pokusí z vašeho účtu přihlásit na novém zařízení nebo změnit heslo, musí projít i druhým krokem v procesu ověřování, což znesnadní jeho cestu za přihlášením. S tímto typem autentizace se můžete setkat např. v bankovních aplikacích, Google účtu, Facebooku a na dalších účtech. [47]

6.3 Žádné instalace aplikací z nedůvěryhodných zdrojů

Společnost Google se snaží dělat dobrou práci při provozování Obchodu Play bez škodlivých aplikací, pro uživatele zřídila službu Play Protect, která sama kontroluje pravidelně aplikace v rámci Google Play, a sama se snaží denně kontrolovat nespočet aplikací pomocí Google Bouncer. Avšak provozovatelé dalších služeb podobného

charakteru nemusí věnovat bezpečnosti zdaleka takovou pozornost. Proto je na místě si tyto servery pečlivě prověřovat na internetu pomocí recenzí různých uživatelů, webových serverů zabývajících se bezpečnostními hrozbami a dalších. Mimo Google Play samozřejmě je i pár zavedených obchodů jako např. Samsung Apps a dalších obchodů provozovaných např. výrobci telefonů, které jsou všeobecně uživateli užívány. Samozřejmě mnoho vývojářů nabízí své aplikace ve více obchodech, takže hodně záleží i na důvěryhodnosti samotného vývojáře. Aplikace mohou dostat do styku vaše zařízení s jakýmkoliv škodlivým kódem připojeným k sobě, což může způsobit instalace dalších nežádoucích aplikací nebo např. nežádoucí oznámení. Takže pokud to není nezbytné, instalaci neznámých aplikací z nedůvěryhodných zdrojů se úplně vyhněte, vždy kontrolujte, zda vaše stahování pochází z ověřeného zdroje. [47]

6.4 Vnímání a rozlišování potencionálně nebezpečných oprávnění aplikací

Pokud nevlastníte telefon s OS Android 6.0 a vyšší, věnujte zvýšenou pozornost už při instalaci jakékoliv aplikace nebo aktualizace, jelikož jejím nainstalováním povolujete přístup k dané funkci. Telefony Android používající verzi 6.0 Marshmallow a vyšší mají při správě oprávnění daleko větší kontrolu. Sama upozorňuje na nebezpečná oprávnění při startu a v nastavení v položce aplikace informuje uživatele o oprávněních pro právě zobrazenou aplikaci. [47]

6.5 Využívání bezplatného online zálohování

K účtu Google se automaticky přidružují kontakty, zprávy, Gmail a také záznamy v kalendáři Google. Pokud si tedy koupíte nový telefon nebo se přihlásíte do svého účtu z webového prohlížeče počítače, můžete automaticky začít s těmito informacemi tam, kde jste přestali. Pokud jste však nenalezli čas na zálohování některých vašich důležitých fotografií, videí a dalších při ztrátě nebo nefunkčnosti telefonu, tak příště více zálohujte. Po internetu jsou zdarma dostupné zálohy online, a to buď zálohování společnosti Google nebo od jiných provozovatelů. Od Googlu lze zálohování upravit v nastavení, u jiných poskytovatelů k tomu slouží hlavně aplikace, kde je možně si dané funkce přednastavit. Mezi dalšími jsou nejvíce populární nejspíše DropBox a OneDrive, které pomocí aplikace dokážou nabídnout podobné řešení funkcí, ale bohužel množství bezplatného úložného prostoru není tak velké. [47]

6.6 Šifrování citlivých dat

Šifrování se snaží ochraňovat data jejich deformací tak, aby ji mohl zobrazit pouze uživatel pomocí klíče nebo hesla. V tomto případě se jedná o využívání šifrování hlavně citlivých dat v zařízení – např. SD karty. Při každém startu jednotlivého šifrovaného celku v telefonu se vás systém zeptá na heslo, jinak to nebude mít žádný další vliv na používání. V telefonech s OS Android 6.0 a výše je šifrování již součást výchozího OS. U starších modelů může způsobovat zpomalování systému. Ve většině případů je šifrování bohužel jednosměrné, takže nebude moci být dešifrován bez ztráty dat. [47]

6.7 Připojování k neznámým wifi sítím

Používáte často otevřené wifi sítě na veřejných místech? Je třeba pořád myslet na to, že ne každá taková síť je bezpečná. V dnešní době hlavně ve městech můžeme narazit na velké množství wifi sítí. Hodně jich však zabezpečuje heslo. Jsou tu také ale i volně přístupné sítě, které jsou mezi lidmi velice oblíbené kvůli nepoužívání svého datového připojení. Lehce se tak můžete setkat například se sítí, přes kterou někdo sleduje vaši komunikaci, nebo další citlivá data. Jestliže máte jakékoliv podezření, je lepší se takovým sítím nakonec vyhnout.

6.8 Instalace antiviru

Mnoho lidí si v dnešní době myslí, že je mobilní antivirus zbytečný, nebo ho dokonce nepoužívá. Navíc ještě může dost zpomalovat hlavně starší telefony. V každém případě je plně aktualizovaný antivirus dobrým společníkem. V Obchodě Play je spousta možností, které můžou uživatelé využít zcela zdarma. Většinou jsou však součástí reklamy, které mohou působit dost otravně. Za placenou verzi může pořizovatel dostat například prostředí bez reklam, časté aktualizace a maximální podporu. Je třeba nepodceňovat situaci a používat co možná nejvíc typů ochrany, při vzniku nové bezpečnostní hrozby ve společnosti je antivir jedním z prvních, který může situaci zachránit skrze brzkou aktualizaci. Při výběru je dobré se orientovat podle zkušeností uživatelů a počtu jejich stažení.

V neposlední řadě je také rozumné vypínat informace o poloze a také bluetooth. Nejen kvůli šetření baterie, ale také kvůli možnosti napadení útočníkem skrze bluetooth a také kvůli sledování vaší polohy.

ZÁVĚR

Hlavním cílem této práce je poskytnout uživatelům mobilních zařízení přehled současných hrozeb, před kterými se mohou sami aktivně bránit. Tento cíl se naplnil hlavně díky praktické části a také třetí kapitole teoretické části, kdy byly uživatelé seznámeni s malwarem, phishingem, spamem, hrozbami při používání wifi sítí. Přínos této práce pro jejího autora spočívá především v teoretické znalosti přehledu bezpečnostních hrozeb, dále v poznání způsobů a možností testování aplikací běžnými nástroji a v neposlední řadě ve zdokonalování při prevenci proti mobilnímu malwaru a dalším bezpečnostním hrozbám různými způsoby.

První kapitola v teoretické části přináší pohled do historie OS Android a také na změny, které přinesla každá jeho nová verze. Dále se zde čtenáři seznámí s architekturou tohoto OS a základními částmi aplikace. V poslední části kapitoly je vyobrazen graf zastoupení podílu uživatelů v jednotlivých verzích Androidu. Po přečtení této kapitoly by měl čtenář porozumět zásadním proměnám, které u tohoto systému za poslední roky nastaly a co některé tyto změny z hlediska bezpečnosti znamenají. Druhá část se zaměřuje na obchod Google Play. Čtenáři se zde dozví stručně o historii tohoto obchodu, o základních typech aplikací a podmínkách o využívání obchodu. Kapitola pokračuje popisem prostředí a také ukázkou instalace aplikace. Dále se čtenář dozví o službě Google Bouncer a Play Protect, které pomáhají v Obchodě Play kontrolovat aplikace. Následuje poslední podkapitola o oprávněních, která se zaměřuje hlavně na potencionálně nebezpečné oprávnění podle serveru Android developers. Ve třetí kapitole teoretické části je věnována pozornost teorii mobilních hrozeb, zejména malwaru, jeho základních i populárních typů, které se každým rokem rozšiřují po celém světě. Dále čtenáři objeví základní informace o phishingu i spamu. Po přečtení této kapitoly by čtenář měl porozumět jednotlivým druhům malwaru a základním pojmům co to je malware, phishing a spam a také znát aktuální útok KRACK a obecně možnost útoků prostřednictvím používáni wifi sítí.

První kapitola praktické části se jmenuje analýza chování uživatelů při práci s OS Android. Pro tyto účely byla použita kvantitativní analýza prostřednictvím internetového dotazníkového formuláře na stránkách vyplnto.cz. V dotazníkovém šetření byly zodpovězeny všechny cíle. Co se týče verifikace hypotéz, podařilo se potvrdit 5 z celkových 6. Jedinou nepotvrzenou hypotézou zůstává otázka, co je to phishing. Správnou odpověď nevědělo požadovaných 90 % lidí, avšak 83 % lidí tuto skutečnost

vědělo, což znamená, že většina lidí tento typ útoku zná. Druhá kapitola v první části ukazuje analýzu vybraných typů aplikací z Obchodu Play za pomoci různých výzkumů z tématem malwaru v jednotlivých typech aplikací. Druhá část této kapitoly ukazuje běžným uživatelům, jak mohou každodenně testovat různé aplikace dostupnými nástroji a vyhýbat se tak nebezpečnému škodlivému kódu. Zároveň umožňuje nahlédnout do možného kriteriálního hodnocení jednotlivých testovaných aplikací. Třetí kapitola praktické části pojednává o možné prevenci proti různým útokům cíleným na zařízení s OS Android. Různá prevence představená v této práci vychází hlavně ze zkušeností samotných uživatelů.

SEZNAM POUŽITÉ LITERATURY

[1] UJBÁNYAI, Miroslav. Programujeme pro Android. Praha: Grada, 2012. Průvodce (Grada). ISBN 978-80-247-3995-3

[2] Android History. *The Verge* [online]. 2011 [cit. 2018-05-16]. Dostupné z: https://www.theverge.com/2011/12/7/2585779/android-history

[3] Android Cup Cake subjektivně. *Svět Androida* [online]. 2009 [cit. 2018-05-16]. Dostupné z: https://www.svetandroida.cz/android-cupcake-15-subjektivne/

[4] Android version comparison. *socialcompare* [online]. 2018 [cit. 2018-05-16]. [cit. 2018-05-19] Dostupné z: http://socialcompare.com/en/comparison/android-versions-comparison

[5] Google Android Donut: mnohá vylepšení, multitouch však nečekejte. *MobilMania.cz – O mobilech víme vše*[online]. 2010 [cit. 2018-05-19] Dostupné z: https://www.mobilmania.cz/bleskovky/google-android-donut-mnoha-vylepseni-multitouch-vsak-necekejte/sc-4-a-1122983/default.aspx

[6] KŮŽEL, Filip. Android 2.2 Froyo udělá z vašeho mobilu Wi-Fi hotspot In: *MobilMania* [online]. 2010 [cit. 2018-05-19]. Dostupné z: https://www.mobilmania.cz/bleskovky/android-22-froyo-udela-z-vaseho-mobilu-wi-fi-hotspot/sc-4-a-1125314/default.aspx

[7] PŘIBYL, Lukáš. Android 2.3 Gingerbread: přehled novinek a displejů In: *MobilMania.cz* [online]. 2010 [cit. 2018-05-19]. Dostupné z: https://www.mobilmania.cz/clanky/android-23-gingerbread-prehled-novinek-a-displeju/sc-3-a-1315128/default.aspx

[8] VÁCLAVÍK, Lukáš. Ice Cream Sandwich Vše co jste chtěli vědět. In: *Cnews* [online]. 2011 [cit. 2018-05-19]. Dostupné z: https://www.cnews.cz/android-4-0-ice-cream-sandwich-vse-co-jste-chteli-vedet

[9] Jelly Beam 4.3. In: *Android* [online]. [cit. 2018-05-19]. Dostupné z: https://www.android.com/versions/jelly-bean-4-3/

[10] Kitkat 4.4. In: *Android* [online]. [cit. 2018-05-19]. Dostupné z: https://www.android.com/versions/kit-kat-4-4/

[11] Lollipop 5.0. In: *Android* [online]. [cit. 2018-05-19]. Dostupné z: https://www.android.com/versions/lollipop-5-0/

[12] Marchmallow 6.0. In: *Android* [online]. [cit. 2018-05-19]. Dostupné z: https://www.android.com/versions/marshmallow-6-0/

[13] Nougat 7.0. In: *Android* [online]. [cit. 2018-05-19]. Dostupné z: https://www.android.com/versions/nougat-7-0/

[14] Oreo 8.0. In: *Android* [online]. [cit. 2018-05-19]. Dostupné z: https://www.android.com/versions/oreo-8-0/

[15] BURIAN, Pavel. *Internet inteligentních aktivit*. Praha: Grada, 2014. Průvodce (Grada). ISBN 978-80-247-5137-5.

[16] Activity. In: *Android developers* [online]. [cit. 2018-05-19]. Dostupné z: https://developer.android.com/reference/android/app/Activity

[17] SZYDLOWSKÁ, Markéta. *Bezpečnost OS Android*. Brno, 2012. Bakalářská práce. Masarykova Univerzita.

[18] Permissions. In: *Android developers* [online]. [cit. 2018-05-19]. Dostupné z: https://developer.android.com/guide/topics/permissions/requesting.html

[19] Distribution Dashboard. In: *Android developers* [online]. 2018, [cit. 2018-05-19]. Dostupné z: https://developer.android.com/about/dashboards/index.html#Screens

[20] Play terms. In: *Google Play* [online]. [cit. 2018-05-19]. Dostupné z: https://play.google.com/intl/en_us/about/play-terms.html

[21] Google using custom malware scanner for Android apps. In: *SGMagazine* [online]. 2. prosince 2012 [cit. 2018-05-19]. Dostupné z: https://www.scmagazine.com/google-using-custom-malware-scanner-for-android-apps/article/541605/

[22] Počítačové viry, červy, trojské koně. In: *Internetem bezpečně* [online]. [cit. 2018-05-19]. Dostupné z: http://www.internetembezpecne.cz/internetem-bezpecne/malware/virus/

[23] Co je to rootkit. In: *AVG* [online]. [cit. 2018-05-19]. Dostupné z: https://support.avg.com/SupportArticleView?l=cs&urlname=What-is-rootkit

[24] Co je to exploit?. In: *Správa sítě* [online]. [cit. 2018-05-19]. Dostupné z: https://www.sprava-site.eu/exploit/

[25] TRLICA, David. Malware BankBot útočil na aplikace. Terčem byly i české banky. In: *Svět Androida* [online]. [cit. 2018-05-19]. Dostupné z: https://www.svetandroida.cz/mobilni-trojan-bankbot-android-banky/

[26] Malware infekce stále častěji míří na klienty bank. In: *Bussiness world* [online]. [cit. 2018-05-19]. Dostupné z: http://businessworld.cz/novinky/malware-infekce-stale-casteji-miri-na-klienty-bank-12254

[27] Android Mobile Security Threats. In: *Kaspersky* [online]. [cit. 2018-05-19]. Dostupné z: https://www.kaspersky.com/resource-center/threats/mobile

[28] Mobile ransomware more than trebled in Q1 2017. In: *Kaspersky* [online]. [cit. 2018-05-19]. Dostupné z: https://www.kaspersky.com/about/press-releases/2017_mobile-ransomware-more-than-trebled-in-q1-2017

[29] Co je to spyware?. In: *Avast* [online]. [cit. 2018-05-19]. Dostupné z: https://www.avast.com/cs-cz/c-spyware

[30] ZACHAR, Martin. Co je to: Adware, Spyware, ... In: *Stahuj.cz* [online]. 2009 [cit. 2018-05-19]. Dostupné z: http://magazin.stahuj.centrum.cz/co-je-to-adware-spyware-/

[31] MACHO, Daniel. Malware Hummingbad nakazil desítky milionů Android zařízení. Kde se ale vzal?. In: *Svět Androida* [online]. 2016 [cit. 2018-05-19]. Dostupné z: https://www.svetandroida.cz/malware-hummingbad-201607/

[32] Sms trojan. In: *Malware bytes* [online]. 2016 [cit. 2018-05-19]. Dostupné z: https://blog.malwarebytes.com/threats/sms-trojan/

[33] Spam. In: *Bezpečný internet* [online]. [cit. 2018-05-19]. Dostupné z: http://www.bezpecnyinternet.cz/zacatecnik/e-mail/spam.aspx

[34] Co je to phishing?. In: *Hoax* [online]. [cit. 2018-05-19]. Dostupné z: http://www.hoax.cz/phishing/co-je-to-phishing

[35] Výhody a nevýhody VPN – vše, co potřebujete vědět. In: *VpnMentor* [online]. [cit. 2018-05-19]. Dostupné z: https://cs.vpnmentor.com/blog/vyhody-nevyhody-vpn-vse-co-potrebujete-vedet/

[36] FILINGER, Zbyněk. Veřejná Wi-Fi je nebezpečná Wi-Fi. Potřebujete VPN. In: *Svět Androida* [online]. 2016 [cit. 2018-05-19]. Dostupné z: https://www.svetandroida.cz/verejna-wi-fi-vpn-201602/

[37] KRACK - ZRANITELNOST PROTOKOLU WPA2 UMOŽŇUJE ČTENÍ ŠIFROVANÝCH DAT. In: *Národní úřad pro kybernetickou a informační bezpečnost*[online]. 2017 [cit. 2018-05-19]. Dostupné z:

https://www.govcert.cz/cs/informacni-servis/hrozby/2557-krack-zranitelnost-protokolu-wpa2-umoznuje-cteni-sifrovanych-dat/

[38] TRLICA, David. Závažná chyba u Wi-Fi ohrožuje telefony i počítače. Jak je na tom Android?. In: *Svět Androida* [online]. 2017 [cit. 2018-05-19]. Dostupné z: https://www.svetandroida.cz/chyba-u-wi-fi-ohrozuje-telefony-pocitace-201710/#comments

[39] Malicious Flashlight Apps on Google Play. In: *Checkpoint* [online]. 2018 [cit. 2018-05-19]. Dostupné z: https://research.checkpoint.com/malicious-flashlight-apps-google-play/

[40] IKRAM, Muhammad, Narseo VALLINA-RODRIGUEZ, Suranga SENEVIRATNE, Mohamed ALI KAAFAR a Vern PAXSON. An Analysis of the Privacy and Security Risks of Android VPN Permission-enabled Apps. In: *SCIRO* [online]. 2017 [cit. 2018-05-19]. Dostupné z: https://research.csiro.au/ng/wp-content/uploads/sites/106/2016/08/paper-1.pdf

[41] STEFANKO, Lukas. Beware ad slingers thinly disguised as security apps. In: *We live security* [online]. 2018 [cit. 2018-05-19]. Dostupné z: https://www.welivesecurity.com/2018/04/05/google-play-ad-slingers/

[42] CASSTILO, Carlos. Fake Cleaning Apps in Google Play: an AutoRun Attack and More. In: *Securing tomorrow McAfee* [online]. 2013 [cit. 2018-05-19]. Dostupné z: https://securingtomorrow.mcafee.com/mcafee-labs/fake-cleaning-apps-in-google-play-an-autorun-attack-and-more/

[43] KORIAT, Oren. A Whale of a Tale: HummingBad Returns. In: *Checkpoint* [online]. 2017 [cit. 2018-05-19]. Dostupné z: https://blog.checkpoint.com/2017/01/23/hummingbad-returns/

[44] KORIAT, Oren, Andrey POLKOVNICHENKO a Bogdan MELNYKOV. FalseGuide misleads users on GooglePlay. In: *Checkpoint* [online]. 2017 [cit. 2018-05-19]. Dostupné z: https://blog.checkpoint.com/2017/04/24/falaseguide-misleads-users-googleplay/

[45] Crooks infiltrate Google Play with malware in QR reading utilities. In: *Sophos* [online]. 2018 [cit. 2018-05-19]. Dostupné z: https://nakedsecurity.sophos.com/2018/03/23/crooks-infiltrate-google-play-with-malware-lurking-in-qr-reading-utilities/

[46] Number of available applications in the Google Play Store from December 2009 to December 2017. In: *Statista* [online]. [cit. 2018-05-19]. Dostupné z: https://www.statista.com/statistics/266210/number-of-available-applications-in-the-google-play-store/

[47] TRIGGS, Robert. Best Android security practices. In: *Android authority* [online]. 2016 [cit. 2018-05-19]. Dostupné z: https://www.androidauthority.com/best-android-security-practices-700393/

[48] JIŘÍKOVÁ, Lucie. OD ANDROID MARKETU AŽ PO GOOGLE PLAY – POHLED DO HISTORIE NEJVĚTŠÍHO ONLINE OBCHODU S APLIKACEMI PRO ANDROID. In: *Androidtip* [online]. 2014 [cit. 2018-05-19]. Dostupné z: http://www.androidtip.cz/android-marketu-az-google-play-pohled-historie-nejvetsiho-online-obchodu-aplikacemi-android/

[49] Google Android. In: *CVEdetails* [online]. 2018 [cit. 2018-05-19]. Dostupné z: https://www.cvedetails.com/product/19997/Google-Android.html?vendor_id=1224

[50] Google Chrome. In: *CVEdetails* [online]. 2018 [cit. 2018-05-19]. Dostupné z: https://www.cvedetails.com/product/15031/Google-Chrome.html?vendor_id=1224

SEZNAM POUŽITÝCH SYMBOLŮ A ZKRATEK

API	Application programming interface
ČSOB	Československá obchodní banka
IEEE	Institute of Electrical and Electronics Engineers
MB	Megabyte
OpenGL/ES	Open graphics libraly for embedded systems
OS	Operační systém
RAM	Random access memory
SDK	Software development kit
SD karta	Externí paměťová karta
SGL	Scalable graphics libraly
SMS	Short message service
SSL	Secure sockets layer
USB	Universal serial bus
VPN	Virtual private network
WIFI	Wireless Fidelity
WPA	Wifi protected access

SEZNAM OBRÁZKŮ

SEZNAM TABULEK

..

SEZNAM PŘÍLOH

PŘÍLOHA P I: OBSAH DISKU CD

:\fulltext.pdf	Plný text bakalářské práce
:\analyza-chovani-uzivatelu_1-100.pdf	Dotazník odpovědi respondentů 1 až 100
:\analyza-chovani-uzivatelu_101-175.pdf	Dotazník odpovědi respondentů 101 až 175
:\analyza-chovani-uzivatelu.xlsx	Surová data z dotazníku v tabulce