Univerzita Tomáše Bati ve Zlíně
Fakulta aplikované informatiky

Zabezpečení mobilního operačního systému

Matúš Gavenda

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:	**Matúš Gavenda**
Osobní číslo:	**A14089**
Studijní program:	**B3902 Inženýrská informatika**
Studijní obor:	**Informační a řídicí technologie**
Forma studia:	**prezenční**
Téma práce:	**Zabezpečení mobilního operačního systému**
Téma anglicky:	**Securing a Mobile Operating System**

Zásady pro vypracování:

1. **Proveďte literární rešerši v oblasti zabezpečení mobilních operačních systémů.**
2. **Definujte nejčastější hrozby současnosti z Internetu.**
3. **Uveďte možnosti standardního zabezpečení v současnosti nejpoužívanějších mobilních operačních systémů.**
4. **Navrhněte další aplikace k doplnění zabezpečení mobilních operačních systémů.**
5. **Ověřte navržené zabezpečení, porovnejte výkon zařízení a výsledky zhodnoťte.**

Rozsah bakalářské práce:

Rozsah příloh:

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

Seznam odborné literatury:

1. **LACKO, L'uboslav. Mistrovství Android. Brno: Computer Press, 2017, 647 s. ISBN 978-80-251-4875-4.**
2. **HERODEK, Martin. 333 tipů a triků pro Android: [sbírka nejužitečnějších postupů a řešení]. Brno: Computer Press, 2014, 205 s. ISBN 978-80-251-4310-0.**
3. **LACKO, L'uboslav. 333 tipů a triků pro iPhone, iPad, iPod. Brno: Computer Press, 2014, 248 s. ISBN 978-80-251-3781-9.**
4. **KOŽÍŠEK, Martin a Václav PÍSECKÝ. Bezpečně n@ internetu: průvodce chováním ve světě online. Praha: Grada Publishing, 2016, 175 s. ISBN 978-80-247-5595-3.**
5. **NOLAN, Godfrey. Bulletproof Android: practical advice for building secure apps. Upper Saddle River: Addison-Wesley, 2015, xix, 207. ISBN 978-0-13-399332-5.**

Vedoucí bakalářské práce: **doc. Ing. Jiří Vojtěšek, Ph.D.**
Ústav řízení procesů

Datum zadání bakalářské práce: **15. prosince 2017**

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

Ve Zlíně dne 15. prosince 2017

doc. Mgr. Milan Adámek, Ph.D.
děkan

L.S.

UNIVERZITA TOMÁŠE BATI VE ZLÍNĚ
Fakulta aplikované informatiky

prof. Ing. Vladimír Vašek, CSc.
ředitel ústavu

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 18.5.2021

Gavenda
.....
podpis diplomanta

ABSTRAKT

Cieľom tejto bakalárskej práce je zoznámiť čitateľa s možnosťami zabezpečenia mobilného operačného systému. Riešenie zahrňuje rady ako sa brániť proti hrozbám z internetu, odporúčané nastavenia a aplikácie pre operačný systém Android 6.0 Marshmallow, ukážka vlastného navrhnutého zabezpečenia, jeho overenie a otestovanie ako navrhnuté zabezpečenie vplýva na výkon a výdrž zariadenia.

Úlohou teoretickej časti je oboznámenie čitateľa s najčastejšími hrozbami z internetu a poukázať na najpoužívanejšie operačné systémy v súčasnosti, pre mobilné zariadenia.

Praktická časť je mierená na rady pre ochranu mobilného operačného systému pred hrozbami. Tiež sú tu popísané štandardné nastavenia zariadenia pre zabezpečenie, návrh vlastného zabezpečenia pomocou aplikácií a následné testovanie výkonu a výdrže zariadenia.

Kľúčové slová: Android, iOS, mobilný operačný systém, Google, mobilný telefón, tablet, smartfón, škodlivý softvér, bezpečnosť

ABSTRACT

The aim of this bachelor's thesis is to acquaint the reader with the security features of the mobile operating system. The solution includes advice on how to defend against threats from the Internet, recommended settings and applications for the operating system Android 6.0 Marshmallow, demonstration of my own proposed security, its verification and testing as the proposed security affects the performance and durability of the device.

The role of the theoretical part is to familiarize the reader with the most common threats from the Internet and point to today´s most used operating systems for mobile devices.

The practical part is based on tips for protecting the mobile operating system from threats. There are also described standard equipment settings for securing, designing custom security using applications and subsequent testing performance and durability of the device.

Keywords: Android, iOS, mobile operating system, Google, mobile phone, tablet, smartphone, malicious software, security

Ďakujem doc. Ing. Jiřímu Vojtěškovi, Ph.D., vedúcemu bakalárskej práce, za podporu, cenné nápady a trpezlivosť. Poďakovanie patrí aj mojej rodine, ktorá ma podporovala po celú dobu štúdia a ich podpora pre mňa veľa znamená.

Prehlasujem, že odovzdaná verzia bakalárskej práce a verzia elektronická nahraná do IS/STAG sú totožné.

OBSAH

ÚVOD

Drvivá väčšina ľudí, si už nedokáže predstaviť svoj život bez smartfónu a pripojenia na internet. Používame ho na skrátenie čakania pri cestovaní, rozhovory s rodinou alebo kamarátmi, zachytenie a zdieľanie momentov v živote, a mnoho ďalšieho.

S nástupom čoraz modernejších a výkonnejších mobilných zariadení poskytujúcich tieto možnosti, narastá aj dôvod dbať na dostatočné zabezpečenie mobilného zariadenia. V dnešnej dobe mobilné zariadenia uchovávajú veľké množstvo osobných informácií majiteľa. Informácie ako napríklad telefónne kontakty, história komunikácie, či už ide o hlasovú komunikáciu, SMS, MMS, emaily, rôzne prihlasovacie údaje, bankové údaje, poloha užívateľa. Práve preto chcem v tejto práci poukázať a informovať o možnostiach uchovania svojich citlivých údajov proti potenciálnemu zneužitiu v súvislosti s hrozbami.

Teoretická časť práce sa skladá z dvoch kapitol. Prvá kapitola sa zaoberá najčastejšími hrozbami z internetu, s ktorými sa môže používateľ stretnúť pri bežnom používaní mobilného zariadenia. Druhá kapitola práce je venovaná najpoužívanejším operačným systémom určeným pre mobilné zariadenia, ich stručným popisom, vlastnostiam a stručnou históriou (Android, iOS).

Praktická časti práce sa venuje kapitola 3,4 a 5. Tretia kapitola je určená tipom ako sa brániť proti najčastejším hrozbám z internetu. V štvrtej kapitole sú popísané a ukázané príklady štandardného zabezpečenia mobilného operačného systému (Android 6.0 Marshmallow). Posledná kapitola práce je venovaná testovaniu navrhnutého zabezpečenia pomocou aplikácií slúžiacich pre zabezpečenie a následné testovanie, ako tieto aplikácie vplývajú na výkon a výdrž vybraného zariadenia.

I. TEORETICKÁ ČASŤ

1 NAJČASTEJŠIE HROZBY SÚČASNOSTI Z INTERNETU

V súčasnej dobe je pojem bezpečnosť na internete veľmi široký a zároveň zohráva dôležitú úlohu. Množstvo užívateľov, stretávajúcich sa denne s internetovými hrozbami, ktoré na nich pôsobia, je čoraz viac.

Výsledný efekt útoku sa v lepšom prípade môže prejaviť v podobe drobných nepríjemností spôsobených bežným užívateľom, ako napríklad krátkodobé výpadky webových stránok. V horšom prípade môže dochádzať k veľkým finančným stratám, stratám osobných údajov alebo životne dôležitých funkcií zariadenia.

Hrozba je označenie pod ktorým môžeme chápať čokoľvek, čo môže nejakým spôsobom viesť k nežiadúcej zmene chovania systému, ovplyvňovaniu jeho parametrov alebo zmene informácií. Môžeme sem zahrnúť všetky osoby, prostriedky, udalosti ale aj myšlienky, ktoré predstavujú potenciálne narušenie integrity, dôvernosti, dostupnosti alebo legálnosti použitia.

Ochranou rozumieme všetky fyzické mechanizmy, procesy alebo definované politiky, ktoré majú slúžiť k ochrane systému alebo majetku všeobecne pred hrozbou alebo útokom. Každá z ochrán sa však vyznačuje svojou zraniteľnosťou. Sú to väčšinou slabé miesta ochrany alebo jej úplná absencia.

Pravdepodobnosť úspešného útoku dokážeme znížiť lepšou ochranou systému. V dnešnej dobe už nie sú ohrozené iba mobilné telefóny a počítače, ale všetky zariadenia s pripojením na internet. [1] [2]

1.1 Vírusy

Názov vírus je odvodený od istých podobností s biologickým originálom. Je schopný sebareplikácie, čo znamená, že dokáže sám seba množiť za prítomnosti vykonateľného hostiteľa ku ktorému je vírus pripojený bez jeho vedomia. Jediným spôsobom, ako sa dokáže vírus dostať do systému, je spustenie infikovaného programu. Vírus sa postupne rozširuje tak, že po spustení infikovaného programu sa aktivuje v operačnej pamäti systému a začne napadať a infikovať ďalšie súbory v tomto systéme. Vírusy často napadajú systémové súbory operačného systému, vďaka čomu dochádza k spomaleniu výkonu zariadenia, jeho zamŕzaniu alebo dokonca k celkovému znefunkčneniu zariadenia. Dokážu mazať súbory a adresáre, meniť obsah súborov, šifrovať dáta, prípadne poškodzovať hardware zariadenia. [1] [3]

1.2 Trójske kone (Trojany)

Trójsky kôň je druh škodlivého kódu, ktorý sa pripája k zdanlivo neškodnému a legitímnemu programu alebo aplikácii. Na rozdiel od vírusov nie je Trojan schopný infikovať súbory a seba-replikovať sa. Akonáhle je program alebo aplikácia nainštalovaný, Trojan sa aktivuje a infikuje zariadenie. Vlastníci týchto škodlivých kódov môžu následne zachytiť citlivé informácie, ako napríklad údaje o prihlásení na bankové účty alebo údaje o kreditných kartách. Taktiež môžu zablokovať prehliadač, čo má za následok, že zariadenie odosiela informácie s vysokou prioritou bez oprávnenia užívateľa. Môže tiež deaktivovať aplikácie alebo úplne paralyzovať zariadenie.

Najznámejšie „Trojany“ na mobilné zariadenia sú The Skulls a Hummer. [4]

1.2.1 The Skulls

The Skulls je druh trójskeho koňa, ktorý sa pokúša prepísať súbory a urobiť ich nepoužiteľnými. Jedná sa o jeden z trójskych koní, ktorý je určený pre SymbOS. Šíry sa prostredníctvom Bluetooth. Ak je nainštalovaný, zakáže všetky vstavané aplikácie na zariadení a nahrádza ich ikonu obrázkom lebky v menu (okrem volania zo zariadenia a prijímania hovorov).

Pre jeho úplné odstránenie je jedinou možnosťou vrátiť zariadenie späť do výrobných nastavení. [5]

1.2.2 Hummer

Hummer je trójsky kôň bežiaci v operačnom systéme Android. Tento škodlivý kód je spustený inštaláciou infikovaných aplikácií, najčastejšie cez obchod Google Play. Keď je zariadenie nakazené, Hummer sa prepne do používateľa ROOT, čím získa všetky privilégia. Znamená to, že získa plný prístup do zariadenia a môže vymazávať a prepisovať ľubovoľné súbory. Následne vloží do zariadenia pop–up reklamy (vyskakovacie reklamy) a začne na pozadí sťahovať a inštalovať nechcené aplikácie a hry. Ak sa ich používateľ pokúsi odstrániť, nainštalujú sa znova.

Škodlivý kód sa dá odstrániť pomocou antivírusových aplikácií, ktoré majú tento kód zahrnutý vo svojej databáze. [6]

1.3 Spyware

Spyware je softvér skrývajúci sa v zariadení bez vedomia a súhlasu používateľa. Využíva sa pre zbieranie informácii o zariadení (hardvéri a softvéri) a jeho užívateľovi, o navštevovaných stránkach, heslách, e-mailových adresách a osobných údajoch – meno, vek, adresa, atď...

Iné druhy spywaru robia zmeny v používateľskom zariadení, ktoré sú nepríjemné a môžu mať za následok spomalenie alebo zničenie zariadenia. Tieto programy môžu zmeniť domovskú stránku alebo stránku vyhľadávania webového prehliadača, alebo pridať do prehliadača ďalšie komponenty, ktoré sú pre používateľa nepotrebné. Taktiež sťažujú zmenu ich nastavení na pôvodný stav. Keďže spyware používa pamäťové a systémové zdroje, aplikácie spustené na pozadí môžu spôsobovať systémové nehody alebo nestabilitu systému.

Pretože je spyware samostatne spustiteľný program, má možnosť sledovať stlačenie kláves, skenovať súbory v pamäti, sledovať iné aplikácie, ako napríklad chatové programy alebo textové procesy, inštalovať ďalší spyware, čítať súbory cookies a preniesť tieto informácie späť autorovi/vlastníkovi spywaru, ktorý ich buď požije na reklamné/marketingové účely, alebo predá inej strane.

Licenčné zmluvy, ktoré sprevádzajú prevzatie softvéru, niekedy varujú používateľa, že bude nainštalovaný Spywarový program spolu s požadovaným softvérom.

Často je spojený so softvérom, ktorý zobrazuje reklamy alebo ktorý sleduje osobné, alebo citlivé informácie nazývaný Adware. [1] [3] [7] [8]

1.4 Adware

Pod pojmom Adware sa skrýva legitímny program, ktorý je určený na zobrazovanie reklám koncovým používateľom, často založený na sledovaní prehliadania výmenou za právo používania programu bezplatne. Niektoré typy Adware môžu obsahovať aj spyware a môžu byť klasifikované ako softvér porušujúci ochranu súkromia. Adware svojou činnosťou môže spomaliť RAM a CPU zariadenia alebo internetové pripojenie používateľa využitím šírky pásma na získanie reklám. [1] [3]

1.5 Phishing

Phishing je proces podvodného pokusu o získanie citlivých informácií ako sú používateľské mená, heslá a údaje o kreditných kartách, ktorý sa maskuje ako dôveryhodný subjekt v elektronickej komunikácii. Na rozdiel od mnoho iných typov hackovania, dokáže Phishing okamžite zistiť heslo bez ohľadu na jeho silu a to tak, že užívateľ nemusí ani poznať rozdiel (napr. stránka banky) a sám vyplní predvolené políčka, kde sú po ňom požadované dôverné informácie. Pri každej takejto správe je treba zvýšiť pozornosť, pretože banky nikdy nevyžadujú podobné zadávanie údajov cez e-mail. [1] [2]

1.6 Ransomware

Ransomware, tiež známy pod pojmami ako crypto virus, crypto trojan, locky virus, encryption virus alebo cryptoworm, je typ škodlivej aplikácie, ktorý zamedzí užívateľovi prístup k dokumentom, obrázkom a ďalším dátam tým, že ich zašifruje. Následne je vyžadovaný dešifrovací kľúč, ktorý „bude“ poslaný užívateľovi po zaslaní požadovanej finančnej čiastky. Akonáhle je čiastka zaplatená, vlastník Ransomware môže (ale nemusí) dešifrovací kľúč poslať.

Zariadenie môže byť nakazené spustením zavírenej prílohy v maile, prostredníctvom webového prehliadača alebo náhodnou návštevou webovej stránky infikovanej týmto škodlivým softvérom.

Väčšina dnešných antivírusov obsahuje nástroj na odstránenie Ransomware, ktorý automaticky testuje a odstráni väčšinu pokusov na preniknutie do zariadenia. [9]

1.7 Červ (Worm)

Červ je druh škodlivého programu, ktorý sa duplikuje z jedného adresára, jednotky, zariadenia alebo siete do iného. Väčšina červov sa posiela e-mailom a mnohí majú funkciu, ktorá im umožňuje posielať sa na každú adresu v konkrétnej poštovej schránke. Ďalšia populárna metóda prenosu červov je prostredníctvom lokálnych sietí.

Na rozdiel od vírusu je červ vlastným programom a nemusí sa pripájať k spustiteľným súborom, hoci niektoré druhy majú vlastnú zložku, ktorá infikuje súbory. Keďže sú spustiteľnými programami, môžu sa nakaziť a všetci „potomkovia“ tejto kópie červa môžu byť infikovaní, a majú schopnosť infikovať súbory na iných zariadeniach po ich spustení. [1] [3]

2 NAJPOUŽÍVANEJŠIE OPERAČNÉ SYSTÉMY PRE MOBILY A TABLETY

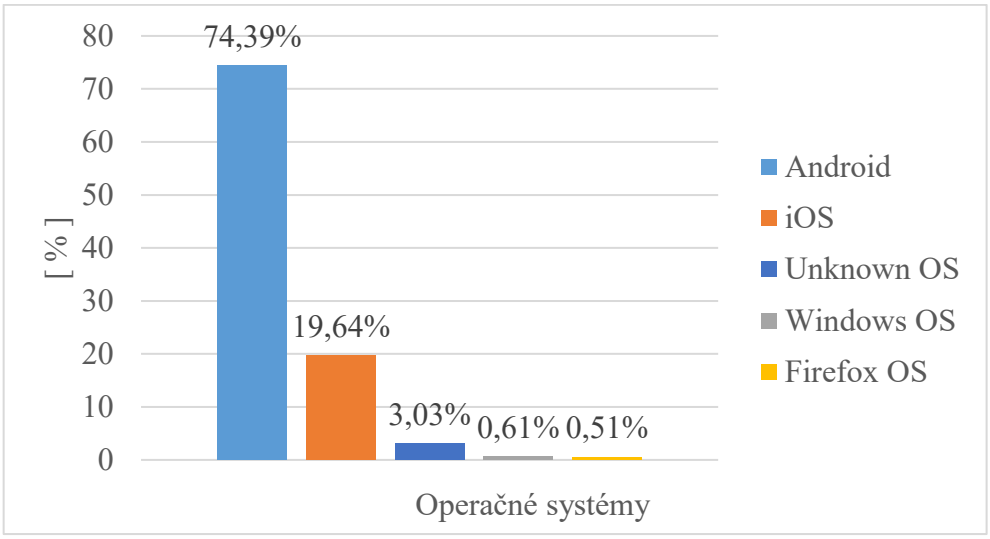
Operačný systém (OS) je základný systémový softvér spravujúci hardvérové a softvérové zdroje zariadenia, a poskytujúci služby programom spusteným na danom operačným systéme. Pri hardvérových funkciách, ako sú napríklad vstupy/výstupy a prideľovanie pamäte, slúži operačný systém ako sprostredkovateľ medzi programami a hardvérom zariadenia. Operačný systém tiež vykonáva úlohy ako je napríklad správa pamäte, jej kontrola a pridelenie programom. Prideľuje prioritu systémovým úlohám, kontroluje vstupné/výstupné zariadenia, spravuje súbory a mnoho ďalšieho. V súčasnosti, takmer všetky zariadenia, obsahujúce integrované obvody, majú svoj vlastný operačný systém. [10] [11]

Medzi najznámejšie operačné systémy pre mobilné zariadenia a tablety patrí: Android OS, iOS, BlackBerry OS, Windows OS.

2.1 Operačné systémy pre mobily a tablety

Na Obrázku 1 jasne vidíme takmer štvornásobnú prevahu operačného systému Android. Na druhom mieste sú so značnou stratou mobilné telefóny s operačným systémom iOS. Tretie miesto obsadili Unknown operačné systémy. Na štvrtom a piatom mieste sa umiestnili operačné systémy Windows a Firefox OS s veľmi malou hodnotou predaja. Ďalej sa nachádzajú ostatné operačné systémy, ktoré kvôli nízkemu používaniu neuvádzam.

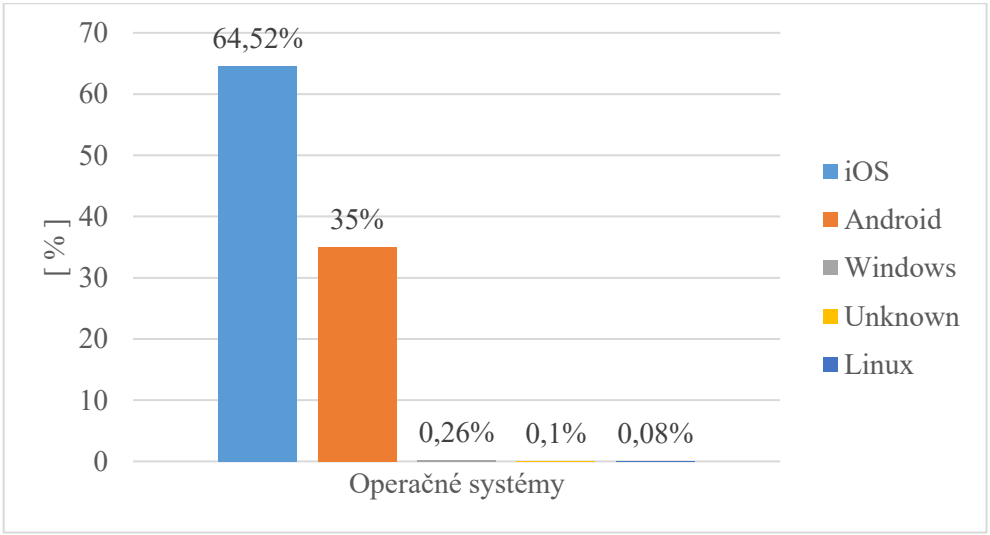
Pri Unknown OS sa predpokladá, že sa jedná z veľkej časti o lacné čínske mobilné telefóny, ktoré bežia na operačnom systéme založenom na programovacom jazyku Java. Tieto zariadenia nie sú také obmedzené ako funkčné mobilné telefóny, ale neponúkajú skutočný zážitok zo smartfónu. Nízka cena týchto mobilných telefónov ich robí populárnymi medzi používateľmi.



Obrázok 1 Podiel na trhu celosvetovo k januáru 2018 pre mobilné telefóny podľa webu Statcounter [19]

Na Obrázku 2 vidíme prevahu operačného systému iOS pre tablety. Na druhom mieste sa umiestnili tablety s operačným systémom Android a na ďalších miestach sa nachádzajú operačné systémy Windows, Unknown OS a Linux. Taktiež, ako pri mobilných operačných systémoch, sa aj tu nachádzajú ďalšie systémy, ale kvôli nízkemu používaniu ich neuvádzam.

Vzhľadom k nízkemu výskytu operačných systémov ako sú Unknown OS, Windows, Linux a Firefox, sa v tejto časti práce zameriam na systémy Android a iOS.



Obrázok 2 Podiel na trhu celosvetovo k januáru 2018 pre tablety podľa webu Statcounter [20]

2.2 Android

Android je softvér pre mobilné telefóny, tablety a škálu zariadení, zahrňujúcich všetko od prenosných počítačov po hodinky. Bol spustený v roku 2003 a podľa väčšiny zahraničných webov sa stal jedným z najobľúbenejších operačných systémov na svete. [12]

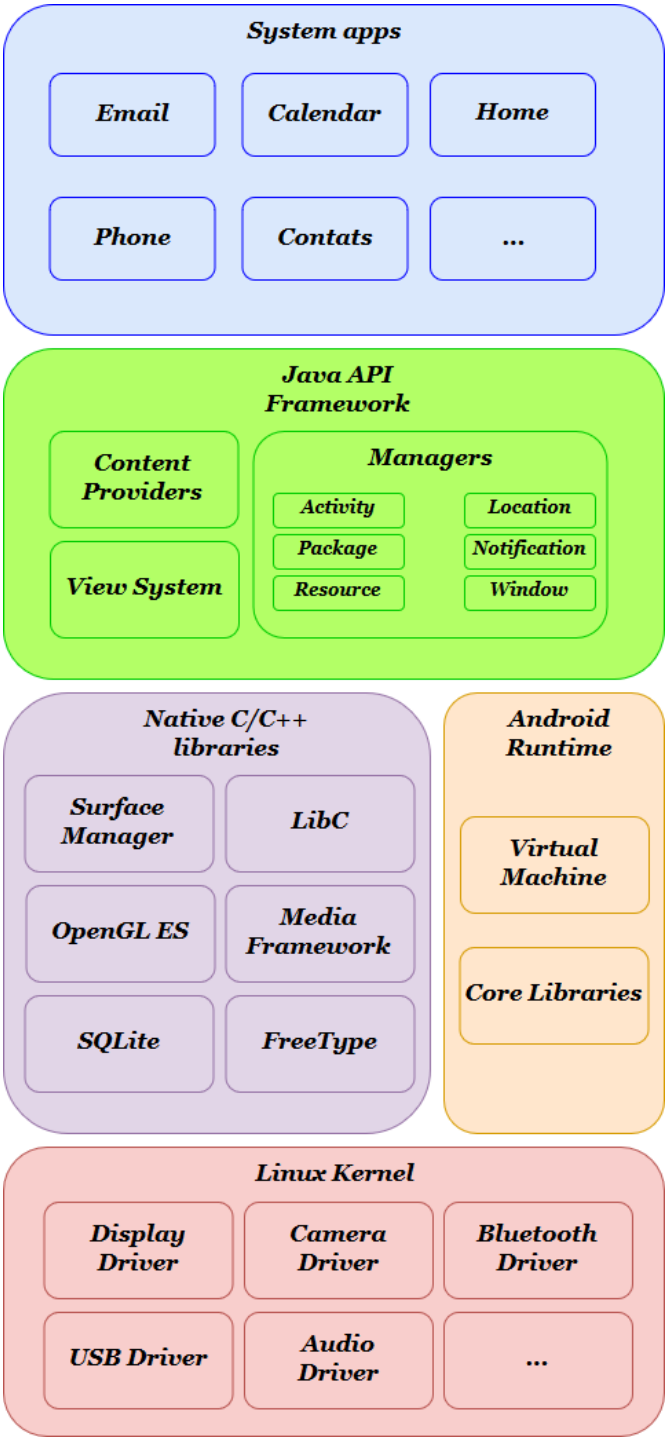
Android je open source platforma vedená spoločnosťou Google s názvom AOSP (Android Open Source Project). Spoločnosť Google používa tento projekt ako základ na vytvorenie svojej verzie systému Android, ktorú potom používajú ostatní výrobcovia zariadení. [13]

2.2.1 História operačného systému Android

Operačný systém Android sa prvýkrát dostal do pozornosti verejnosti v roku 2005, keď spoločnosť Google odkúpila spoločnosť Android, Inc. V tejto dobe ale ešte nebolo veľmi známe, čo konkrétne so spoločnosťou zamýšľa. Informácie sa dostali na verejnosť až v roku 2007, kedy spoločnosť Google oznámila prvú skutočne otvorenú platformu pre mobilné zariadenia na svete. [12]

2.2.2 Architektúra operačného systému Android

Operačný systém Android sa skladá z nasledujúcich vrstiev, znázornených na diagrame.



Obrázok 3 Architektúra operačného systému Android [21]

Linux kernel

Linux jadro, umiestnené v spodnej časti softvérového zásobníka Android, poskytuje úroveň abstrakcie medzi hardvérom zariadenia a hornými vrstvami softvérového balíka Android. Založené na verzii systému Linux 2.6 poskytuje jadro systému Android služby ako sú napríklad správa napájania, správa pamäte a ovládače zariadení. [14] [15] [16]

Hardware Abstraction Layer (HAL)

HAL, alebo hardvérová abstrakčná vrstva, je špeciálne navrhnutá pre dodávateľov. Táto vrstva pomáha vložiť funkcie do systému bez toho, aby došlo k akýmkoľvek jeho úpravám. Každý operačný systém má inak navrhnutú HAL, pretože sú špecifické pre každé zariadenia. HAL sa skladá z dvoch typických štruktúr: modul a zariadenie.

Štruktúra modulov v HAL sa ukladá ako zdieľaná knižnica vo formáte .so, ktorá pozostáva zo základných metadát, ako je číslo verzie, autor, ktorý navrhol modul a podobne, zatiaľ čo štruktúra zariadenia je skutočný hardvér produktu. [14] [15] [16]

Android Runtime

Od zariadenia so systémom Android verzie 5.0 alebo vyššej, každá aplikácia beží vo svojom vlastnom procese a má vlastnú inštanciu Android Runtime (ART). Android Runtime vytvára prostredie pre spustenie viacerých virtuálnych strojov na zariadeniach s nízkou pamäťou pomocou súborov DEX. DEX je formát bytecode navrhnutý špeciálne pre Android, ktorý kompiluje aplikácie v programovacom jazyku Java, ktoré následne môžu bežať na platforme Android. [14] [15] [16]

Native C/C++ Libraries

Knižnice C/C++ zahŕňajú širokú a rôznorodú škálu funkcií zahrňujúcich grafiku 2D a 3D grafiky, komunikáciu s protokolmi Secure Sockets Layer (SSL), správu databáz SQLite, prehrávanie zvuku a videa, rendering bitmapových a vektorových písiem, subsystém zobrazovania, správu grafickej vrstvy a implementáciu štandardnej knižnice jazyka C (libc). [14] [15] [16]

Java API Framework

Celý súbor funkcií operačného systému Android je k dispozícii prostredníctvom rozhraní API napísaných v jazyku Java. Tieto rozhrania API tvoria stavebné bloky, potrebné na vytvorenie aplikácií pre systém Android, a to zjednodušením opätovného použitia jadrových, modulárnych systémových komponentov a služieb, medzi ktoré patrí:

- Bohatý a rozšíriteľný systém zobrazenia slúžiaci na vytvorenie používateľského prostredia aplikácie vrátanie zoznamov, mriežok, textových polí, tlačidiel a dokonca aj vstavaného webového prehliadača.
- Správca zdrojov, poskytujúci prístup k zdrojom, ako sú lokalizované reťazce, grafika a súbory rozloženia.

- Správca upozornení, ktorý umožňuje všetkým aplikáciám zobrazovať vlastné upozornenia v stavovom riadku.
- Správca aktivít, riadiaci životný cyklus aplikácií a poskytujúci spoločný spätný zásobník navigácie.
- Poskytovatelia obsahu, ktorí umožňujú aplikáciám prístup k údajom z iných aplikácií, napríklad aplikácia Kontakty, alebo pre zdieľanie vlastných údajov. [14] [15] [16]

System Apps

Android obsahuje sadu hlavných aplikácií pre e-mail, SMS správy, kalendáre, prehliadanie internetu, kontakty a ďalšie. Aplikácie, ktoré sú súčasťou platformy, nemajú žiadny špeciálny stav medzi aplikáciami, ktoré sa používateľ rozhodne nainštalovať. Takže aplikácia tretej strany sa môže stať predvoleným webovým prehliadačom, správcom SMS alebo dokonca predvolenou klávesnicou. Aj tu však platia niektoré výnimky, napríklad aplikácia Nastavenie systému. [14] [15] [16]

2.2.3 Výhody operačného systému Android

Výhodou operačného systému Android je veľmi dobré súbežné spracovanie úloh (multitasking) a efektivita v oznámeniach o úlohách v operačnom systéme, ako sú: e-maily, aplikácie a ich aktualizácie. Operačný systém Android je open-source platforma, takže je ľahko prispôsobiteľný, existuje naň obrovské množstvo bezplatných aplikácií a taktiež existuje množstvo zariadení, ktoré pracujú na tomto operačnom systéme. [17] [22]

2.2.4 Nevýhody operačného systému Android

Nevýhodou v rámci operačného systému Android je optimalizácia, ktorá nie je najlepšia pre všetky zariadenia z dôvodu častého vydávania novších operačných systémov. To sa odráža aj na zákazníckej podpore, ktorá je takmer nulová, a nízkom počte bezpečnostných aktualizácií, ktoré nevychádzajú tak často ako by mali, pre staršie zariadenia vôbec. Ďalšou nevýhodou v rámci bezpečnosti je možnosť inštalovania aplikácií tretích strán z iných zdrojov než je oficiálny obchod. Taktiež meniace sa rozhranie v každom zariadení a potreba mať vytvorený účet na Google môžeme brať ako nevýhodu. [23]

2.3 iOS

iOS (predtím iPhone OS), je mobilný operačný systém vytvorený a vyvinutý spoločnosťou Apple Inc. výlučne pre svoj hardvér, čo sa pozitívne prejavuje na jeho rýchlej odozve a tiež výdrži batérie. Je to operačný systém, ktorý v súčasnosti ovláda mnohé mobilné zariadenia spoločnosti, vrátane iPone, iPad, iPod Touch. Rovnako, ako operačný systém Android, je iOS jeden z najpopulárnejších operačných systémov na svete.

Používateľské rozhranie iOS je založené na priamej manipulácii pomocou gest s viacerými dotykmi. Prvky zariadenia pozostávajú z posuvníkov, spínačov a tlačidiel, ktoré uľahčujú prechádzanie medzi jednotlivými aplikáciami. [18]

2.3.1 História operačného systému iOS

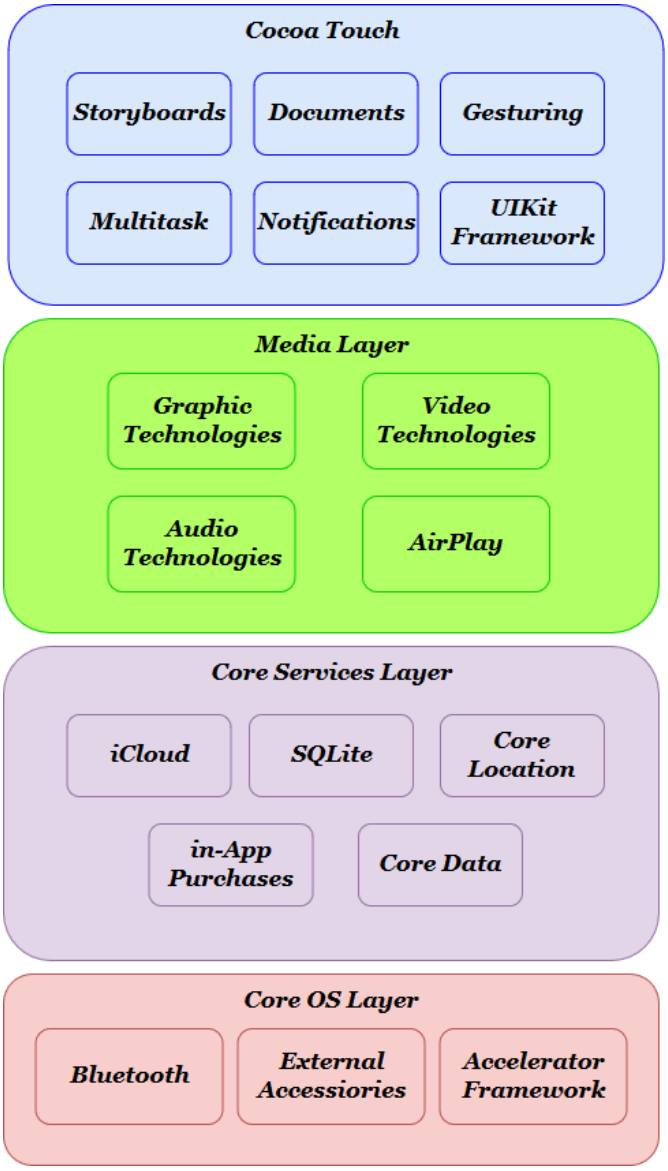
Operačný systém bol spolu s prvým iPhone zariadením predstavený v januári 2007 a uvedený na trh v júni toho istého roku. Prvý operačný systém iPhone nemal oficiálny názov, ale Steve Jobs uviedol, že je to verzia OS X, pretože zdieľal kód s operačným systémom Mac. Prvý systém bol dosť okliešťený čo sa týka funkčnosti. Neobsahoval žiadny obchod s aplikáciami, žiadne priečinky, nepodporoval multitasking. Bol ale revolučný so zavedením konceptu „multi-touch“ obrazoviek do sveta. Ako uviedol Jobs, systém tiež kombinoval „iPod, telefón a internetový komunikačný prostriedok“.

Ani nie o rok neskôr iPhone pridal App Store v telefóne OS 2. Milióny stiahnutí boli neskôr pravdepodobne najdôležitejšou súčasťou úspechu iPhone. [25]

Prelom nastáva až s uvedením iPhone 4 v roku 2010, ktorý priniesol dve veľké softvérové funkcie a to aplikáciu multitaskaing a FaceTime. Zaviedol tiež koncept zložiek. V tomto roku tiež Apple upúšťa od označenia „iPhone“ a začína používať názov „iOS“. [24]

2.3.2 Architektúra operačného systému iOS

Architektúra iOS je zjednodušenou verziou operačného systému Mac OS X, používaného v počítačoch od spoločnosti Apple. Táto architektúra sa skladá z nasledujúcich vrstiev zobrazených na diagrame.



Obrázok 4 Architektúra operačného systému iOS [26]

Core OS Layer

Technológie a frameworky vo vrstve Core OS poskytujú na nízkej úrovni služby týkajúce sa hardvéru a sietí. Tieto služby sú založené na zariadeniach vo vrstve Kernel a Device Drivers. Vrstva Core OS implementuje funkcie súvisiace s bezpečnosťou aplikácií.

- Gatekeeper umožňuje používateľom zablokovať inštaláciu softvéru, ktorý nepochádza z Mac App Store a od identifikovaných vývojárov. Ak aplikácia nie je podpísaná Developer ID certifikátom vydaným spoločnosťou Apple, nebude sa na systémoch spúšťať, ak majú túto možnosť zabezpečenia spustenú.

- Aplikácia Sandbox poskytuje poslednú obrannú líniu pred ukradnutím, poškodením alebo odstránením používateľských údajov ak je systém napadnutý škodlivým kódom. Sandbox taktiež minimalizuje škody spôsobené chybou v kódovaní. Jeho stratégia je dvojitá a to tak, že umožňuje podpísať ako aplikácia komunikuje so systémom. Následne poskytne aplikácii iba prístup, ktorý potrebuje na svoju prácu a nič viac. Taktiež umožňuje používateľovi transparentne prideliť aplikácii prístup pomocou dialógov Otvoriť a Uložiť, a ďalších známych interakcií používateľov.
- iOS používa bezpečnostnú technológiu známu ako podpisovanie kódov, ktorá umožňuje potvrdiť, že aplikácia bola skutočne vytvorená daným výrobcom. Po podpísaní aplikácie dokáže systém rozpoznať akúkoľvek zmenu, či už ide o náhodnú zmenu alebo zmenu škodlivým kódom. Rôzne bezpečnostné technológie, vrátane App Sandbox a rodičovskej kontroly, závisia od podpísania kódu. [27]

Core Services Layer

Technológie obsiahnuté vo vrstve Core Services Layer sa nazývajú základné služby, pretože poskytujú základné služby pre aplikácie, ale nemajú žiadny vplyv na používateľské rozhranie aplikácie. Vo všeobecnosti sú tieto technológie závislé na rámcoch a technológiách v dvoch najnižších vrstvách OS X – teda vrstve Core OS, a vrstve Kernel a jeho ovládačoch zariadenia. [27]

Media Layer

Charakteristickými znakmi používateľského rozhrania OS X je jeho grafika. Využitie technológie Media Layer umožňuje, aby aplikácie používali 2D a 3D grafiku, animácie, obrazové efekty a profesionálne audio a video funkcie. OS X podporuje viac ako 100 typov médií, ktoré pokrývajú celý rad audio, video, obrázkov a streamovaných formátov. [27]

Cocoa Touch Layer

Aplikačná vrstva Cocoa Touch Layer je primárne zodpovedná za vzhľad aplikácií a ich reakciu na akcie používateľov. Navyše mnohé funkcie, ktoré definujú používateľské rozhranie OS X, ako je Centrum upozornení, Režim celej obrazovky a Automatické ukladanie, sú taktiež implementované Cocoa Touch Layer. [27]

2.3.3 Výhody operačného systému iOS

Výhodou je optimalizácia hardvéru aj softvéru riadená spoločnosťou Apple. Aj pre staršie zariadenia vychádzajú pravidelné aktualizácie. iOS je prívetivý z hľadiska užívateľského

rozhrania, má vynikajúcu zákaznícku podporu a celkový prístup k zákazníkovi. Aplikácií je síce menej ako pre operačný systém Android ale z hľadiska bezpečnosti a kvality sú na tom lepšie. [23]

2.3.4 Nevýhody operačného systému iOS

Keďže iOS nie je open-source, všetky jeho služby a zariadenia patria spoločnosti Apple, ktorá má plnú kontrolu nad aplikáciami a obsahom, ktorý je väčšinou platený a nie je možné ho ďalej zdieľať. Nevýhodou je tiež povinnosť používania služby iTunes pre synchronizáciu všetkých súborov so zariadením. iOS taktiež nepodporuje externé ukladanie, čo znamená že zariadeniu nie je možné rozšíriť úložisko pomocou SD kariet. [23]

II. PRAKTICKÁ ČASŤ

3 OCHRANA PROTI ŠKODLIVÉMU SOFTVÉRU

V tejto časti bakalárskej práce popisujem základné a najčastejšie zabezpečenie proti škodlivému softvéru popisovanému v teoretickej časti, kapitola 1. V kapitole 5 je následne prakticky ukázané ako sa proti týmto škodlivým softvérom brániť.

3.1 Ochrana proti vírusom a červom

Pre ochranu zariadenia proti vírusom sa používa antivírusový softvér, ktorý slúži ako pomyselná brána medzi zariadením a internetom. Antivírusový program, pri sťahovaní súborov alebo aplikácií z internetu a pred ich uložením do zariadenia, preskenuje danú aplikáciu a zaistí, že sa vírus do zariadenia nedostane. Taktiež je dobré dbať na to, aby bol daný antivírusový program, operačný systém a rôzne ďalšie programy pravidelne aktualizované, pretože nové hrozby z internetu sa objavujú denne.

V tomto prípade sa dajú použiť aj bezpečnostné balíky firewall, ktoré sú určené pre zabránenie neoprávneného prístupu do alebo zo súkromnej siete. Firewally môžu byť implementované ako hardvér a softvér, alebo kombinácia oboch. Tiež môžu byť aj súčasťou operačného systému. Sieťové firewally sú často použité pre zabránenie neoprávnených používateľov internetu pristupovať k súkromným sieťam pripojeným na internet. Všetky správy vstupujúce alebo opúšťajúce súkromnú sieť prechádzajú cez bránu firewall, ktorá skúma každú správu a blokuje tie, ktoré nespĺňajú dané bezpečnostné kritériá. Softvérové firewally sú nainštalované v zariadení rovnako ako každý softvérový program a užívatelia si ich dokážu prispôsobiť, čo umožňuje určitú kontrolu nad funkciami ochrany. Taktiež chránia zariadenia pred vonkajšími pokusmi o ich ovládanie alebo prístupmi k tomuto zariadeniu.

3.2 Ochrana proti Trójskym koňom

V tejto súvislosti je prvou a najlepšou možnosťou ochrany proti trójskym koňom nikdy neotvárať prílohy e-mailu alebo spustiť program, ak si užívateľ nie je istý z akého zdroja pochádza. Tieto typy vírusov sú v súčasnosti rozšírené najmenej, keďže ich funkcia sa postupom času nemení. Preto na ich detekciu a odstránenie postačí antivírusový program.

3.3 Ochrana proti Spyware a Adware

Možno najdôležitejším krokom v zabránení infikovania zariadenia Spywarom je mať nainštalovaný nástroj, ktorý dokáže detekovať a zabrániť inštalácií škodlivého kódu do zariadenia. Väčšina antivírusových programov je účinná pri identifikácií rôznych typov Spywaru,

ale nemusí rozpoznať všetky jeho varianty. Dobrým riešením je mať nainštalovaný okrem antivírusového softvéru aj softvér na detekciu Spywaru. Spyware sa do zariadenia často dostáva pri návšteve infikovaných alebo škodlivých webových stránok. Preto by mal byť užívateľ opatrný pri klikaní na odkazy webových stránok z neznámych zdrojov. Okrem toho je dobré sťahovať programy iba z dôveryhodných webových stránok.

Spyware sa dokáže nainštalovať do zariadenia aj pomocou pop-up okna. Preto je potrebné dbať na zvýšenú pozornosť pri zobrazení nežiaduceho alebo náhodného upozornenia a neklikať na tlačidlo „Súhlasím“ alebo „OK“, čím sa uzavrie kontextové okno. V skutočnosti sa do zariadenia nainštaluje škodlivý softvér. Namiesto toho je dobré toto okno zavrieť kliknutím na „X“ v rohu upozornenia, ktoré je vo veľmi veľa prípadoch zle viditeľné.

Aktualizovanie webového prehliadača môže taktiež pomôcť zabrániť inštalácií Spywaru. Väčšina prehliadačov dokáže upozorniť na škodlivé programy a navrhnúť bezpečný postup v prípade možnej infikácie.

3.4 Ochrana proti Phishing

Výrazné zníženie šance na to stať sa obeťou útoku typu Phishing, je byť opatrný pri online prehliadaní a kontrole e-mailov. Je dobré neklikať na odkazy v e-maile, pokiaľ si užívateľ nie je istý, či sa jedná o autentický zdroj. Ak má užívateľ pochybnosti, je vhodné otvoriť nové okno prehliadača a zadať adresu URL do panela s adresou. Tiež je potrebné dávať si pozor na e-maily vyžadujúce dôverné informácie – hlavne ak sa jedná o osobné údaje alebo bankové informácie. Legitímne organizácie, vrátane banky, totiž nikdy nebudú požadovať citlivé informácie prostredníctvom e-mailu. Veľmi veľa e-mailov slúžiacich na Phising je veľmi ľahké rozoznať. E-maily sa od tých pravých odlišujú množstvom slov, veľkými a malými písmenami, a výkričníkmi. Môžu tiež obsahovať neosobný pozdrav alebo nepravdepodobný obsah.

Druhou dôležitou vecou je venovať pozornosť skráteným linkom, najmä na sociálnych médiách. Cyber-kriminálnici často používajú tieto služby na to, aby si používateľ myslel, že klikol na legitímny odkaz, ale v skutočnosti je neúmyselne nasmerovaný na falošnú stránku. Tieto falošné stránky sú používané na ukradnutie zadaných osobných údajov alebo na vykonanie útoku typu „drive-by-download“, čím zamorujú zariadenie škodlivým softvérom.

Užívateľ by mal vždy, ak je to možné, používať bezpečnú webovú stránku (označenú protokolom https:// a ikonou zámku v paneli s adresou prehliadača), ktorú chce prehľadávať, a to

hlavne pri odosielaní citlivých informácií ako sú osobné údaje. Nikdy by nemal používať verejné, nezabezpečené Wi-Fi na prezeranie bankovníctva, nakupovanie alebo zadávanie osobných údajov. Pokiaľ je to možné, treba použiť internet od operátora.

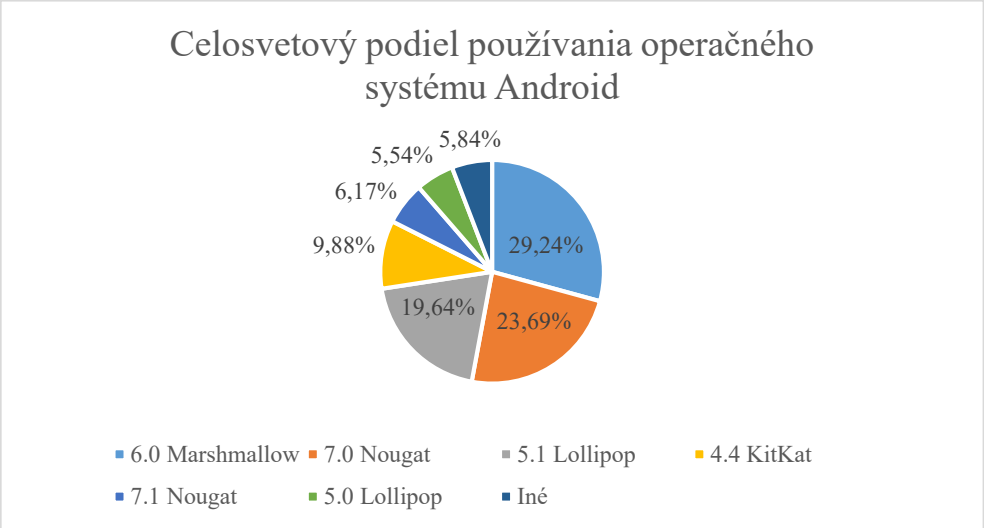
3.5 Ochrana proti Ransomware

Najlepšou ochranou proti Ransomware je prekonať útočníkov tým, že užívateľ nebude ohrozený ich útokom. Znamená to denné zálohovanie dôležitých údajov, takže aj v prípade, že sa zariadenie uzamkne a zašifruje, nebude potreba platiť útočníkom za to, aby svoje údaje znovu získal. Tiež je dobré nezabudnúť na to, že Ransomware dokáže šifrovať súbory na mapovaných jednotkách. To zahŕňa akékoľvek externé jednotky ako je napríklad USB, ako aj všetky súbory v sieťach alebo cloudových súboroch. Takže to, čo užívateľ potrebuje, je bežný režim zálohovania, externý disk alebo zálohovacia služba, ktorá je odpojená od zariadenia, ak nie je potrebná.

4 ŠTANDARDNÉ ZABEZPEČENIE MOBILNÉHO OPERAČNÉHO SYSTÉMU

Táto kapitola popisuje mnou odporúčané postupy, tipy a aplikácie pre štandardné zabezpečenie mobilného operačného systému s operačným systémom Android 6.0 Marshmallow. Špecifikáciu testovaného zariadenia nájdete v prílohe (***P I: HW ŠPECIFIKÁCIA MOBILNÉHO TELEFÓNU LENOVO A7000***).

Tento operačný systém bol zvolený z dôvodu, že sa jedná o najpoužívanejšiu verziu operačného systému Android v dobe písania práce, t.j. Január 2018, ako môžeme vidieť na Obrázku 5, ale taktiež z dôvodu vlastnenia zariadenia s týmto systémom. Čo sa odráža na jednoduchšom testovaní zabezpečenia, než by bolo pri emulovaní operačného systému na počítači, ktoré by nebolo tak presné ako na reálnom zariadení. [28]



Obrázok 5 Používané verzie os Android k januáru 2018 podľa webu Statcounter [28]

4.1 Fyzické zabezpečenie mobilného telefónu

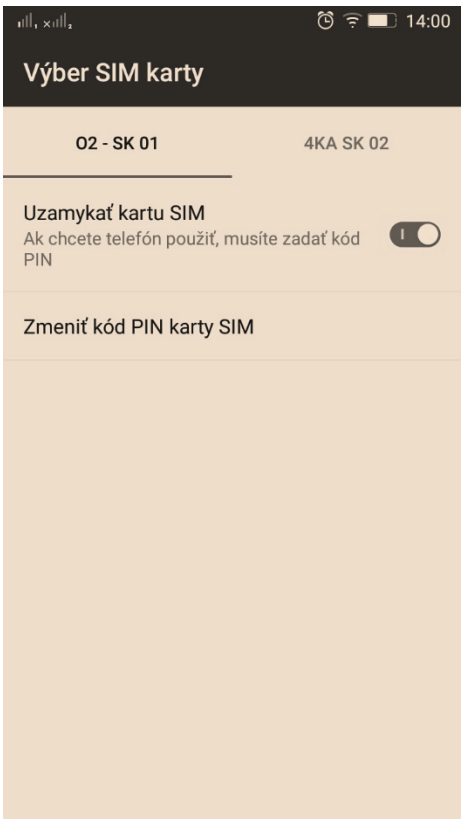
Strata alebo odcudzenie mobilného telefónu je jedna z najčastejších príčin straty osobných údajov. Mobilné zariadenia sa strácajú alebo končia v rukách niekoho iného pravidelne. Či už sa jedná o služobný mobilný telefón alebo vlastný, skutočnosť, že nakoniec pristane v rukách iného človeka, je vážny bezpečnostný problém. Je to jeden z najhorších scenárov, pretože mobilný telefón v dnešnej dobe obsahuje obrovské množstvo informácií o užívateľovi, či už sa jedná o osobné údaje, heslá alebo e-maily. Pritom ide iba o jednu stranu mince. Čo

napríklad, ak užívateľ povolí inému človeku použiť jeho mobilné zariadenie na telefonovanie alebo napísanie SMS správy? Povolenie takéhoto prístupu do mobilného zariadenia sa môže rovnať strate veľmi citlivých informácií o vlastníkovi (prípadne zamestnávateľovi).

Tipov, ako sa proti takejto strate osobných údajov brániť, je viacero. Jednou zo základných chýb užívateľov je ponechanie predvoleného zámku karty SIM (PIN kódu). Formát PIN kódu býva spravidla veľmi ľahko zapamätateľný, preto ho väčšina užívateľov nezmení.

Ako si zmeniť PIN kód SIM karty ?

Vybrať v ponuke ikonu *Nastavenie* -> ísť do ponuky „*systém*“ -> pokračovať do „*zabezpečenie*“ -> ďalej do „*Nastavenia zabezpečenia karty SIM*“ -> zvoliť možnosť „*Uzamykať kartu SIM*“ (ak nie je zapnutá) a vybrať „*Zmeniť PIN karty SIM*“



Obrázok 6 Nastavenie PIN kódu pre SIM kartu

Ďalším odporúčaným krokom pre zabezpečenie mobilného zariadenia je nastavenie uzamykacej obrazovky po každom uspaní zariadenia. Týchto zabezpečení existuje viacero, ako napríklad prejdenie prstom, hlasové odblokovanie, odblokovanie vzorom, PIN kódom alebo heslom. Z týchto nastavení rozhodne neodporúčam odblokovanie prstom, pretože sa jedná len o potiahnutie prsta po displeji zariadenia. Taktiež neodporúčam odomykanie hlasom, pri

ktorom je znížená bezpečnosť tým, že táto možnosť má problém s rozpoznaním, ak zaznamená podobný hlas ako má vlastník zariadenia. Rovnako neposkytuje dostatočnú ochranu v prípade nahrávky vlastníkovho hlasu.

Odporúčanou formou zabezpečenia je odblokovanie vzorom alebo heslom. Tieto dve možnosti poskytujú dostatočnú formu zabezpečenia, pričom uzamknutie mobilného zariadenia heslom je bezpečnejšie ale pomalšie, a uzamknutie vzorom menej bezpečné ale za to rýchlejšie. Samozrejme aj tu platí, že čím viac znakov heslo obsahuje, tým zabezpečenejšie sa zariadenie stáva.

Ako zabezpečiť zariadenie uzamykacou obrazovkou ?

Vybrať v ponuke ikonu *Nastavenie* -> ísť do ponuky „*osobné*“ -> pokračovať do „*uzamknúť obrazovku*“ -> zvoliť jednu z možností uzamknutia obrazovky

Obrázok 7 Nastavenie zabezpečenia obrazovky

Posledným odporúčaným krokom pred stratou alebo krádežou mobilného zariadenia sú programy tretích strán s funkciami Anti-Theft. Tieto aplikácie dokážu monitorovať stratené alebo ukradnuté zariadenie pomocou GPS a určiť jeho polohu. Ja osobne môžem odporučiť aplikáciu ***ESET Mobile Security & Antivirus*** . Jedná sa o aplikáciu s mnohými funkciami,

vrátane antivírusu. Tento program dokáže pomocou GPS zistiť stav zariadenia, jeho poslednú známu polohu, posledné navštívené stránky. Dokáže odosielať fotografie z predného a zadného fotoaparátu, či má dokonca možnosť poslať správu pri zle zadanom hesle alebo neznámej SIM karte s informáciami o nej.

4.2 Zálohovanie a synchronizácia dát

Veľká väčšina užívateľov pravidelne nezálohuje svoje dáta. V dnešnej dobe sa dá o dáta prísť kedykoľvek. Zálohovanie sa môže zdať časovo náročné a zastrašujúce, ale vôbec to tak nie je. Každý to zvládne a každý by to mal robiť.

Odborníci odporúčajú pravidlo 3-2-1 na zálohovanie: tri kópie dokumentov, dve lokálne (na rôznych zariadeniach) a jedna mimo lokality. Pre veľký počet ľudí to znamená mať pôvodné dáta uložené v počítači, zálohu na externom pevnom disku a ďalšie dáta uložené na cloude. S takýmto systémom je veľmi nepravdepodobné, že sa stratia všetky údaje v prípade, že bude zariadenie stratené, poškodené, atď... [29]

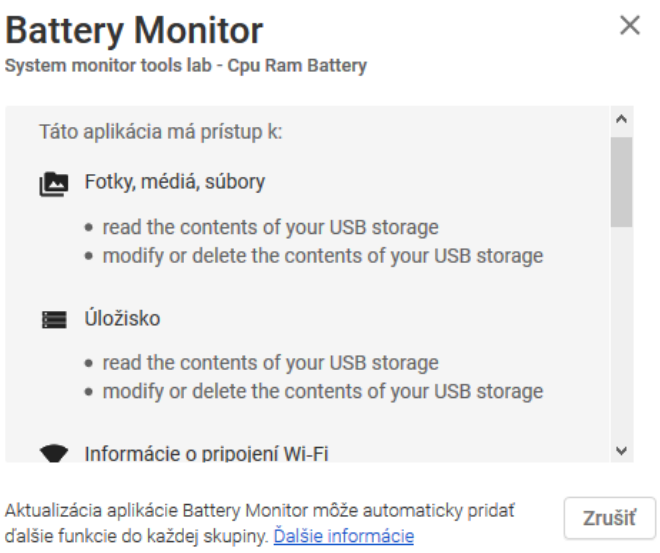
V dnešnej dobe je na výber veľa aplikácii, ktoré poskytujú cloudové služby. Aplikáciu stačí len stiahnuť, nainštalovať, nastaviť a o všetko ostatné sa aplikácia postará sama. Cloudové služby slúžia tiež veľmi dobre ako synchronizačný nástroj, keďže celá synchronizácia prebieha na internete. Ide o to, že sa údaje synchronizujú so serverom, ktorý vedie k cieľu úložiska v cloude, a tým dokáže zmeniť každú úpravu dokumentu v zariadení a zároveň aj na cloude. Takto užívateľovi odpadá starosť o neustále kopírovanie a prepisovanie dokumentu. Ďalšou výhodou cloudových služieb je, že sú multiplatformné, tzn. dokumenty alebo dáta uložené na mobilnom telefóne môžu byť otvorené, upravené, kopírované na ďaľších zariadeniach majúcich a podporujúcich danú službu.

Mnou podporované aplikácie na zálohovanie a synchronizáciu dát pre mobilné zariadenia sú ***Microsoft OneDrive*** a ***Google Drive*** **.** Google Drive odporúčam hlavne kvôli previazaniu na služby od spoločnosti Google, či už ide o e-mailového klienta, kancelársky balík alebo zariadenia s operačným systémom Android. Veľkou výhodou je taktiež otváranie, upravovanie a zdieľanie priamo v aplikácií. V prípade Microsoft OneDrive platí, rovnako ako pri predchádzajúcej aplikácii, previazanie na služby od Microsoftu s tým, že aplikácia umožňuje zálohovať nielen dokumenty ale aj nastavenie zariadenia, a v prípade poruchy na zariadení dokáže vrátiť systém do pôvodného stavu.

4.3 Inštalovanie aplikácií

Aplikácie sú jedným z najčastejších zdrojov infikovania operačného systému škodlivým softvérom. Preto najlepším možným riešením, ako inštalovať aplikácie do zariadenia, je cez obchod Google Play. Pri inštalovaní aplikácie je dobré dbať na zvýšenú pozornosť z dôvodu možného stiahnutia nechcenej aplikácie, pretože Google Play obsahuje ohromné množstvo rôznych aplikácií a nie všetky sú bezpečné. K väčšej bezpečnosti má dopomôcť aj aplikácia Google Play Protect, ktorá je priamo inštalovaná k aplikácií Google Play a pravidelne kontroluje aplikácie a zariadenie, a hľadá stopy po škodlivom softvéri, preto je dobré túto funkciu povoliť v nastaveniach aplikácie. Taktiež pomáha sledovať hodnotenia a recenzie aplikácie. V prípade jej nahlásenia ako škodlivého softvéru viacerými užívateľmi sa Google touto aplikáciou začne zaoberať.

Ďalšou veľmi dôležitou vecou pri inštalovaní nových aplikácií z obchodu Google Play sú povolenia, ktoré aplikácie vyžadujú od daného mobilného zariadenia. Môže ísť o všetko od informácií o pripojení k internetu až po monitorovanie hovorov. Preto je dobré si tieto povolenia kontrolovať pri každej inštalácii.



Obrázok 8 Povolenia pre aplikáciu

Poslednou dôležitou vecou je mať v nastaveniach zariadenia vypnutú možnosť povolenia inštalácie aplikácií z neznámych zdrojov. Týmto nastavením sa zamedzí inštalovanie aplikácií z iných zdrojov, než sú overené zdroje.

4.4 Pravidelná aktualizácia operačného systému a aplikácií

Aktualizácia softvéru v operačnom systéme Android je veľmi jednoduchá a stačí k tomu iba pripojenie na internet. Služba Google Play sa automaticky postará o to, aby bola v zariadení nainštalovaná aktuálna verzia softvéru. Samozrejme sa priamo v aplikácii dá nastaviť spôsob automatickej aktualizácie, prípadne jej vypnutie. Túto možnosť však neodporúčam z dôvodu zabezpečenia zariadenia. Mnohé zo zastaralých aplikácií môžu obsahovať chyby alebo škodlivý softvér, čo môže viesť k spomaleniu alebo úplnému znefunkčneniu zariadenia.

Čo sa týka pravidelnej aktualizácie operačného systému a bezpečnostných aktualizácií je to, čo sa operačného systému týka, horšie. Z dôvodu rýchleho vydávania novších a novších verzií operačného systému dochádza k strate podpory pre staršie verzie. Taktiež dosť záleží na výrobcovi daného zariadenia, ktorý by mal dodržiavať nasadzovanie opravných aktualizácií na zariadenie.

4.5 Vypínanie automatického pripojenia na Wi-Fi, Bluetooth

Poslednou radou pri zabezpečení mobilného operačného systému je zvýšená pozornosť pri pripájaní k nezabezpečeným sieťam. Veľká väčšina užívateľov zabúda po práci s mobilným zariadením vypínať Wi-Fi a môže sa stať, že sa zariadenie pripojí k nezabezpečenej sieti. Väčšina týchto sietí síce nebezpečná byť nemusí ale môže sa stať, že sa útočník veľmi ľahko pomocou nezabezpečeného pripojenia dostane k citlivým informáciám.

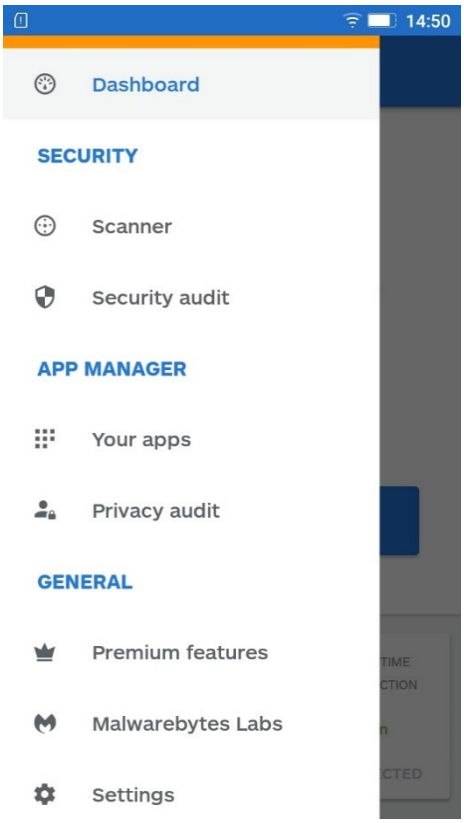
Ak už sa užívateľ chce pripojiť na takto nezabezpečenú sieť, odporúčam nepracovať s citlivými údajmi.

4.6 Ďalšie odporúčané programy

Prehliadač Adblocker - Za mňa veľmi osvedčený program, ktorý slúži ako dobrá alternatíva k prehliadačom. Dokáže blokovať všetky druhy reklám na webových stránkach, či už ide o reklamné videá alebo pop-up reklamy. Tým sa znižuje riziko nakazenia zariadenia škodlivým softvérom. Bližšie informácie o programe v prílohe (***P II: ODPORÚČANÉ APLIKÁCIE PRE ZABEZPEČENIE OPERAČNÉHO SYSTÉMU ANDROID***).

Malwarebytes – Odporúčam ako náhradný antivírus. Jedná sa o program pre kontrolu a ochranu zariadenia pred škodlivým softvérom ako je Malware, Ransomware a iné bezpečnostné hrozby pre mobilné zariadenia, s pravidelne aktualizovanou databázou. Program dokáže nájsť aj také hrozby, ktoré iný antivírusový program nedokáže, preto odporúčam aj pri

podozrení, že je zariadenie infikované, preskenovať ho okrem používaného antivírusu aj touto aplikáciou. Na Obrázku 10 môžeme vidieť hlavné menu aplikácie po nainštalovaní v mobilnom zariadení. Bližšie informácie o programe v prílohe (***P II: ODPORÚČANÉ APLIKÁCIE PRE ZABEZPEČENIE OPERAČNÉHO SYSTÉMU ANDROID***).



Obrázok 9 Aplikácia Malwarebytes v obchode Google Play a prehľad hlavného menu programu

5 TESTOVANIE NAVRHNUTÉHO ZABEZPEČENIA

V predchádzajúcej kapitole sme si predstavili rôzne nastavenia a aplikácie, ktoré dokážu zabezpečiť zariadenie a znížiť tak šancu útoku, či už ide o fyzickú stratu zariadenia alebo o útok z internetu.

Táto kapitola bakalárskej práce ukazuje mnou zvolené nastavenie zabezpečenia mobilného operačného systému, či už ide o priame nastavenie alebo aplikáciu slúžiacu na zvýšenie bezpečnosti zvoleného operačného systému. V kapitole taktiež môžeme vidieť overenie mnou navrhnutého zabezpečenia operačného systému a tiež aj test výkonu a výdrže zariadenia.

5.1 Nastavenie a aplikácie pre zabezpečenie zariadenia

Čo sa týka nastavovacej časti, na zariadení je nastavený PIN kód, spolu z uzamykaním obrazovky na heslo a to nie len manuálnym vypnutím displeja zariadenia, ale aj automatickým zhasnutím obrazovky po 30 sekundách neaktivity užívateľa. V nastavení zariadenia je taktiež deaktivovaná možnosť inštalovať aplikácie z neznámych zdrojov. Zariadenie je tiež pripojené k službe Google pre synchronizáciu a ukladanie dát na cloud.

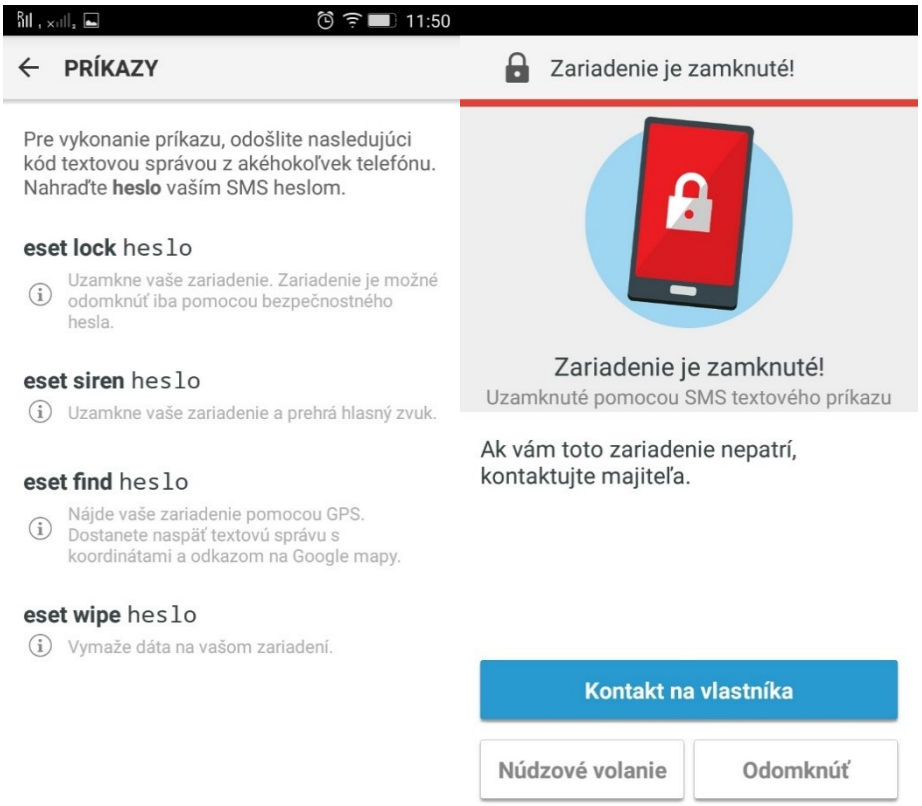
Aplikácie, ktoré som zvolil pre zabezpečenie operačného systému, sú ***ESET Mobile Security & Antivirus*** a taktiež program ***NoRoot Firewall,*** pomocou ktorého dokážeme aplikáciám povoliť alebo zakázať komunikáciu s internetom. Ako internetový prehliadač som zvolil Chrome, ktorý ma v sebe vstavanú funkciu bezpečného prehliadania, pomocou ktorej dokáže upozorniť na nebezpečnú internetovú stránku.

5.2 Overenie navrhnutého zabezpečenia

Overenie navrhnutého zabezpečenia prebiehalo v nasledujúcich krokoch, kde som pri overení proti krádeži vyskúšal väčšinu možností, ktoré ponúkal program ***ESET Mobile Security & Antivirus***, presnejšie jeho funkcia Anti-Theft. Ďalšou možnosťou testovania bolo testovanie proti útokom z internetu, kde som pomocou falošného vírusu overil správne nastavenie aplikácie. Posledným testom som zaistil bezpečnosť pri prehliadaní internetu cez mobilné zariadenie. Bližšie informácie o programe v prílohe (***P II: ODPORÚČANÉ APLIKÁCIE PRE ZABEZPEČENIE OPERAČNÉHO SYSTÉMU ANDROID***).

5.2.1 Overenie zabezpečenia proti strate a krádeži

Mobilné zariadenie je pomocou programu ***ESET Mobile Security & Antivirus*** zabezpečené proti krádeži a to hneď za pomoci niekoľkých funkcií. Medzi najhlavnejšiu funkciu patrí možnosť zvoliť aplikáciu ako správcu svojho zariadenia, čím sa aktivuje bezpečnostní opatrenie, ktoré pri 3 zlých pokusoch zadaných pri odblokovaní zariadenia toto zariadenie zablokuje. Následné odblokovanie prebieha formou užívateľského hesla ktoré si užívateľ v danej aplikácii zvolí ako bezpečnostné. Ako môžeme vidieť na Obrázku 9 zariadenie dokážeme taktiež ovládať na diaľku pomocou SMS príkazov, či už ide o uzamknutie telefónu, poslanie GPS súradníc zariadenia alebo kompletné vymazanie dát v zariadení.



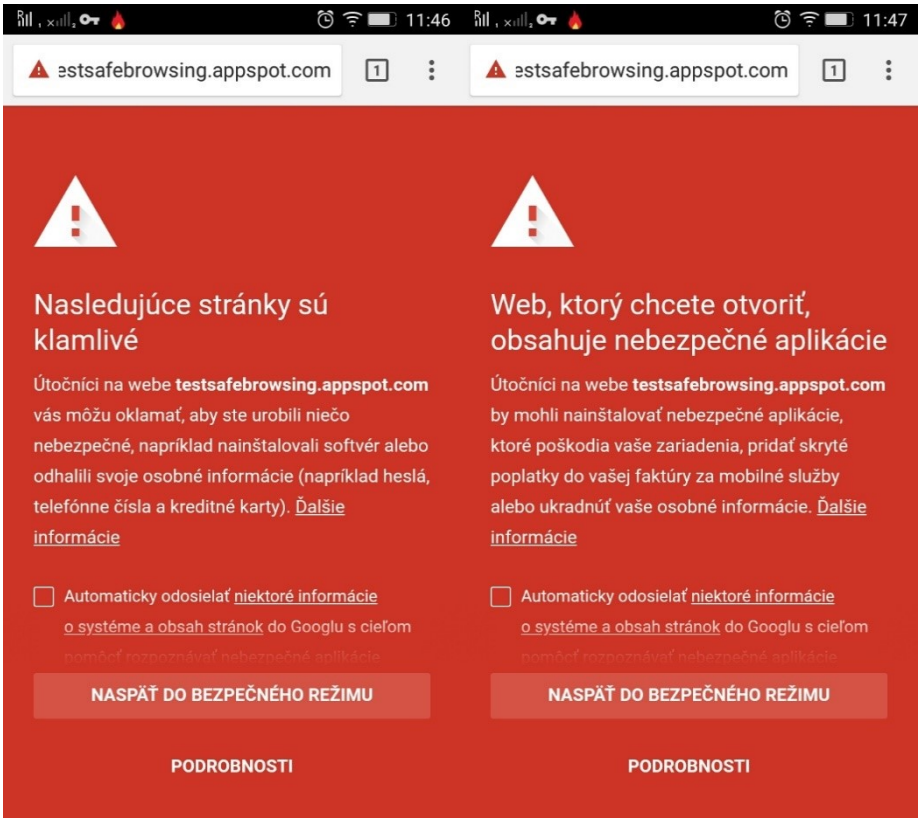
Obrázok 10 Uzamknutie zariadenia pomocou SMS príkazu

5.2.2 Overenie proti hrozbám z internetu

Obrázok 10 ukazuje upozornenie z antivírusového programu pri pokuse o pripojenie k nezabezpečenému internetovému pripojeniu. Toto upozornenie taktiež vypisuje možné riziká ktoré užívateľ podstupuje pri pripojení k tejto sieti.

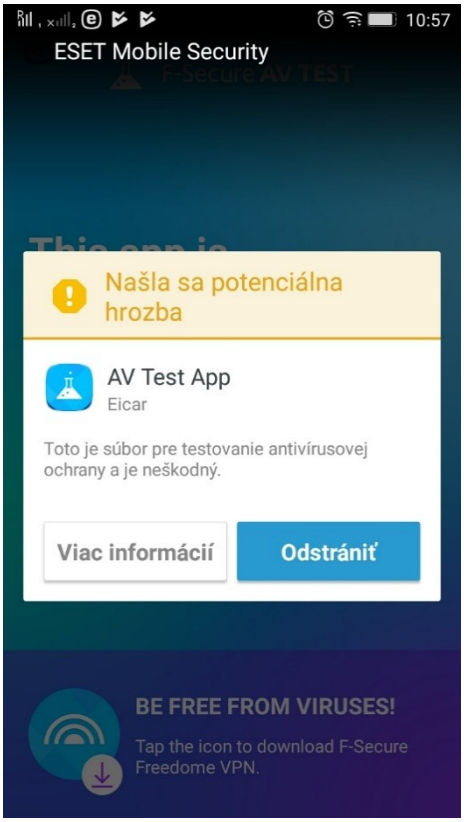
Obrázok 11 Upozornenie na nezabezpečené pripojenie

Zabezpečenie pri internetovom prehliadaní bolo testované pomocou webovej stránky http://testsafebrowsing.appspot.com/, ktorá obsahuje viaceré možnosti ktoré môžu nastať ak užívateľ narazí na potenciálne nebezpečnú stránku, obsahujúcu škodlivý softvér. Test bol uskutočnený pri zapnutej funkcii internetového prehliadača Chrome, a to bezpečné prehliadanie, ktoré má za úlohu blokovať stránky obsahujúce škodlivý softvér tak, ako to je vidieť na Obrázku 11.



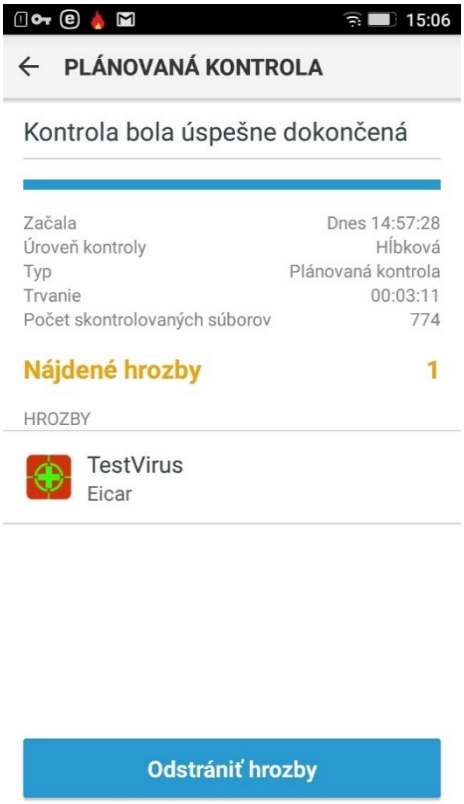
Obrázok 12 Testovanie zabezpečenia prehliadania

Pre otestovanie, či antivírusový program zaregistruje škodlivý softvér v zariadení, som použil ***AV Test App.*** Jedná sa o aplikáciu simulujúcu nainštalovanie škodlivej aplikácie do zariadenia. Slúži na otestovanie správneho nastavenia antivírusového programu. Ako vidieť na Obrázku 12, antivírusový program zachytil škodlivý softvér, z čoho môžeme usudzovať, že pracuje správne a dokáže zachytiť aj iné škodlivé programy.



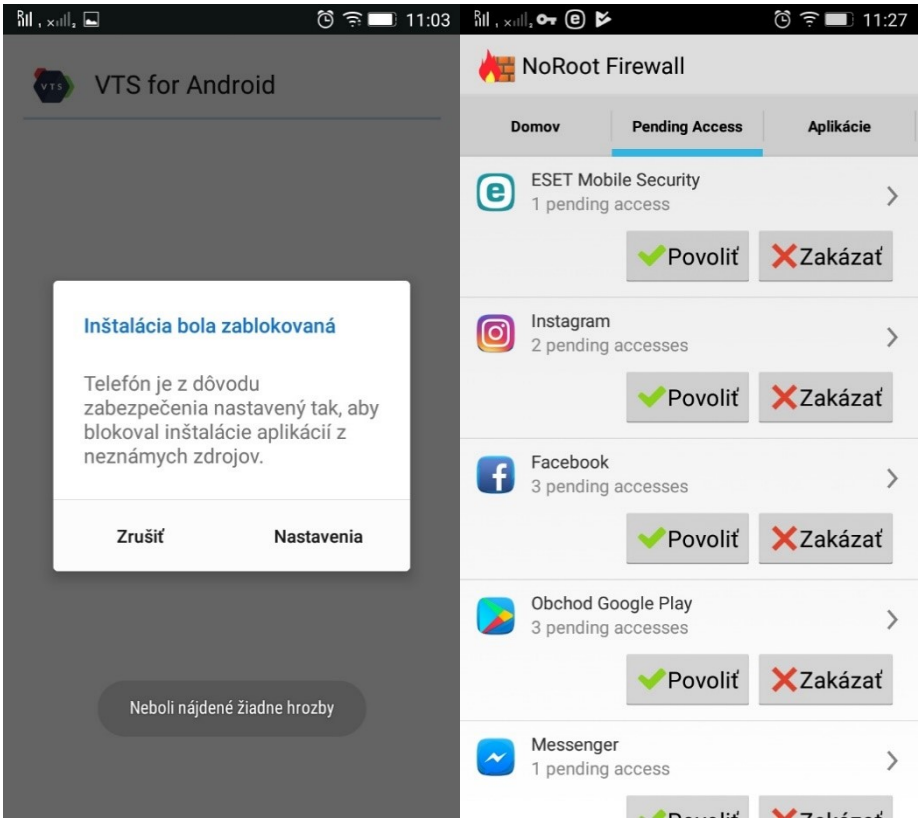
Obrázok 13 Zachytenie hrozby č.1 pomocou antivírusového programu

Ďalšia aplikácia pre otestovanie zabezpečenia mobilného systému je IKARUS TestVirus. Jedná sa o staršiu aplikáciu pracujúcu na rovnakom princípe ako predchádzajúca. Jej úlohou je simulovať stiahnutie škodlivej aplikácie do zariadenia a otestovanie správnej funkčnosti antivírusových programov. Zachytenie tejto aplikácie antivírusovým programom môžeme vidieť na Obrázku 15.



Obrázok 14 Zachytenie hrozby č.2 pomocou antivírusového programu

Posledný z testov môžeme vidieť na Obrázku 13, kde sa na ľavej strane nachádza systémové nastavenie pre zablokovanie inštalovaných aplikácií z neznámych zdrojov. Na pravej strane je zoznam povolení z programu ***NoRoot Firewall***, ktorý zaznamená a čaká na povolenie užívateľa pre každú aplikáciu ktorá sa nachádza v zariadení a snaží sa pristupovať na internet, ale aj pre stiahnuté aplikácie z internetu. Takto má užívateľ prehľad o všetkých aplikáciách na jednom mieste a v prípade, že je aplikácia pre užívateľa neznáma, zablokovať jej prístup do zariadenia. Ďalšie informácie o programe v prílohe (***P II: ODPORÚČANÉ APLIKÁCIE PRE ZABEZPEČENIE OPERAČNÉHO SYSTÉMU ANDROID***).



Obrázok 15 Povolenia pre aplikácie v zariadení

Hlavnou úlohou tejto kapitoly bolo ukázať na reálnom zariadení možnosti zabezpečenia operačného systému pred hrozbami z internetu a tiež to, že existuje mnoho aplikácií ktoré zvyšujú bezpečnosť zariadenia. Ide len o príklady použitia, nie o presný postup zabezpečenia. Taktiež tu nie sú popísané úplne všetky možnosti zabezpečenia, pretože každý mobilný systém a každá aplikácia má rozdielnu funkčnosť a rôzne možnosti zabezpečenia.

5.3 Testovanie výkonu zariadenia

Na testovanie výkonu zariadenia som používal tieto aplikácie.

Elixir 2

Aplikácia slúžiaca na monitorovanie správania zariadenia a systému v reálnom čase. Obsahuje všetky dôležité informácie o telefóne, vrátane spustených aplikácií. Viac informácií o programe v prílohe (***P III: PROGRAMY PRE TESTOVANIE VÝKONU A VÝDRŽE ZARIADENIA***).

Geekbench 4

Jedná sa o jednu z najobľúbenejších aplikácií pre testovanie výkonu zariadenia v obchode Google Play. Je užívateľsky prístupná, nezaberá veľa miesta v zariadení a testovanie netrvá príliš dlho. Obsahuje aktualizované testy CPU, ktoré modelujú reálne úlohy a aplikácie. Sú navrhnuté aby presne a rýchlo merali výkon mobilného procesora v reálnych podmienkach. Okrem toho meria výkon jedného ale aj všetkých jadier procesoru. Veľkou výhodou je dostupnosť na iných platformách. Viac informácií o programe v prílohe (***P III: PROGRAMY PRE TESTOVANIE VÝKONU A VÝDRŽE ZARIADENIA***).

Battery Monitor

Aplikácia slúžiaca na sledovanie vlastností batérie. Môžeme sledovať teplotu a informácie o batérií v reálnom čase vrátane teploty, zdravia, stavu napájania a napätia, a vykresliť ho do prehľadného grafu. Aplikácia tiež dokáže spustiť teplotný alarm pri prehrievaní zariadenia. Viac informácií o programe v prílohe (***P III: PROGRAMY PRE TESTOVANIE VÝKONU A VÝDRŽE ZARIADENIA***).

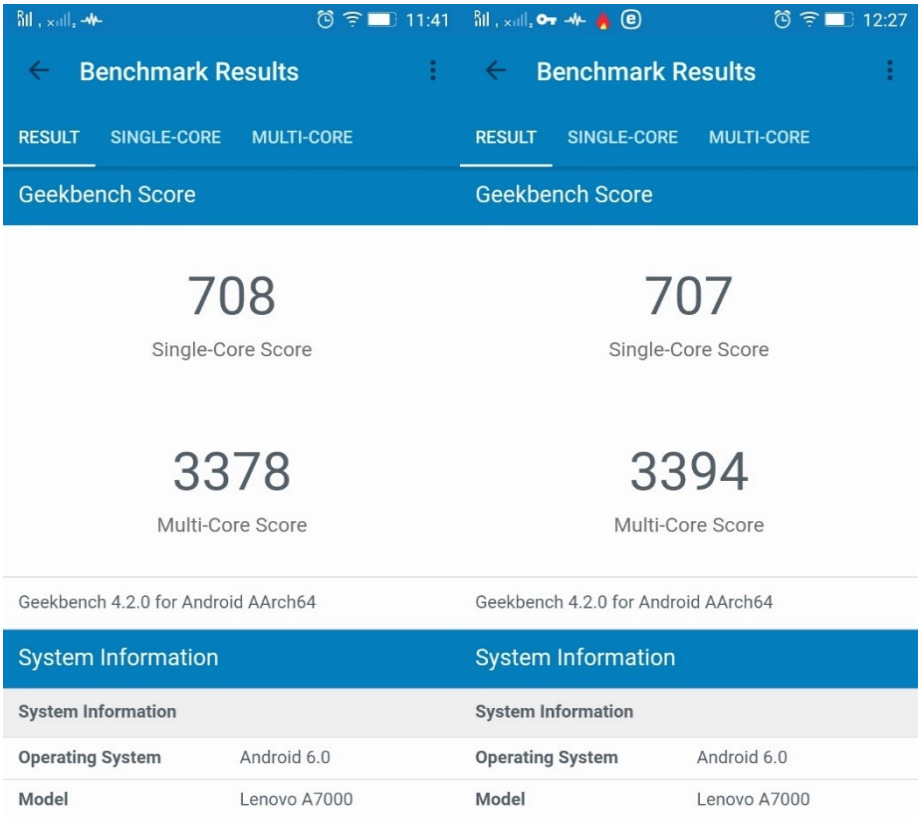
5.4 Spôsob testovania výkonu a výdrže zariadenia

Pri testovaní výkonu a výdrže mobilného zariadenia som postupoval nasledovne:

Zmeral som výkon a výdrž zariadenia pri bežnom používaní mobilného zariadenia s aplikáciami pre bežné používanie a komunikáciu, ale bez navrhnutých aplikácií slúžiacich na zabezpečenie. Následne som nainštaloval a nakonfiguroval mnou zvolené zabezpečovacie aplikácie a nastavenia, a zmeral výkon a výdrž zariadenia, pomocou programov spomenutých vyššie.

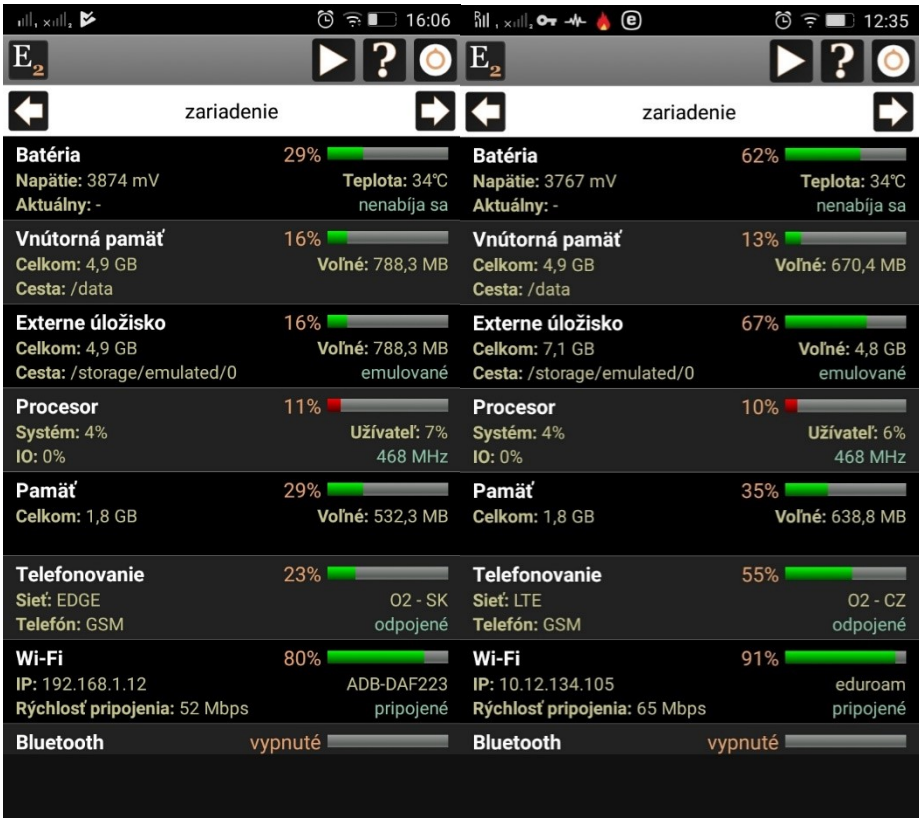
5.5 Test výkonu zariadenia

Ako môžeme vidieť z testu výkonu zariadenia pomocou programu **Geekbench 4** na Obrázku 14, zariadenia bez nainštalovaných a spustených bezpečnostných aplikácií na ľavej strane získali v teste minimálne rozdielny počet bodov ako test výkonu pri spustených bezpečnostných aplikáciách a to **708 bodov** pre jedno jadro procesora a **3378 bodov** pre všetky jadrá na ľavej strane, a **707 bodov** pre jedno jadro a **3394 bodov** pre všetky jadrá procesoru. Keďže ide iba o benchmark aplikáciu, jej výsledky nie sú vôbec smerodajné v praktickom použití.



Obrázok 16 Test výkonu zariadenia pomocou aplikácie Geekbench 4 na ľavej strane bez a na pravej strane s nainštalovanými aplikáciami

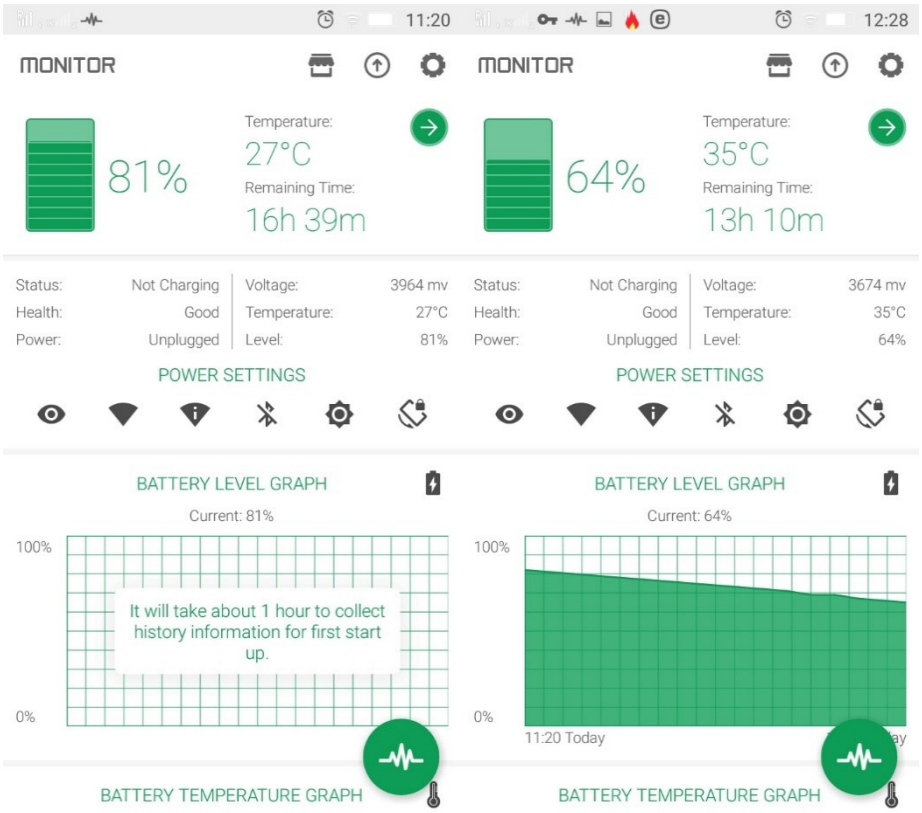
Pre reálne meranie výkonu zariadenia som využil program ***Elixir 2***. Obrázok 15 ukazuje na ľavej strane testovanie pred nainštalovaním bezpečnostných aplikácií, na pravej strane následne test zariadenia po nainštalovaní bezpečnostných aplikácií. Po podrobnejšom preskúmaní vidíme, že vyťaženie procesora v reálnom čase pri oboch testovaniach dopadlo s minimálnym rozdielom, pohybovalo sa okolo 10 – 20%. Taktiež môžeme vidieť významnejší rozdiel vo využití pamäte RAM, čo môžeme pripísať spusteným bezpečnostným aplikáciám na pozadí. Čo sa týka plynulosti pri používaní zariadenia s nainštalovanými aplikáciami, je tento pocit bohužiaľ horší. Zariadenia reaguje pomalšie a pri bežnom používaní bolo citeľné zasekávanie.



Obrázok 17 Test výkonu zariadenia pomocou aplikácie Elixir 2 na ľavej strane bez a na pravej strane s nainštalovanými aplikáciami

5.6 Test výdrže zariadenia

Pri testovaní výdrže pomocou aplikácie ***Battery Monitor*** môžeme na Obrázku 16 pozorovať výdrž batérie, ktorá po približne jednej hodine používania s nainštalovanými bezpečnostnými aplikáciami klesla o 3 hodiny.



Obrázok 18 Testovanie výdrže batérie pomocou programu Battery Monitor na ľavej strane bez a na pravej strane s nainštalovanými aplikáciami

5.7 Zhodnotenie výsledkov

Ako môžeme vidieť v predchádzajúcej podkapitole, inštalované aplikácie na výkon procesoru zariadenia nemajú vplyv. Rozdiely pozorujeme najmä vo využití pamäte RAM a výdrži batérie.

Preto možno tvrdiť, že dnešné aplikácie slúžiace pre zabezpečenie mobilného zariadenia sú navrhnuté tak, že znateľne neovplyvňujú výkon zariadenia tak, aby to bolo poznať pri práci zo zariadením.

Čo sa týka zabezpečenia mobilných operačných systémov, pre nové verzie operačného systému by mali byť dostatočné bezpečnostné záplaty dodávané výrobcom v pravidelných aktualizáciách. Pre staršie zariadenie by som odporúčal minimálne nainštalovaný aktualizovaný antivírusový program pre detekciu škodlivých kódov.

ZÁVER

Cieľom práce bolo ukázať a otestovať zabezpečenie mobilného operačného systému, s využitím aplikácií získaných z obchodu Google Play.

V teoretickej časti sú popísané najčastejšie hrozby z internetu, s ktorými sa v dnešnej dobe môže stretnúť každý. Je stručne vysvetlené ako sa daný škodlivý kód dokáže dostať do zariadenia, aké môže spôsobiť problémy, či už sa jedná o poškodeniu zariadenia alebo zneužitiu osobných údajov užívateľa. V ďalších častiach sú popísané najpoužívanejšie operačné systémy, pre mobilné telefóny a tablety. Špecifickejšie sú popísané operačné systémy Android a iOS. Sú popísané ich vlastnosti, architektúra, výhody a nevýhody používania týchto operačných systémov pre používateľa.

V praktickej časti sú navrhnuté rady akým spôsobom sa brániť proti hrozbám z internetu popísaným v teoretickej časti. Taktiež sú ukázané a vysvetlené postupy štandardného zabezpečenia pre operačný systém Android 6.0 Marshmallow, ktorý je v dobe písania tejto práce najpoužívanejšou verziou operačného systému Android. Tento operačný systém bol zvolený tiež z dôvodu vlastnenia zariadenia a teda aj jednoduchšieho testovania zabezpečenia na tomto zariadení.

Výsledkom práce je navrhnuté vlastné riešenie pre zabezpečenie mobilného operačného systému s využitím aplikácií. Navrhnuté zabezpečenie je otestované, či už proti strate alebo krádeži zariadenia, tak aj proti hrozbám z internetu. Praktická časť je tiež doplnená o testovanie výkonu a výdrže zariadenia pri nainštalovaných aplikáciách slúžiacich na zabezpečenie. Bližšie informácie o aplikáciách použitých v práci sú uvedené v prílohách, či už ide o odkazy na stiahnutie, potrebná verzia operačného systému, alebo posledná aktualizácia aplikácie.

Programy použité v práci majú slúžiť ako príklady zabezpečenia mobilného operačného systému. Z dôvodu obrovského množstva takýchto programov boli použité tie, s ktorými mám osobné skúsenosti. Zabezpečenie nemusí zachytiť všetky druhy škodlivých kódov ktoré existujú. Taktiež obrovský vplyv na zabezpečenie má sám vlastník zariadenia, v prípade že sám vyhľadáva a navštevuje nebezpečné stránky alebo inštaluje aplikácie z neoficiálnych zdrojov. Navrhnuté zabezpečenie môže byť použité aj na iných verziách operačného systému Android.

ZOZNAM POUŽITEJ LITERATÚRY

[1] JIROVSKÝ, Václav. *Kybernetická kriminalita: nejen o hackingu, crackingu, virech a trojských koních bez tajemství*. Praha: Grada, 2007. ISBN 978-80-247-1561-2.

[2] KOŽÍŠEK, Martin a Václav PÍSECKÝ. *Bezpečně n@ internetu: průvodce chováním ve světě online*. Praha: Grada Publishing, 2016. ISBN 978-80-247-5595-3.

[3] HÁK, Igor. *Moderní počítačové viry.* [online]. , 110 [cit. 2018-04-28]. Dostupné z: http://www.cmsps.cz/~marlib/bezpecnost/viry/velka_kniha_o_virech.pdf

[4] The Top 5 Most Common Types of Phone Viruses and How to Know If You Have One. *Solver Your Tech* [online]. [cit. 2018-04-28]. Dostupné z: http://www.solveyour-tech.com/top-5-common-phone-viruses-know-one/

[5] BLAU, John. 'Skulls' Trojan attacks Symbian mobile phones. *Computerworld* [online]. [cit. 2018-04-28]. Dostupné z: https://www.computerworld.com/article/2568212/malware-vulnerabilities/-skulls--trojan-attacks-symbian-mobile-phones.html

[6] SMITH, Chris. Android malware earned a Chinese hacking group over $500,000 per day. *BGR* [online]. [cit. 2018-04-28]. Dostupné z: http://bgr.com/2016/06/30/android-hummer-trojan-malware/

[7] *Škodiace programy - MALWARE* [online]. , 3 [cit. 2018-04-28]. Dostupné z: http://www.spsske.sk/store/file/predmety/INFORMATIKA/6_%20V%C3%ADrusy.pdf

[8] BEAL, Vangie. Spyware. *Webopedia* [online]. [cit. 2018-04-28]. Dostupné z: https://www.webopedia.com/TERM/S/spyware.html

[9] Ransomware. *Avast* [online]. [cit. 2018-04-28]. Dostupné z: https://www.avast.com/cs-cz/c-ransomware

[10] Operating System: Operating system definition and examples of operating systems in use today. *Lifewire* [online]. [cit. 2018-04-28]. Dostupné z: https://www.lifewire.com/operating-systems-2625912

[11] *Operačné systémy* [online]. , 20 [cit. 2018-04-28]. Dostupné z: http://mirectu.kvalitne.cz/studium/OS/os.pdf

[12] CALLAHAM, John. The history of Android OS: its name, origin and more. *Android Authority* [online]. [cit. 2018-04-28]. Dostupné z: https://www.androidauthority.com/history-android-os-name-789433/

[13] About the Android Open Source Project. *Android Open Source Project* [online]. [cit. 2018-04-28]. Dostupné z: https://source.android.com/

[14] Structure of an Android Operating System. *EDUCBA* [online]. [cit. 2018-04-28]. Dostupné z: https://www.educba.com/structure-of-an-android-operating-system/

[15] Platform Architecture. *Android Developers* [online]. [cit. 2018-04-28]. Dostupné z: https://developer.android.com/guide/platform/#hal

[16] Android - Architecture. *Tutorialspoint* [online]. [cit. 2018-04-28]. Dostupné z: https://www.tutorialspoint.com/android/android_architecture

[17] HILL, Simon. Android vs. iOS: Which smartphone platform is the best?. *Digital Trends* [online]. [cit. 2018-04-28]. Dostupné z: https://www.digitaltrends.com/mobile/android-vs-ios/

[18] NATIONS, Daniel. What Is the iPhone OS (iOS)?: iOS Is the Operating System for Apple's Mobile Devices. *Lifewire* [online]. [cit. 2018-04-28]. Dostupné z: https://www.lifewire.com/what-is-ios-1994355

[19] Mobile Operating System Market Share Worldwide. In: *Statcounter Global Stats* [online]. [cit. 2018-04-28]. Dostupné z: http://gs.statcounter.com/os-market-share/mobile/worldwide/#monthly-201801-201801-bar

[20] Tablet Operating System Market Share Worldwide. In: *Statcounter Global Stats* [online]. [cit. 2018-04-28]. Dostupné z: http://gs.statcounter.com/os-market-share/tablet/worldwide/#monthly-201801-201801-bar

[21] The Android software stack. In: *Android Developers* [online]. [cit. 2018-04-28]. Dostupné z: https://developer.android.com/guide/platform/images/android-stack_2x.png

[22] KAPUSTA, Matúš. 10 dôvodov, prečo je Android stále lepší ako iOS. In: *MôjAndroid* [online]. [cit. 2018-04-28]. Dostupné z: https://www.mojandroid.sk/10-dovodov-android-lepsi-ios/

[23] IOS vs Android : Pros and Cons | Which one is best?. In: *Android Authority* [online]. [cit. 2018-04-28]. Dostupné z: https://www.androidauthority.com/community/threads/ios-vs-android-pros-and-cons-which-one-is-best.48864/

[24] The History of iOS, from Version 1.0 to 11.0: iOS history and details about each version. In: *Lifewire* [online]. [cit. 2018-04-28]. Dostupné z: https://www.lifewire.com/ios-versions-4147730

[25] HEATH, Alex. A look back at how far the iPhone's software has come. In: *Business Insider* [online]. [cit. 2018-04-28]. Dostupné z: http://www.businessinsider.com/the-history-of-ios-2016-6#it-also-combined-an-ipod-a-phone-and-an-internet-communicator-as-jobs-explained-3

[26] IOS – Architecture. In: *Intellipaat* [online]. [cit. 2018-04-28]. Dostupné z: https://tilakgondi.files.wordpress.com/2015/01/35f47-1.png

[27] About Developing for Mac. *Apple Developer* [online]. [cit. 2018-04-28]. Dostupné z: https://developer.apple.com/library/content/documentation/MacOSX/Conceptual/OSX_Technology_Overview/About/About.html#//apple_ref/doc/uid/TP40001067-CH204-TPXREF101

[28] Mobile & Tablet Android Version Market Share Worldwide. In: *Statcounter Global Stats* [online]. [cit. 2018-04-28]. Dostupné z: http://gs.statcounter.com/android-version-market-share/mobile-tablet/worldwide/#monthly-201801-201801-bar

[29] Znáte zálohovací pravidlo 3 - 2 – 1?. *Data Help* [online]. [cit. 2018-05-07]. Dostupné z: https://www.datahelp.cz/clanky/znate-zalohovaci-pravidlo-3---2-1

ZOZNAM POUŽITÝCH SYMBOLOV A SKRATIEK

RAM	**R**andom **A**cces **M**emory
CPU	**C**entral **P**rocessing **U**nit
SMS	**S**hort **M**essage **S**ervice
MMS	**M**ultimedia **M**essaging **S**ervice
OS	**O**peračný **S**ystém
AOSP	**A**ndroid **O**pen **S**ource **P**roject
HAL	**H**ardware **A**bstraction **L**ayer
ART	**A**ndroid **R**un**t**ime
DEX	**D**alvik **Ex**ecutable
SSL	**S**ecure **S**ockets **L**ayer
API	**A**pplication **P**rogramming **I**nterface
URL	**U**niform **R**esource **L**ocator
USB	**U**niversal **S**erial **B**us
SIM	**S**ubscriber **I**dentity **M**odule
PIN	**P**ostal **I**ndex **N**umber

ZOZNAM OBRÁZKOV

ZOZNAM PRÍLOH

PRÍLOHA P I: HW ŠPECIFIKÁCIA MOBILNÉHO TELEFÓNU LENOVO A7000

Veľkosť displeja	**5,5 " IPS LCD 1280 x 720 HD/WXGA**
Procesor	**Eight-core (1,5 GHz)**
Interná pamäť	**8 GB**
RAM	**2 GB**
Batéria	**2900 mAh**
Operačný systém	**Android 6.0 Marshmallow**

PRÍLOHA P II: ODPORÚČANÉ APLIKÁCIE PRE ZABEZPEČENIE OPERAČNÉHO SYSTÉMU ANDROID

Špecifické informácie o aplikáciách sa môžu odlišovať pre rôzne verzie operačného systému Android. V práci uvádzam informácie pre Android 6.0 Marshmallow.

Zoznam použitých aplikácií

- ESET Mobile Security & Antivirus
- NoRoot Firewall
- Malwarebytes Security: Virus Cleaner, AntiMalware
- Prehliadač Adblocker

ESET Mobile Security & Antivirus

Odkaz na stiahnutie	**https://play.google.com/store/apps/details?id=com.eset.ems2.gp**
Posledná aktualizácia ku dňu 11. 5. 2018	**10. 5. 2018**
Veľkosť	**21,18 MB**
Verzia	**4.0.41.0**
Vyžaduje Android	**4.0 a vyššie**
Dostupnosť	**Zdarma – možnosť zakúpenia premium verzie**

NoRoot Firewall

Odkaz na stiahnutie	**https://play.google.com/store/apps/details?id=app.greyshirts.firewall**
Posledná aktualizácia ku dňu 11. 5. 2018	**30. 11. 2014**
Veľkosť	**1 MB**
Verzia	**3.0.1**
Vyžaduje Android	**4.0 a vyššie**
Dostupnosť	**Zdarma**

Malwarebytes Security: Virus Cleaner, AntiMalware

Odkaz na stiahnutie	**https://play.google.com/store/apps/details?id=org.malwarebytes.antimalware**
Posledná aktualizácia ku dňu 11. 5. 2018	**11. 4. 2018**
Veľkosť	**72,25 MB**
Verzia	**3.3.0.6**
Vyžaduje Android	**4.1 a vyššie**
Dostupnosť	**Zdarma – možnosť zakúpenia premium verzie**

Prehliadač Adblocker

Odkaz na stiahnutie	**https://play.google.com/store/apps/details?id=com.hsv.freeadblockerbrowser**
Posledná aktualizácia ku dňu 11. 5. 2018	**5. 5. 2018**
Veľkosť	**122 MB**
Verzia	**60.0.3112.107**
Vyžaduje Android	**4.0 a vyššie**
Dostupnosť	**Zdarma – možnosť zakúpenia premium verzie**

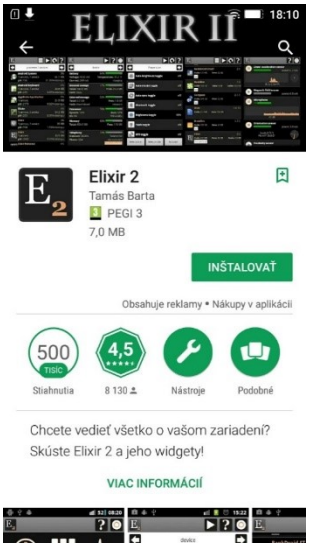
PRÍLOHA P III: PROGRAMY PRE TESTOVANIE VÝKONU A VÝDRŽE ZARIADENIA

Zoznam použitých aplikácií

- Elixir 2
- Geekbench 4
- Battery Monitor

Elixir 2

Odkaz na stiahnutie	**https://play.google.com/store/apps/details?id=com.bartat.android.elixir**
Posledná aktualizácia ku dňu 11. 5. 2018	**25. 3. 2018**
Veľkosť	**11 MB**
Verzia	**2.43.5**
Vyžaduje Android	**4.0 a vyšši**
Dostupnosť	**Zdarma (pre monitorovanie v reálnom čase) – možnosť zakúpenia premium verzie**



Geekbench 4

Odkaz na stiahnutie	**https://play.google.com/store/apps/details?id=com.primatelabs.geekbench**
Posledná aktualizácia ku dňu 11. 5. 2018	**3. 11. 2017**
Veľkosť	**96 MB**
Verzia	**4.2.0**
Vyžaduje Android	**5.0 a vyššie**
Dostupnosť	**Zdarma**

Battery Monitor

Odkaz na stiahnutie	**https://play.google.com/store/apps/details?id=com.glgjing.hulk**
Posledná aktualizácia ku dňu 11. 5. 2018	**11. 4. 2018**
Veľkosť	**1,5 MB**
Verzia	**6.4.0**
Vyžaduje Android	**2.3 a vyššie**
Dostupnosť	**Zdarma**