UNIVERZITA KONŠTANTÍNA FILOZOFA V NITRE

FAKULTA PRÍRODNÝCH VIED

BEZPEČNOSŤ MOBILNÝCH ZARIADENÍ

DIPLOMOVÁ PRÁCA

2017 **Bc. JAN FRANCISTI**

UNIVERZITA KONŠTANTÍNA FILOZOFA V NITRE

FAKULTA PRÍRODNÝCH VIED

BEZPEČNOSŤ MOBILNÝCH ZARIADENÍ

DIPLOMOVÁ PRÁCA

Študijný odbor: 9.2.9 Aplikovaná informatika
Študijný program: Aplikovaná informatika
Školiace pracovisko: Katedra informatiky
Školiteľ: PaedDr. Peter Švec, Ph.D.

Nitra 2017 Bc. Jan Francisti

Univerzita Konštantína Filozofa v Nitre
Fakulta prírodných vied

ZADANIE ZÁVEREČNEJ PRÁCE

Meno a priezvisko študenta: Bc. Jan Francisti
Študijný program: Aplikovaná informatika (Jednoodborové štúdium, magisterský II. st., denná forma)
Študijný odbor: 9.2.9 aplikovaná informatika
Typ záverečnej práce: Diplomová práca
Jazyk záverečnej práce: slovenský
Sekundárny jazyk: anglický

Názov: Bezpečnosť mobilných zariadení

Anotácia: Inteligentné telefóny a tablety bez ohľadu na použitý operačný systém obsahujú citlivé údaje, ktoré sa častokrát prenášajú dátovou sieťou na rôzne servery. Je otázne, či je tento prenos kontrolovateľný a s vedomím používateľa.

Ciele práce:
Cieľom práce je popísať jednotlivé platformy (Android, Windows a iOS) a zamerať sa na zachytenie a vyhodnotenie dátovej prevádzky vybraných zariadení. Odchytávanie prevádzky bude realizované pomocou kontrolovaného hotspotu. Očakávame, že zariadenia odosielajú údaje bez vedomia používateľa. Cieľom je teda tento predpoklad potvrdiť alebo vyvrátiť a zároveň zadefinovať prípadné opatrenia na zvýšenie bezpečnosti.

Požiadavky na vedomosti a zručnosti:
Podrobnejšie poznať problematiku bezpečnosti mobilnej platformy, schopnosť nakonfigurovať hotspot odchytávajúci sieťovú komunikáciu, schopnosť analyzovať odchytené sieťové spojenia

Školiteľ: PaedDr. Peter Švec, Ph.D.
Oponent: Mgr. Martin Cápay, PhD.
Katedra: KI - Katedra informatiky

Dátum zadania: 30.09.2015

Dátum schválenia: 14.10.2015 prof. Ing. Milan Turčáni, CSc.
schválil/a

POĎAKOVANIE

Touto cestou by som sa rád poďakoval školiteľovi PaedDr. Petrovi Švecovi, Ph.D. za cenné rady pri praktickej časti diplomovej práce, odbornú pomoc a konzultácie, ktoré mi poskytol pri jej spracovaní.

ABSTRAKT

FRANCISTI, Jan: Bezpečnosť mobilných zariadení. [Diplomová práca]. Univerzita Konštantína Filozofa v Nitre. Fakulta prírodných vied. Školiteľ: PaedDr. Peter Švec, Ph.D. Stupeň odbornej kvalifikácie: Magister odboru Aplikovaná informatika. Nitra: FPV, 2017. 72 s.

Inteligentné zariadenia, ako sú mobily a tablety sú každým dňom čoraz viac používanejšie v súčasnej komunikácii, v organizáciách rôznych typov. Počet týchto zariadení rapídne rastie a s ním vznikajú aj hrozby, ktoré rôznymi spôsobmi narúšajú ich funkčnosť. Predkladaná práca rieši problematiku bezpečnosti mobilných zariadení s výrobnými nastaveniami, pripojených do bezdrôtovej siete, kde je hlavným cieľom zistiť, či tieto zariadenia už pri svojom prvom pripojení do siete ohrozujú súkromie používateľa. Diplomová práca pozostáva z teoretickej a praktickej časti. Do teoretickej časti patrí analýza súčasného stavu, v ktorej sú bližšie popísané operačné systémy, ktoré sú najzastúpenejšie v súčasných mobilných zariadeniach. V praktickej časti diplomovej práce boli otestované zariadenia niekoľkých výrobcov s operačnými systémami iOS, Android a Windows. Bola vytvorená experimentálna bezdrôtová sieť ktorá mala za úlohu odchytiť všetku komunikáciu odchádzajúcu zo zariadenia. Poslednú časť práce tvorí vyhodnotenie použitých nástrojov, mobilných zariadení a ich operačných systémov, na ktorých pracujú, tiež výsledky činnosti zariadení po pripojení do siete. Z analýzy odchytených údajov vyplýva, že zariadenia pracujúce na platforme Windows Phone sú najbezpečnejšie. Pri platformách Android a iOS, ktoré sú aj najpoužívanejšie, preukazovali určitý stupeň ohrozenia, keďže automatický bez vedomia používateľa odosielali súkromné údaje.

Kľúčové slová: Mobilné zariadenie. Bezpečnosť siete. Operačný systém. Bezdrôtová sieť.

ABSTRACT

FRANCISTI, Jan: Mobile Device Security. [Diploma Thesis]. Constantine the Philosopher University in Nitra. Faculty of Natural Sciences. Supervisor: PaedDr. Peter Švec, Ph.D. Degree of Qualification: Master of Applied Informatics. Nitra: FNS, 2017. 72 p.

Smart devices such as mobile phones and tablets every day are increasingly more widely used in the current communication in organizations of various types. The number of these devices is growing rapidly and with it the threat generated by the various ways to interfere with their functioning. This work provide solutions of the security of mobile devices with factory settings connected to the wireless network, where the main purpose is to find out if these devices already at its first connection to the network threaten the privacy of the user. Diploma thesis consists of theoretical and practical part. In theoretical part it includes analysis of current situation, which are detailed operating systems that are most-represented in current mobile devices. In the practical part were tested several manufacturers devices with iOS, Android and Windows. The created experimental wireless network had has sought to capture all traffic outbound from the device. The last part of the thesis is assessed using tools, mobile devices and their operating systems on which they work, also the performance of the device after they are connected to the network. An analysis of the captured data indicates that devices operating on Windows Phone are the safest. Android and iOS platforms, which are the most used, demonstrating a certain degree of risk, given automatically without the user's knowledge dispatched private data.

Keywords: Mobile device. Network security. Operating system. Wireless networks.

OBSAH

ZOZNAM ILUSTRÁCIÍ A TABULIEK

ZOZNAM SKRATIEK A ZNAČIEK

AES	Advanced Encryption Standard
API	Application Programming Interface
ARP	Address Resolution Protocol
CMOS	Complementary Metal Oxide Semiconductor
CRM	Customer Relationship Management
DHCP	Dynamic Host Configuration Protocol
DNS	Domain Name System
DTLS	Datagram Transport Layer Security
GPS	Global Positioning System
HTPP/S	Hypertext Transfer Protocol /Secure
IP	Internet Protocol
MDM	Mobile Device Management
MFA	Multi-factor Authentication
OCSP	Online Certificate Status Protocol
OSI	Open Systems Interconnection
SQL	Structured Query Language
SSL	Secure Sockets Layer
SSO	Single sign-on
TCP	Transmission Control Protocol
TLS	Transport Layer Security
TPM	Trusted Platform Module
UDP	User Datagram Protocol
UID	Unique Identifier
VPN	Virtual Private Network
WNS	Windows Push Notification Services

SLOVNÍK POJMOV

Cache pamäť	Rýchla vyrovnávacia pamäť používaná procesorom počítača na zníženie priemernej doby prístupu do hlavnej pamäte.
Cloud storage	Model, na ktorý sa ukladajú údaje v logických skupinách, a fyzická časť modelu sa skladá z viacerých serverov.
Cookies	Malé množstvo dát, ktoré WWW server pošle prehliadaču, ktorý ho uloží na počítači užívateľa. Pri každej ďalšej návšteve toho istého servera potom prehliadač tieto dáta posiela späť serveru.
Firewall	Sieťové zariadenie alebo softvér, ktorého úlohou je oddeliť siete s rôznymi prístupovými právami a kontrolovať tok dát.
Hotspot	Miesto alebo zariadenie poskytujúce prístup do bezdrôtovej siete.
Jailbreak	Prekonanie obmedzení v počítačovom systéme, alebo v zariadení ako sú zariadenia spoločnosti Apple.
Kernel	Jadro, centrálny komponent väčšiny operačných systémov, ktorý má za úlohu zabezpečiť bežiacim programom prístup k hardvéru počítača.
Kryptoanalýza	Veda zaoberajúca sa metódami získavania obsahu šifrovaných informácií bez prístupu k tajným informáciám.
Rooting	Podobné pojmu Jailbreak, rozlišuje sa v tom, že ide prekonanie na telefónoch či tabletoch s operačným systémom Android.
Spyware	Počítačový program, ktorý sa bez vedomia užívateľa pokúša získať citlivé údaje z počítača.
SQL Injection	Bezpečnostná chyba založená na možnosti manipulovať s dátami v databáze bez nutnosti vlastníctva legitímnych prístupových údajov.

ÚVOD

Používanie smartfónov a ďalších mobilných zariadení je v súčasnosti natoľko rozšírené ako nikdy pred tým. Mnohí používatelia ešte teraz telefóny vnímajú rovnako ako pred desiatimi rokmi a neuvedomujú si, že smartfóny predstavujú malé počítače. Autor Guzman (2016) v článku o sledovaní aktivity mobilných zariadení hovorí, že používatelia tak majú v dispozícii moderné zariadenia a každodenne využívajú ich výhody. Pri používaní smartfónov často dostáva pohodlie používateľa prednosť pred zabezpečením zariadení a údajov v nich uložených.

Smartfóny a tablety bez ohľadu na použitý operačný systém obsahujú citlivé údaje, ktoré sa častokrát prenášajú dátovou sieťou na rôzne servery. Je otázne, či je tento prenos kontrolovateľný a s vedomím používateľa. Podľa štatistík (Alison, 2016), viac ako 89 % používateľov si neuvedomuje, že by ich telefón prenášal dôverné informácie o online platbách. Skoro dve tretiny používateľov sa obáva viac o bezpečnosť počítača ako o bezpečnosť mobilného zariadenia. Častými hrozbami bezpečnosti mobilných zariadení sú aj aplikácie, ktorých je dnes zverejnených a dostupných veľký počet a nevieme, čo všetko sa v nich skrýva. Vhodným opatrením podľa Computer Security Incident Response Team Slovakia (Csirt.sk, 2016) na predchádzaniu vzniku rizík môže byť použitý proces preverovania aplikácii, ktorý je zložený z dvoch častí: testovania a schvaľovania aplikácii. Aj napriek tomu, že známe firmy, ktoré majú na starosti obchody z aplikáciami ako sú Appstore (App Store, 2016) a Google Play (Google Play, 2016) a ktoré aj preverujú aplikácie, často sa stane, že sa im nepodarí odhaliť čo všetko aplikácia obsahuje.

Predkladaná diplomová práca sa zaoberá skúmaním bezpečnosti mobilných zariadení po pripojení do lokálnej siete a monitorovaním aktivity telefónov a ich činnosti. Pri monitorovaní sa vytvorí prístupový bod s možnosťou sledovania odoslaných paketov. Práca je rozdelená do dvoch častí.

V teoretickej časti sa zameriavame na platformy, na ktorých mobilné zariadenia fungujú, medzi ktoré patria iOS, Android a platforma Windows Phone. Ďalej uvedieme aktuálne hrozby s ktorými čelia jednotlivé platformy, tiež zabezpečenie ochrany telefónov.

V praktickej časti pomocou softvérových nástrojov vytvoríme prístupový bod, na ktorom budú pripojené mobilné zariadenia. Po pripojení zvolených telefónov do siete, otestujeme činnosť zariadení. Po otestovaní zariadení, analyzujeme jednotlivé pakety

a skúmame aké pakety sa odosielajú medzi zdrojom a cieľom. V poslednej kapitole vyhodnotíme výsledky získaných z testovania zariadení. Či zariadenia odosielajú informácie, ktoré by mali zostať iba v rámci zariadenia. Následne navrhneme metódy ako ochrániť súkromné informácie a ako sa treba zachovať po pripojení do voľnej bezdrôtovej siete, na čo si dávať pozor. Tiež uvedieme nástroje, ktoré napomáhajú poskytnúť anonymitu na internete a zabezpečujú bezpečnú komunikáciu.

1 ANALÝZA SÚČASNÉHO STAVU

Mobilné zariadenia často obsahujú alebo majú prístup k citlivým informáciám, ktoré by mal byť chránené. Používanie smartfónov prináša nové bezpečnostné rizika, ktoré by mal zvážiť každý používateľ, predtým ako na ňom pracuje s informáciami, ktoré sú nejakým spôsobom súkromné. V prvom rade je potrebné zabezpečiť, aby nedošlo k úniku údajov a to ani v prípade straty či odcudzenia telefónu. Taktiež je dôležité zabezpečiť, aby sa mobilné zariadenia nestali vstupnou bránou pri prieniku k ďalším informáciám, ktoré sú uložené na iných miestach, či už na počítačoch alebo v Cloude (Hevesi, 2016).

Kudakwashe (2015) uvádza že, postupom času sa mobilné zariadenia stali terčom všetkých typov útokov, ktoré existujú pre tradičné počítače a z dôvodu rizík aj cieľom nových hrozieb, špecifických iba pre mobilné zariadenia. Preto by mali byť mobilné zariadenia chránené ešte širšou skupinou bezpečnostných techník ako tradičné desktopy alebo notebooky. Bez ohľadu na to, aké sú hrozby a možnosti útokov.

1.1 Hrozby útočiace na mobilné zariadenia

Mobilné aplikácie dnes ponúkajú takú úroveň pohodlia, že si mnohé veci môžeme prostredníctvom internetu pozrieť kdekoľvek sa nachádzame, stačí na to iba telefón a pripojenie do internetu. Táto extrémna úroveň pohodlia so sebou prináša veľké množstvo bezpečnostných rizík, ako napríklad citlivé informácie z elektronického bankovníctva, heslá navštevovaných stránok, čísla platobných kariet a iné.

Na prvom mieste ide o nebezpečné ukladanie dát v telefóne. Keng-Boon (2016) podotýka, že nebezpečné ukladanie dát môže viesť k ich strate, či už v prípade nesprávneho zabezpečenia aplikácií alebo straty mobilného zariadenia. Ide o bežné údaje s ktorými používateľ každodenne pracuje, napríklad používateľské mená a heslá stránok, ktoré navštevuje alebo cookies webových stránok. Osobné údaje používateľa ako adresa bydliska, dátumy narodenie, sociálne údaje, kontakty ľudí a ďalšie. Taktiež sem patria aj údaje používaných aplikácii, ako rôzne záznamy aplikácii, nastavenia, história a správa cache pamäti.

Medzi ďalšiu hrozbu patrí slabá kontrola zo strany serveru. Servery, na ktorých sú uložené aplikácie by mali obsahovať bezpečnostné opatrenia, ktoré by znemožnili neoprávneným používateľom pristúpiť k údajom. Tvorcovia aplikácii by mali mať vlastné servery alebo servery iných firiem, ktoré ich prenajímajú a používajú opatrenia.

Existujú firmy, ktoré tieto služby poskytujú a ktoré okrem uskladnenia údajov poskytujú aj ich ochranu (CSSCorp, 2016).

Pri tvorení mobilných aplikácií dochádza k výmene údajov typom klient-server. K tejto výmene údajov prichádza prostredníctvom sieti operátora a internetu. Ak je aplikácia zle naprogramovaná a nie je dostatočne zabezpečená, prostriedky hrozby môžu použiť rôzne techniky na zobrazenie citlivých údajov, kým údaje prechádzajú sieťou. K úniku údajov môže dôjsť v sieti používateľa alebo na sieťovom zariadení, ktoré prepája používateľa s internetom (Yanrong, 2016).

Po stiahnutí a inštalovaní aplikácie, kód aplikácie je uložený na zariadenie používateľa. Na ten spôsobom môžu útočníci vytvoriť textový súbor do ktorého vsunú kód na vykonanie útoku. Útoky vsunutia, ako je SQL Injection na zariadení používateľa, môžu byť ťažké, ak aplikácia pracuje s viac ako jedným používateľským kontom na jednej aplikácii, so zdieľaným zariadením alebo s plateným obsahom. Ďalšie injekčné body sú určené na preťaženie zložiek aplikácie, ktoré nemajú takú veľkú úspešnosť vďaka spravovaným ochranám kódu aplikačných jazykov (Choras, 2013).

Kim (2015) uvádza, že aplikácie a systémy s nimi sa spájajúce, musia byť chránené autorizáciou a osvedčenými postupmi overovania. Tým sa zaistí, že zariadenie, používatelia a systémy, ktorí sú oprávnení k prenosu dát v aplikácii môžu pracovať a nepovolené zariadenia, používatelia a skripty sú identifikované a blokované.

Nevhodné sa správanie v priebehu relácie patrí tiež k hrozbám, ktoré môžu narušiť bezpečnosť. Niektoré aplikácie majú nastavený čas relácie a po vypršaný času sa jednotlivé okno aplikácie uzatvára a používateľ je prinútení reláciu zopakovať. Toto zabezpečenie by malo predísť ak by sa niekto iný dostál do zariadenia používateľa. Tieto postupy by mali byť zavedené pre všetky aplikácie, ktoré pracujú s citlivými údajmi (Tiago, 2016).

Pri navštevovaných stránkach, vstupy ako sú cookies, premenné prostredia a skryté časti formulárov používateľ nemôže zmeniť. Napriek tomu útočník ich dokáže meniť prostredníctvom špeciálneho klienta alebo určitým útokom. Útočník zmenu môže vykonať bez vedomia používateľa. Ak sa vykonávajú bezpečnostné rozhodnutia, ako je autorizácia či identifikácia na základe hodnôt týchto vstupov, môže útočník obísť zabezpečenie softvéru. Bez dostatočného šifrovania, kontroly integrity alebo iného mechanizmu je každý vstup, ktorý pochádza zvonku, považovaný za nedôveryhodný (Amerah, 2014).

V kryptografii sa útok postrannými kanálmi berie ako akýkoľvek útok, ktorý sa na rozdiel od klasickej kryptoanalýzy nesnaží nájsť nedostatky v štruktúre algoritmu, ale sa pokúša zneužiť informácie priamo z fyzickej implementácie systému počas behu šifrovacieho algoritmu. Sledovaním ako, kedy a kde sa dáta presúvajú môže útočník nájsť a využiť bezpečnostnú dieru.

Šifrovacie systémy sa neustále vyvíjajú, pretože sú neustále odhalené alebo prelomené. Používateľ by sa mal uistiť, že kryptografia, ktorú využíva je stabilná a doteraz nebola prelomená. Tento nedostatok môže byť detekovaný pomocou nástrojov a techník, ktoré vyžadujú manuálne ručné analýzy, ako sú penetračné testovanie, modelovanie hrozieb a interaktívne nástroje (Adli, 2016).

Medzi ďalšie zraniteľné miesto v bezpečnosti mobilných zariadení patrí zverejňovanie citlivých informácií. Ak budú aplikácie, systémy alebo kryptografické metódy vyvinuté alebo použité inými spoločnosťami napadnuté alebo prelomené, údaje každého používateľa budú v ohrození. Akonáhle sú časti týchto citlivých údajov sprístupnené, môžu byť použité na prelomenie iných databáz a systémov pre prístup k údajom.

Skenovaním dát na zraniteľnosť spôsobenú prienikom do iných aplikácií alebo spoločností môže používateľ získať ochranu pred rizikom (Mariantonietta, 2013).

1.2 Dôvody ohrozujúce bezpečnosť

Keď sa hovorí o bezpečnosti mobilných zariadení, väčšina mobilných zariadení sa nachádza v tej skupine, ktorá čaká na útok. Kvôli nedostatku bezpečnosti, mobilné zariadenia sa stávajú cieľom mnohým útočníkov. Každý rok sa počet útokov zväčší o viac ako 100% od minulého roku.

Mobilné zariadenia podľahli množstvu hrozieb, ktoré využívajú rad slabých miest, bežne sa vyskytujúcich v každom zariadení. Tieto chyby môžu byť dôsledkom nedostatočných kontrol, ale môžu aj vyplývať zo slabého zabezpečenia zariadenia. Výrobcovia telefónov sa snažia každou aktualizáciou čím lepšie zabezpečiť ochranu, ale aj napriek tomu, útočníci vždy pátrajú po zraniteľných miest platformy odkiaľ môžu vykonať útok. Avšak, bezpečnostné kontroly nie sú vždy dôsledne uplatňované na zariadeniach. Taktiež niektorí používatelia si nesú vedomí, že je dôležité umožniť bezpečnostné kontroly na zariadeniach a prijať odporúčané postupy (Cooney, 2012).

Najčastejším problémom je, že používatelia nemajú fyzický zabezpečený telefón. Pri starších mobiloch to bolo uzamknutie heslom, či už číselnou kombináciou alebo aj

pomocou kombinácie písmen. Tiež existuje voľba odmoknutia mobilu takým spôsobom, že si používateľ „nakreslí“ niečo na obrazovke a tým spôsobom ho odomkne. Pri novších modeloch, s ktorými sa stretávame aj dnes, majú v sebe zabudovanú biometrickú čítačku otlačku prsta pomocou ktorej môžeme odmoknúť zariadenie. Ďalej existuje aj odmoknutie hlasom, kde stačí aby mobil rozpoznal farbu hlasu používateľa. Taktiež niektorí používateľa zabúdajú na uzamknutie aplikácií, v ktorých sa nachádzajú citlivé údaje. Mnohí používateľa robia chybu pri voľbe hesla, lebo si zvolia rovnaké heslo ako napríklad hesla platobných kariet, pričom to útočník môže využiť pre ďalšie útoky. Alebo volia jednoduché hesla, ktoré nepredstavujú problém pre útočníka, z toho dôvodu aby mali zabezpečené zariadenie (Falconi, 2016).

Dvojfaktorová autentizácia nie je vždy používaná pri vykonaní citlivých operácií na mobilných zariadeniach. Debiao (2013) uvádza, že používatelia zvyčajne používajú statické heslá namiesto dvojfaktorovej autentizácie online transakcií. Použitie statických hesiel obsahuje niekoľko nedostatkov, útočník ich môže ľahko uhádnuť, používateľ ich môže zabudnúť, alebo môžu byť odchytené. Pričom dvojfaktorová autentizácia poskytuje vyššiu úroveň zabezpečenia než tradičné heslá. Táto autentizácia sa týka konkrétneho systému, v ktorom používateľ pracuje a používajú sa aspoň dva rôzne faktory a prevažne ide o veci, ktoré nejakým spôsobom súvisia s používateľom. V mobilných zariadeniach môžu byť použité ako druhý faktor v niektorých systémoch. Môžu byť náhodne generované alebo zastlaté prostredníctvom textovej správy.

Ďalším problémom je, že bezdrôtové prepojenia k WiFi nie sú vždy šifrované. Dôsledkom je napríklad odosielanie e-mailu, ktorý si môže útočník ľahko prečítať vrátene používateľského mena a hesla. Existuje veľa aplikácií, ktoré neimplementujú šifrovanie dát, ktoré sú vysielané a prijímané cez sieť a tým spôsobom môžu byť zachytené útočníkom. Pokiaľ aplikácia pre prenos dát nepoužíva protokol https, ktorý je šifrovaný ale iba http, údaje môžu byť ľahko odchytené.

Po pripojení do nezabezpečenej sieti, môže používateľ zanechať svoje osobné údaje zariadenia, kde môže byť ohrozený krádežou identity. Tiež sa môže stáť obeťou útoku man-in-the-middle, kde sa útočník nachádza uprostred komunikácie používateľa so sieťou a odchytáva celú komunikáciu. (Bicakci, 2014).

V mnohých aplikáciách, ktoré používateľ stiahne sa môže nachádzať malware. Malware môže byť ukrytý v údajoch aplikácie a používateľ po stiahnutí nemusí ani vedieť čo všetko stiahol s aplikáciou. Malware sa často ukrýva za aplikáciami ako sú

rôzne nástroje na zrýchlenie telefónu alebo hier a používateľ nemá potuchu či ide o legitímnu aplikáciu alebo o škodlivý softvér. Tento malware sa aktivuje prostredníctvom stiahnutej aplikácii a následne môže odchytávať činnosť telefónu a následne posielať zachytené údaje na zvolené úložisko (Shabtai, 2014).

Mobilné zariadenia často nepoužívajú bezpečnostný softvér. Mnohé platformy v svojich vopred inštalovaných aplikáciách takýto nástroj neobsahujú, ktorý slúži na ochranu pred škodlivými aplikáciami, spywarom a malwareom. Taktiež málokedy si používatelia podobný nástroj nainštalujú, lebo si myslia že ich zariadenie nástroj už obsahuje. Na Obrázku 1 sa nachádza zoznam najpoužívanejších nástrojov na zvýšenie bezpečnosti mobilných zariadení. Aj napriek tomu, že tieto nástroje môžu spomaliť činnosť zariadenia a znížiť výdrž batérie, na druhej strane ochránia mobil pred mnohými útokmi a tým znížia riziko ohrozenia údajov.

Obrázok 1 Najpoužívanejšie bezpečnostné nástroje pre Júl 2016[1]

Častokrát sú na mobilných zariadeniach staré verzie operačných systémov. Tým pádom mnohé bezpečnostné záplaty alebo opravy nie sú inštalované a existuje väčšie riziko útoku. Mnoho používateľov ignoruje správy, že je vydaná nová aktualizácia platformy a trvá aj niekoľko týždňov alebo aj mesiacov kým si ju používateľ nainštaluje. Tiež napríklad pri platforme ako je Android na ktorej pracujú telefóny viacerých výrobcov a tiež môže potrvať keď vývojári vytvoria novú aktualizáciu pre každého výrobcu. Po výrobe novej aktualizácie, musí byť najprv otestovaná. Ten proces tiež trvať dlhšie kým príde po konečného používateľa čo tiež zväčšuje riziko. Ďalším problémom aktualizácie môže byt starosť zariadenia. Napríklad telefóny pracujúce na platforme Android a ktoré sú staršie ako jeden rok, nemusia už byť podporované a ich majitelia sa nedočkajú aktuálnych aktualizácií.

[1] Zdroj obrázku 1: https://www.av-test.org/en/antivirus/mobile-devices/

Pri neaktualizovanej platforme, sa častokrát neaktualizujú aj aplikácie, čoho dôsledkom je nenainštalovanie bezpečnostných záplat. Mnoho aplikácií neobsahujú možnosť informovania používateľa o vzniku novej verzie aplikácie. Ďalším problémom je, že pri mobilných zariadeniach, webové prehliadače sú už vopred inštalované a aktualizujú sa spolu s operačným systémom, čo tiež predstavuje hrozbu (Dar, 2014).

Mnohé mobilné zariadenia neobsahujú možnosť obmedzeného pripojenia k internetu. Taktiež mnohé zariadenia neobsahujú firewall, ktorý obmedzuje pripojenie. Ak je zariadenie pripojené do rozsiahlej sieti využíva komunikačné porty pre pripojenie aj s inými zariadeniami. To útočníkovi umožňuje získať prístup do telefónu cez nezaistený port. Brána firewallu zabezpečuje také porty a umožňuje používateľovi voľbu spojenia. Bez použitia firewallu telefóny môžu byť otvorené cez nezaistené komunikačné porty a umožniť útočníkovi prienik (Ping, 2013).

Veľakrát sa na mobilných zariadeniach vykonávajú nepovolené modifikácie zo strany používateľov. Proces modifikácie zariadenia odstraňuje niektoré obmedzenia aby si používateľ mohol pridať rôzne funkcie. Pri telefónoch výrobcu Apple ide o *Jailbreak* a pri platforme Android o *Rooting*. Tieto funkcie umožňujú prístup ku kernelu operačného systému, aby umožnili montáž neautorizovaných funkcii alebo aplikácií. Na jednej strane to používatelia robia aby si inštalovali určité vylepšenia ako je firewall a iné a na druhej strane čelia k zvýšenému bezpečnostnému riziku. Tiež zariadenia, ktoré vlastnia túto funkciu nemusia dostávať informáciu o aktualizáciu softvéru a dodatočne zvyšujú riziko útoku (Jayaprakash, 2015).

1.3 Zvýšenie bezpečnosti mobilných zariadení

Každoročne pribúdajú informácie o útokoch na mobilné zariadenia. Bezpečnostný experti neustále varujú, že sa telefóny stávajú čoraz väčším magnetom pre vykonávanie útokov. Telefóny sa stáli zariadenia, ktoré sú úzko spätá s používateľmi, lebo pomocou nich sa vykonajú každodenné činnosti, od surfovania na internete a čítania mailov až po platenie v obchode. Tieto činnosti lákajú útočníkov, aby sa dostali po citlivé údaje nachádzajúce sa v telefónoch. Aby sa počet útokov znížil na minimum, existuje množstvo jednotlivých krokom, ktoré napomáhajú výrazne zvýšiť bezpečnosť (Lastovka, 2016).

Jeden z najjednoduchších riešení je fyzické zabezpečenie telefónu. Každý výrobca ponúka možnosť uzamknutia telefónu. Ako sa vyvíjali telefóny, vyvíjali sa aj riešenia uzamkýnania mobilných zariadení. Najprv to bolo klasické uzamknutie, kde sa

od používateľa vyžadovalo heslo. Neskôr vyšli na trh zariadenia, ktoré už v sebe obsahovali senzor na odomknutie pomocou odtlačku prsta. Najnovší trend, ktorý by sa mal nachádzať v telefónoch už v roku 2017 je CMOS senzor, ktorý má schopnosť detektovať dúhovku používateľa a na ten spôsob odomknúť telefón. Tento senzor vyvíja spoločnosť *Xintec* a podľa ich predpovedí, senzor by sa mal už nachádzať v budúcom modeli telefónu iPhone od firmy *Apple* (Shen, 2016).

Každý používateľ by si mal preventívne kontrolovať stav účtu na telefóne. Existujú rôzne paušály, pri ktorých používateľ platí koľko spotrebuje. Takéto paušály sú terčom pre útočníkov, kde pomocou textových správ, alebo telefónnych hovorov, infikujú telefón a môžu minúť veľké množstvo prostriedkov. Takéto útoky sa na mobilnom zariadení môžu prejaviť ako nezvyčajné sa správanie telefónu, textové správy a zmeškané hovory z neznámych čísel, podozrivé poplatky za telefónny účet, alebo náhly pokles baterky (Holmes, 2013).

Zálohovanie a zabezpečenie dát, je jedno z riešení ako ochrániť údaje, či už pred stratou telefónu, odcudzením alebo vymazaním. Pri zálohovaní sa vytvára kópia údajov z telefónu, kontakty, správy, nastavenia aplikácii, fotografie a ďalšie údaje. Používateľ ma možnosť zvoliť si, ktoré údaje chce zálohovať, tiež zvoliť si čas a ako často sa budú údaje zálohovať. Každý výroba už ponúka svoj program zálohovania dát, pri iOSe je to *iCloud*, pri Androide *GoogleDisk* a pri Winsows Phone *OneDrive*. Zálohovanie sa môže vykonať buď na počítač pri synchronizácii mobilu alebo do Cloudu. Existujú mnohé Cloudové aplikácie ktoré slúžia ako úschovňa údajov, ako sú *Dropbox* ale *Mega*. Dobrá vlastnosť týchto nástrojov, že sa môžu inštalovať aj na počítačoch a iných zariadeniach a uložené údaje sa môžu prezerať nie len na telefóne. Avšak pri zálohovaný údajov do Cloudu, by si mal používateľ zvážiť, ktoré dáta bude zálohovať. Tieto nástroje sú tiež častým terčom útočníkov, na ktoré tiež vykonávajú útoky, s cieľom získania údajov (Jatinder, 2016).

Pri inštalovaní aplikácií by si používateľ mal prečítať aký prístup schvaľuje, keďže ide o prístup k určitým častiam telefónu ako sú kamera, mikrofón, ale aj osobné údaje. Po schválení, aplikácia ma prístup k údajom a útočník ich môže prostredníctvom aplikácie prezerať. Pre lepšie zabezpečenie, by si mal používateľ v nastaveniach telefónu prezrieť aplikácie a skontrolovať, ktorá aplikácia ma ku ktorej časti prístup a v prípade podozrivej aplikácie, prístup k údajom zamedziť (Mariantonietta, 2013).

Dnes už skoro každé zariadenie v sebe obsahuje zabudovaný GPS lokalizátor, Bluetooth či WiFi kartu. Autor Goodrich (2012) hovorí, že pri ich nepoužívaný by nemuseli byť zapnuté a to z niekoľkých dôvodov. Zmenšujú výdrž baterky, pri opätovnom vyhľadávaní bezdrôtovej siete, alebo pri hľadaní GPS signálu v uzatvorenom priestore. Taktiež tieto funkcie sa môžu stáť aj vstupnou bránou pre útočníka. Prostredníctvom Bluetoothu sa môže útočník dostať do telefónu a prebrať nad ním ovládanie. Tiež by mal používateľ zvážiť pripojenie do neznámej verejnej WiFi siete, pre prípad ochrany osobných údajov.

Ďalším prvkom je ten, ktorý sa používa spolu s mobilným zariadením a ktorý mu obľahčuje prácu je NFC tag. Toto zariadenie slúži aby sa do neho nahrali určité správania telefónu v jeho blízkosti. Napríklad keď sa telefón nachádza v spálni, aby sa automatický vypol zvuk a podobne. Sú aj také zariadenia, ktoré obsahujú tlačidla a po stlačení sa napríklad odomkne telefón. Tieto zariadenia môžu byť zneužité od strany útočníkov prostredníctvom odcudzenia a následného použitia na odomknutie telefónu. Výrobcovia týchto zariadení radia používateľom, aby ich nepoužívali na verejných miestach kvôli ich zneužitiu (Wagoner, 2014).

Moderné mobilné zariadenia obsahujú možnosť strateného módu. Ide o funkciu, ktorá sa aktivuje v prípade straty a odcudzenia telefónu. Zariadenia obsahujú nastavenie vzdialeného ovládania. Toto ovládanie sa uskutočňuje prostredníctvom webového prehliadača, pomocou mobilnej siete alebo GPS signálu. Používateľ si môže zadefinovať, čo sa udeje s telefónom v prípade straty alebo odcudzenia. Existujú voľby ako vymazať všetky údaje, restovať telefón do továrenského nastavenia, vypísať kontaktné údaje v prípade vrátenia telefónu (Katina, 2013).

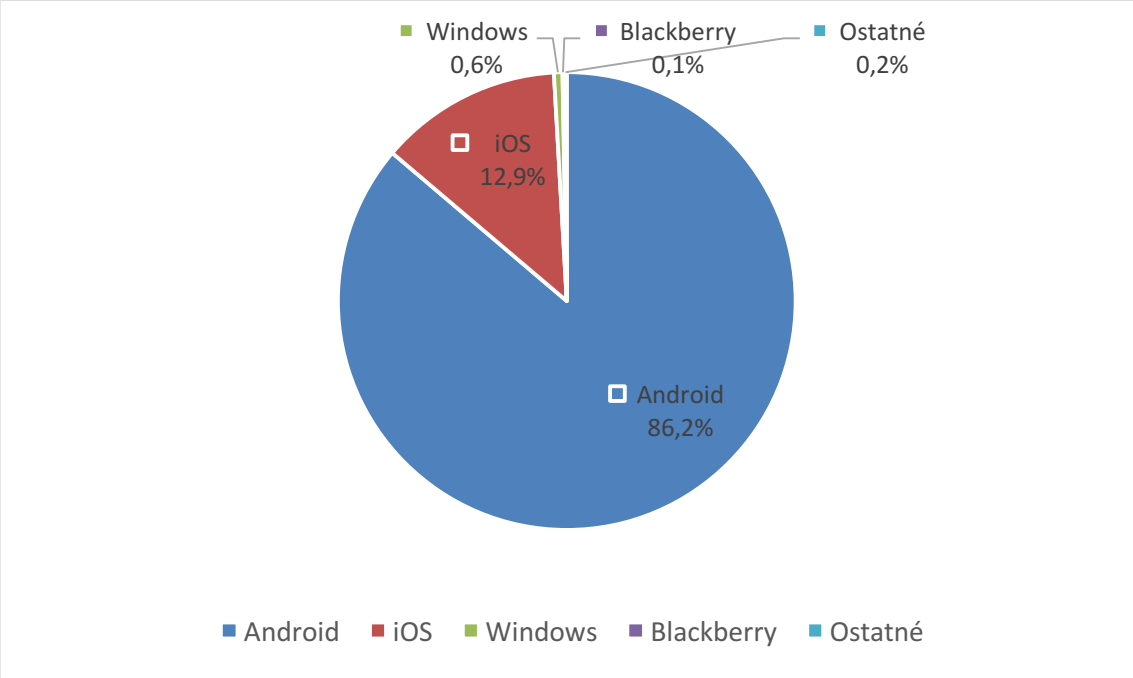
Vytvorenie viac používateľských účtov je ďalšie riešenie ako ochrániť zariadenie. Mnohí používatelia zdieľajú jedno zariadenie aj s ostatnými členmi a na ten spôsob ohrozujú svoje údaje. Používatelia ako sú deti, častokrát zoberú rodičom mobil či už na hranie hier alebo inú zábavu. V prípade, že aplikácie ako sú elektronické bankovníctvo alebo online obchody nie sú uzamknuté, mohlo by dôjsť do rôznych nepríjemných situácií. Vytvorením ďalšieho účtu si môže používateľ ustrážiť svoje súkromie a osobné údaje (Dzyre, 2016).

1.4 Operačné systémy pracujúce na zariadeniach

Posledné roky medzi najpoužívanejšie platformy mobilných zariadení jednoznačne patria iOS od spoločnosti Apple, Android od spoločnosti Google

a Windows Phone na ktorom pracuje Microsoft. Sú to tri operačné systémy, ktoré zastupujú celé trhovisko prenosných zariadení. Okrem telefónov, tieto platformy sa nachádzajú aj na tabletoch.

Každý rok tieto spoločnosti bojujú navzájom medzi sebou a to viacerých kategóriách. Ako prvé je to podiel zastúpenia platformy na trhu kde sú lídrami spoločnosti Apple a Google, čo môžeme vidieť aj na Grafe 1. Medzi ostatné operačné systémy patria rôzne distribúcie Linuxu, Symbian, ktorý sa používal pri starších telefónoch a ďalšie platformy na špecifické účely.



Graf 1 Zastúpenia platforiem na mobilných zariadeniach pre 2Q 2016[2]

Medzi ďalšiu kategóriu patrí bezpečnosť operačného systému, ktorú budeme testovať aj v praktickej časti práce. Každoročne sa dozvedáme o nových hrozbách, ktoré smerujú na mobilné telefóny a taktiež aj o nových nadstavbách operačných systémoch, ktoré zabezpečujú a zvyšujú bezpečnosť. Každá spoločnosť ma vlastné spôsoby ako zabezpečiť telefón. Keďže je Android najzastúpenejší medzi telefónmi, najviac útokov je zameraných práve na túto platformu.

Bates (2016) uvádza, že každá platforma má aj svoje výhody aj nevýhody keď ide o bezpečnosť. Zariadenia s najlepšou bezpečnosťou by bolo spojením niekoľkých zariadení do jedného. Vo svojom teste porovnal najzastúpenejšie značky mobilných

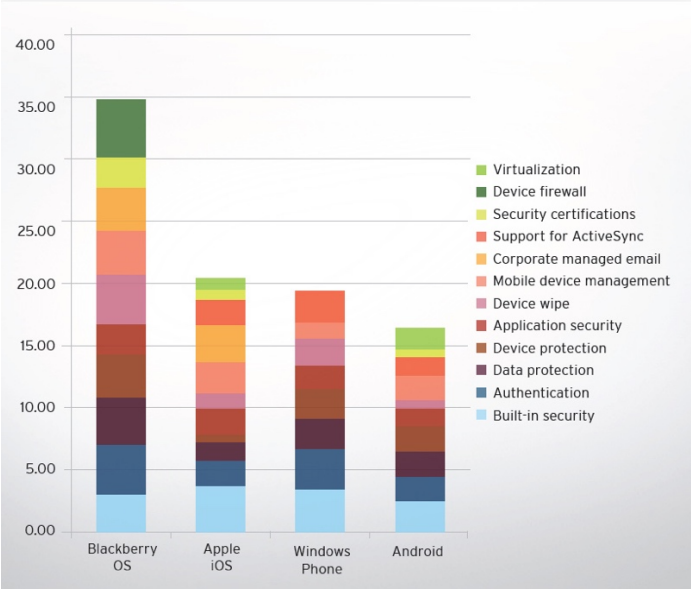
[2] Zdroj grafu 1: http://www.macprices.net/2016/08/21/five-of-top-10-worldwide-mobile-phone-vendors-increased-sales-in-q2-2016-gartner/

zariadení. Ako negatívne zhodnotil Android a iOS, kde pri sťahovaní môžeme stiahnuť aj rôzne škodlivé nástroje, ktoré môžu ohroziť bezpečnosť. Za bezpečné zariadenia zvolil staršie verzie od firmy BlackBerry a Ubuntu, ktoré nie sú až tak používané a ktoré majú dobre zaistenú bezpečnosť.

Ďalšie testovanie, ktoré boli vykonané firmou Mandalorian ukázali, že medzi bezpečné zariadenia patria aj telefóny, ktoré pracujú na operačnom systému Windows. Pri skúšaní bezpečnosti Windows sa ukázal ako najzložitejší na rozbitie (Pham, 2015).

Bezpečnostný model Windowsu je reštriktívny vo vnútri, kde pri každej novej verzii bol dobre zabezpečený. Veľkou výhodou Windowsu oproti iným platformám, ktoré obsahujú obchod z aplikáciami je to, že pri Windowse sú aplikácia testované reálnymi ľuďmi. Tiež sú aj vykonávané náhodné testy pre ďalších aktualizáciách aplikácie.

Na druhej strane keď hovoríme o platforme Windows, čoraz menej výrobcov kladie túto platformu do zariadení pričom táto platforma pomaly zaniká a tiež sa prestáva aktualizovať verzie. Na ten spôsob sa stáva ľahším terčom na zníženie bezpečnosti (Smartceo, 2016).



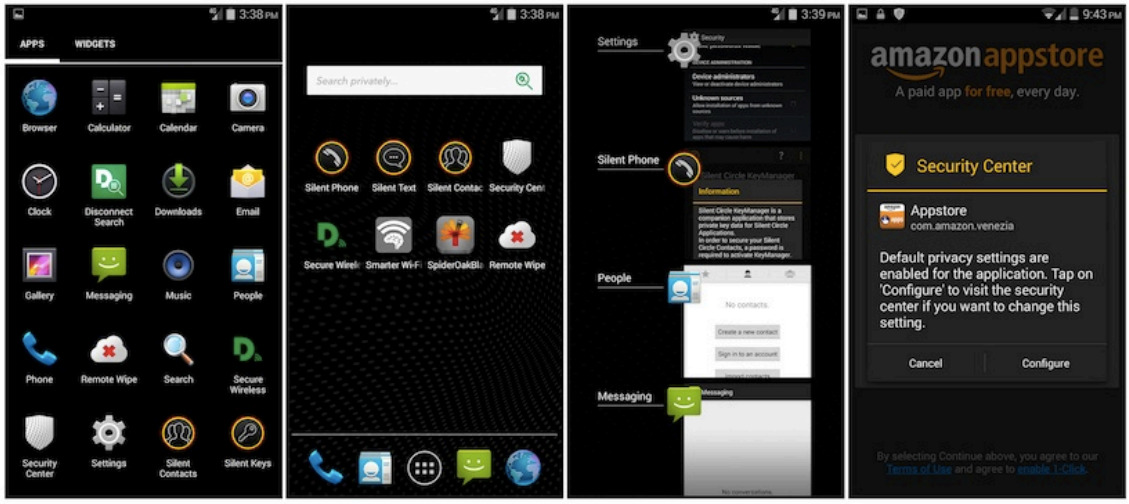
Graf 2 Porovnanie bezpečnosti operačných systémov[3]

Na Grafe 2 sú výsledky testu, ktorý realizovala spoločnosť Trend Micro, kde otestovala niekoľko mobilných zariadení. Na zariadeniach boli inštalované posledné verzia jednotlivých platforiem. Testované boli jednotlivé segmenty, ktoré zabezpečujú mobilné zariadenia. Patria tam napríklad firewall, bezpečnostné certifikáty, bezpečnosť

[3] Zdroj grafu 2: http://tech4tea.com/blog/2012/04/16/blackberry-os-vs-ios-vs-windows-phone-vs-android/

zabudovaných aplikácii, ochrana dát a iné. Aj pri tomto testovaní sa potvrdilo, že operačný systém firmy BlackBerry je najlepší pre používateľov z hľadiska bezpečnosti o čom svedčia aj číselné výsledky testu (Tech4tea, 2012).

Medzi najbezpečnejšie operačné systémy patria aj PrivatOS, ktorý je zabudovaný do zariadenia Blackphone. Bol navrhnutý roku 2014 a napísaný v jazyku C. Bol zameraný na používateľov, ktorí potrebovali zvýšenie súkromia a bezpečnosti. Platforma používa, šifrovanie pre telefónne hovory, e-maily, správy a prehľadanie internetu. PrivatOS bol upravená verzia Androidu 4.4.2, ktorej pracovné prostredie je zobrazené na Obrázku 2 a prišla so zväzkom bezpečnostných nástrojov. Avšak, na rozdiel od Androidu, PrivatOS nie je open source (Circle, 2016).



Obrázok 2 Používateľské rozhranie platformy PrivatOS[4]

1.4.1 iOS

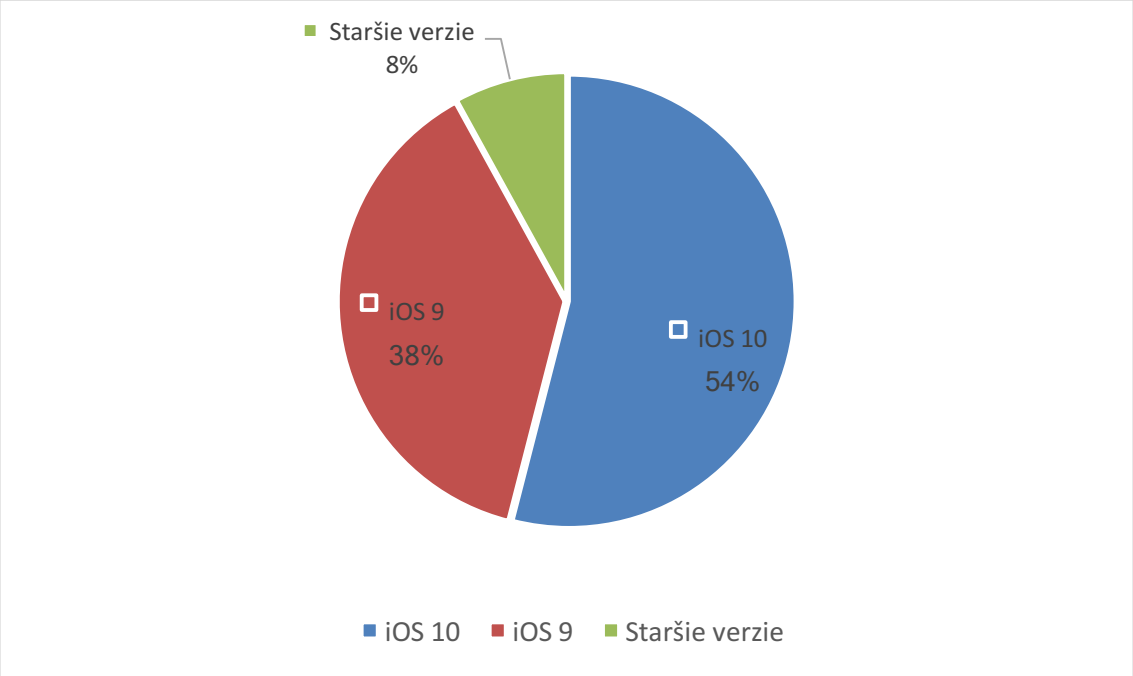
Platforma iOS je operačný systém od firmy Apple, ktorá pracuje za zariadeniach iPhone a iPad. Prvá verzia tejto platformy bola predstavená v roku 2007 spolu s prvým Appleovym telefónom. Bol to systém, ktorý vyvolal veľký rozruch kvôli svojmu jednoduchému a praktickému vzhľadu a tiež dobrému zabezpečeniu. Vývoj nových modelov zariadení sledovala aj každoročná aktualizácia systému a tento rok bola vydaná verzia 10 pri príležitosti nového iPhonu 7. Každá nová verzia platformy predstavuje nejaké vylepšenia, či už z hľadiska rýchlosti a optimalizácie. Tiež pridávanie nových funkcií, ktoré podporujú nové technológie ale aj zvýšenie bezpečnosti. Akonáhle sa vyskytnú nejaké systémové zranenia spoločnosť vydá novú

[4] Zdroj obrázku 2: http://pocketnow.com/wp-content/uploads/2014/08/blackphone-review-software-1.jpg

aktualizáciu, kde sú chyby opravené. Firma Apple podporuje ak program, kde ponúka peňažné odmeny pre ľudí, ktorí otestujú softvér a zistia nejaké chyby.

Na druhej strane existujú aj spoločnosti, ktoré zase ponúkajú finančné odmeny pre teamy ľudí, ktorým sa podarí odhaliť chyby na jadre systému a na ten spôsob odomknúť systém pre ďalšie softvérové rozšírenie a na ten spôsob odomknutie mnohých funkcií zariadenia, ktoré sa opierajú aj o bezpečnosť. Napríklad spoločnosť *Zerodium* ponúka sumu viac ako milión dolárov pre odomknutie verzie 10 (Hardwick, 2016).

Aktualizácia na novšiu verziu je zložená iba z niekoľkých krokov a väčšina používateľov si aktualizuje zariadenia hneď po vydaní novej verzie. Používateľ dostane oznámenie o aktualizácii pre iOS na zariadení alebo cez iTunes a aktualizáciu je možné vykonať aj bezdrôtovo. Na Grafe 3 môžeme vidieť, že viac ako polovica používateľov používa poslednú verziu operačného systému.



Graf 3 Podiel inštalovaných verzií platformy iOS[5]

Keď ide o bezpečnosť spoločnosť Apple ma to rozdelene do niekoľkých kategórii. Rozlišuje zabezpečenie systému, kryptovanie a ochranu údajov, bezpečnosť aplikácií, sieťová bezpečnosť a hardvérové zabezpečenie zariadenia.

[5] Zdroj obrázku 3: https://techcrunch.com/2016/10/11/according-to-apples-official-figures-ios-10-adoption-rate-now-at-54/

Každé zariadenie iOS kombinuje softvér, hardvér a služby, ktorých cieľom je pracovať spoločne pre maximálnu bezpečnosť a transparentné užívateľské skúsenosti. iOS nielen chráni zariadenie a jeho dáta, ale celý ekosystém, vrátane všetkého čo používateľ vykonáva nepripojený, na sieťach alebo s hlavnými internetovými službami. iOS a iOS zariadenia poskytujú pokročilé bezpečnostné funkcie a napriek tomu sú tiež ľahko použiteľné. Kľúčové bezpečnostné funkcie, ako šifrovanie zariadenia nie sú konfigurovateľné, takže používatelia nemôžu urobiť chybu (Apple, 2016).

Bezpečnostný systém je navrhnutý tak, aby oba softvér a hardvér boli v bezpečí naprieč všetkými hlavnými súčasťami každého zariadenia. To zahŕňa boot-up proces, aktualizácie softvéru a bezpečné enklávy. Táto architektúra je zásadná pre zabezpečenie v iOS a nikdy sa dostane do cesty použiteľnosti zariadenia. Každý krok v procese spúšťania obsahuje zložky, ktoré sú kryptograficky podpísané spoločnosťou Apple s cieľom zabezpečiť integritu a dovoliť postúpenie iba po overení dôvery. To zahŕňa bootloader, jadro, rozšírenie jadra a baseband firmware (Zibreg, 2014).

Roemmele (2013) uvádza, že *Secure Enclave* je koprocesor, ktorý je vyrobený v A-procesorom rade. Používa šifrované pamäte a obsahuje hardvér generátor náhodných čísel. *Secure Enclave* poskytuje všetky kryptografické operácie pre správu kľúčov pre ochranu údajov a udržuje integritu ochrane osobných údajov, aj keď by došlo k porušeniu jadra.

Bezpečný *boot chain*, podpisovanie kódu a zabezpečenie runtime proces, pomáhajú zaistiť, aby iba dôveryhodný kód a aplikácia mohli bežať na zariadení. iOS obsahuje ďalšie šifrovanie a ochranu dát, funkcie pre zaistenie používateľských dát. To poskytuje významné výhody pre používateľov a správcov IT, chrániaci osobné i firemné údaje za všetkých okolností a na poskytnutie metódy pre okamžité a úplné vzdialené vymazanie v prípade krádeže alebo straty zariadenia.

Na mobilných zariadeniach, rýchlosť a efektivita energie sú veľmi dôležité. Kryptografické operácie sú zložité a môžu zaviesť výkonnosť alebo životnosť batérie, pokiaľ kryptografia nebude správne navrhnutá. Každé zariadenie iOS má vyhradený AES 256 šifrovací engine vstavaný do cesty DMA medzi údajovou pamäťou a hlavnou systémovou pamäťou, aby šifrovanie súborov bolo vysoko efektívne. Ochrana dát je realizovaná výstavbou a správou hierarchie kľúčov a stavia sa na hardvérové šifrovanie technológií zabudovaných do každého zariadenia. Ochrana dát je riadená na základe

priradenia každého súboru k triede. Každá trieda používa rôzne zásady na určenie, kedy sú dáta prístupné (Sheldon, 2016).

Apple obsahuje aj nástroj *keychain*, ktorý slúži na zachovávanie hesiel, ako pri aplikáciách tak aj pri navštevovaných stránkach cez prehliadač. Výhodou nástroja je, že sa môže prenášať ako jeden súbor a je ho možné používať aj na iných zariadeniach, ktoré používajú rovnaký prihlasovací účet. Kľúče pre obe triedy ochrany údajov a Keychain sú zhromažďované a spravované nástrojom keybags. iOS používa nasledujúcich päť keybags, používateľ, zariadenie, zálohovanie, úschovy a iCloud zálohovanie (Burgess, 2014).

Existuje veľa sieťových bezpečnostných opatrení, pomocou ktorých organizácie môžu udržiavať dáta v bezpečí, pretože cestujú do a zo zariadenia. Používatelia pristupujú k sieťam odkiaľkoľvek na svete, takže je dôležité, aby sa zabezpečilo, že sú oprávnení a ich dáta sú chránené počas prenosu. iOS používa a poskytuje prístup k štandardným sieťovým protokolom pre overené, povolenie a šifrovanie komunikácie. Na dosiahnutie týchto cieľov zabezpečenia iOS integruje osvedčené technológie a najnovšie štandardy pre obe WiFi aj mobilné dátové pripojenie k sieti. Na iných platformách, je potrebný softvér na vytvorenie firewall. Vzhľadom k tomu, iOS dosahuje znížený počet útokov tým, že obmedzuje vypočúvacie porty a odstraňuje zbytočné sieťové nástroje, ako sú telnet, shells, alebo webový server (Apple, 2016).

iOS podporuje mechanizmy TLS a DTLS. Safari, Kalendár, Mail a ďalšie internetové aplikácie automaticky používajú tieto mechanizmy, ktoré umožňujú šifrovanie komunikačného kanála medzi zariadením a sieťovou službou. Zabezpečené sieťové služby, ako je VPN zvyčajne vyžadujú minimálnu inštaláciu a konfiguráciu pre prácu s iOS. Taktiež podporuje VPN na dopyte po sieťach, ktoré používajú overovanie na základe bezpečnostného certifikátu.

V dokumentoch o bezdrôtovom pripojení k sieti (Apple, 2012) uvádza, že platforma podporuje WiFi protokolov priemyselných štandardov, vrátane WPA2 Enterprise, na overenie prístupu k bezdrôtový sieťam. WPA2 Enterprise používa 128-bitové AES šifrovanie, čo umožňuje užívateľom najvyšší stupeň istoty, že ich dáta zostanú chránené pri odosielaní a prijímaní komunikácie cez pripojenie k sieti. S podporou 802.1x, IOS zariadenia môžu byť integrované do širokého spektra prostredí overovania RADIUS.

Počas pripojenia do bezdrôtovej siete podporovaná je aj autentizácia SSO. SSO spolupracuje so sieťami na základe protokolu Kerberos pre autentizáciu používateľov k službám, ktoré sú oprávnené na prístup. SSO je možné použiť pre celý rad sieťových aktivít, zo zabezpečených Safari relácií alebo aplikácií tretích strán.

Na prenos dát medzi zariadeniami Apple zahŕňa nástroj AirDrop. Na prenos sa používa buď Bluetooth alebo WiFi. Odoslaný údaj za *zahashuje* a môže ho prijať iba osoba, ktorá sa nachádza v kontaktoch odosielateľa. Ak sa nájde zhoda, odosielajúce zariadenie vytvára peer-to-peer sieť WiFi a inzeruje o výsadok pripojenia pomocou Bonjour. Použitím tejto súvislosti prijímacie zariadenia posielajú ich úplnú totožnosť hash iniciátorovi (Forrest, 2015).

1.4.2 Android

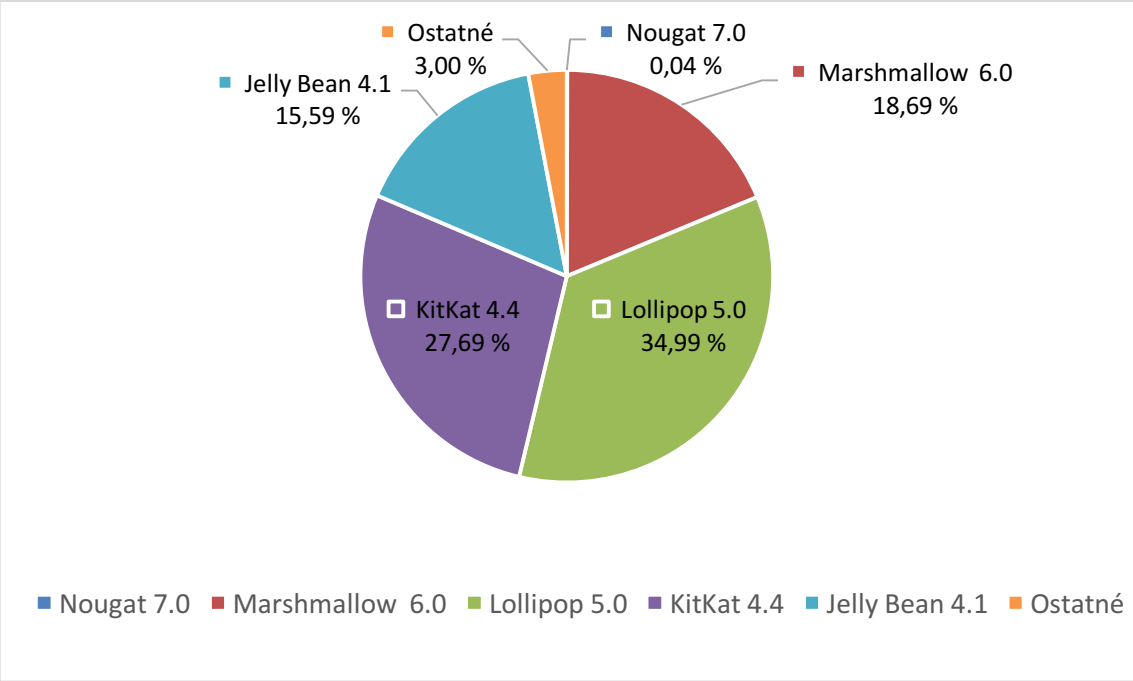
História platformy Android siaha do roku 2003, keď bola vytvorená ako start-upová firma. Následne ju v roku 2005 odkúpila spoločnosť Google a bola vytvorená aliancia s viac ako tridsiatimi spoločnosťami, ktoré mali na svojich telefónoch zabudovať túto platformu. V roku 2008 firma HTC vydala prvý telefón na ktorom pracoval operačný systém Android, ktorý bol založený na jadre Linuxu 2.6 a zároveň to bol prvý komerčný telefón, ktorý obsahoval Android platformu (Open Handset Alliance, 2007).

Následne tento operačný systém začalo používať viac výrobcov a keďže bola platforma pod open-source licenciu pre vývojárov, každý výrobca si prispôsoboval určité časti platformy na základe vyrábaného hardvéru. Tým pádom začal Google pretekať s spoločnosťou Apple o podiele trhu telefónov s príslušnými platformami, čo sa aj podarilo v roku 2010 a trvá aj dodnes, kde väčšina telefónov pracuje na Androide.

Taktiež, v roku 2010 Google vydala svoj vlastný telefón s názvom Nexus, ktorý bol vyrábaný spoločnosťami LG a Asus. Telefón sa vyznačoval nízkou cenou a dobrým výkonom a Google ho považovala za vlajkovú loď telefónu, ktorý pracoval na Androide na ktorom predstavila najnovší softvér a hardvér. Koncom roka 2016 vydali ďalšiu sériu telefónov pod označením Pixel, ktoré sú podobné telefónom Nexus aj z hľadiska hardvéru aj softvéru a konkurujú ostatným vedúcim spoločnostiam (Wray, 2010).

Podobne ako spoločnosť Apple aj Google každoročne na konferenciách predvádza nové verzie a vynovenia platformy Android kde uvádzajú rýchlosť stabilitu ale samotnú bezpečnosť systému. Posledná vydaná verzia bola 7.0 alebo Nougat a bola prístupná pre všetky telefóny, ktoré boli vyrobené po roku 2015. Celkový prehľad verzií

platformy Android je zobrazený na Grafe 4. Keďže novšie verzie platformy sú podporované iba pre novšie telefóny, mnohí používatelia zostávajú na starších verziách, ktoré sú náchylnejšie na útoky a sú terčom mnohých útočníkov.



Graf 4 Podiel inštalovaných verzií platformy Android[6]

Od vzniku prvej verzie Androidu, všetky zariadenia majú spoločný bezpečnostný model, ktorý zaisťuje každé zariadenie s bezpečným a izolovaným prostredím známym ako karanténa. Android predstavuje myšlienku izolovaného priestoru medzi zariadením a aplikáciami, kde chráni aplikácie pred útokmi a tiež časti hardvéru pred škodlivými aplikáciami. Pri všetkých aplikáciách na zariadení sa používa Sandbox, vrátane aplikácii na úrovni systému. Ide o základnú technológiu bezpečnostného systému. Android na identifikáciu a izoláciu používa Linuxové jadro. Ku každej aplikácii je priradené ID používateľa a je vykonávaná ako samostatný proces. V tomto sa Android líši od ostatným systémov, pretože pre každú žiadosť prideľuje nový proces a nové používateľské práva (Sims, 2012).

Časom sa tento model vyvíjal a začal sa používať SELinux, ktorý dokáže znížiť závažnosť rizík a zabezpečiť šifrovanie voľného priestoru na telefóne. S verziou 4.4 sa SELinux spojil s UID a vytvorila sa karanténa na úrovni jadra. Jadro vynucuje zabezpečenie medzi aplikáciami a systémom na úrovni procesu prostredníctvom štandardných linuxových zariadení, ako sú používateľské mená a skupiny, ktoré sú

[6] Zdroj grafu 4: https://developer.android.com/about/dashboards/index.html

priradené k aplikáciám. Všetok softvér nad jadrom, vrátane operačného systému knižníc, aplikačný framework a všetkých aplikácií bude prevádzkovaný v rámci svojej vlastnej aplikačnej karanténe. Vzhľadom k aplikačnej karanténe aplikácie majú prístup len k obmedzenému sortimentu systémových prostriedkov. Tieto obmedzenia sú implementované v mnohých rôznych formách. Niektoré možnosti sú obmedzené zámerným nedostatkom API k citlivým funkciám. V niektorých prípadoch, oddelenie rolí poskytuje bezpečnostné opatrenia, ako v prípade izolácie jednotlivých aplikácií. V iných prípadoch citlivé API sú určené pre použitie dôveryhodných aplikácií a sú chránené prostredníctvom bezpečnostného mechanizmu známeho ako oprávnenie (Android, 2016).

Ďalší nástroj, ktorý Android používa na zabezpečenie je *Verified Boot*, ktorý tiež obsahuje hardvérovo založený koreň dôvery a slúži na potvrdzovanie stavu každej fázy v procese spúšťania aplikácií. Pri štarte, Android varuje používateľa v prípade, že operačný systém bol zmenený z továrenského nastavenia verzii, poskytuje informáciu o varovaní, a ponúka riešenie na opravenie vzniknutej poruchy. V závislosti od vzniknutej poruchy používateľ bude mať voľbu či povolí štartovanie systému alebo aplikácie bez ohľadu na poruchu, alebo pozastaví spúšťanie, pokiaľ porucha nebude odstránená (Andorid, 2016).

Hoffman (2016) uvádza, že šifrovanie bolo predstavené vo verzii 3.0 a postupne sa vyvíjalo. Počnúc so systémom Android 5.0, bolo odporučené, aby výrobcovia povolili šifrovanie pre všetky zariadenia. S operačným systémom 6.0 zariadenia, ktoré používajú uzamknutie a majú AES šifrovací výkon nad 50MiB by mali vždy šifrovať súkromné dáta aplikácii a zdieľaného ukladania dát. Okrem toho sa požaduje, aby hlavné úložisko bolo šifrované za všetkých okolností. Android 6.0 tiež umožňuje výmenu pamäťového médiá, aj napriek tomu že je obsah na nich šifrovaní. Údaje o pamäťových kartách SD nedá čítať, pokiaľ je karta z iného zariadenia, alebo ako sú na karte nastavené iné šifrovacie pravidlá. Avšak pokiaľ je karta formátovaná vo formáte FAT32, aplikáciou ukladané údaje nie sú izolované.

Android v novej verzii pridalo do nastavenia položku Security patch level. Táto položka ukazuje dátum poslednej inštalovanej bezpečnostnej verzii a ponúka používateľom aby mali na zariadení inštalovanú aktuálnu verziu a na ten spôsob zabezpečili zariadenie pred útokmi. Android na stránke každý mesiac zobrazuje

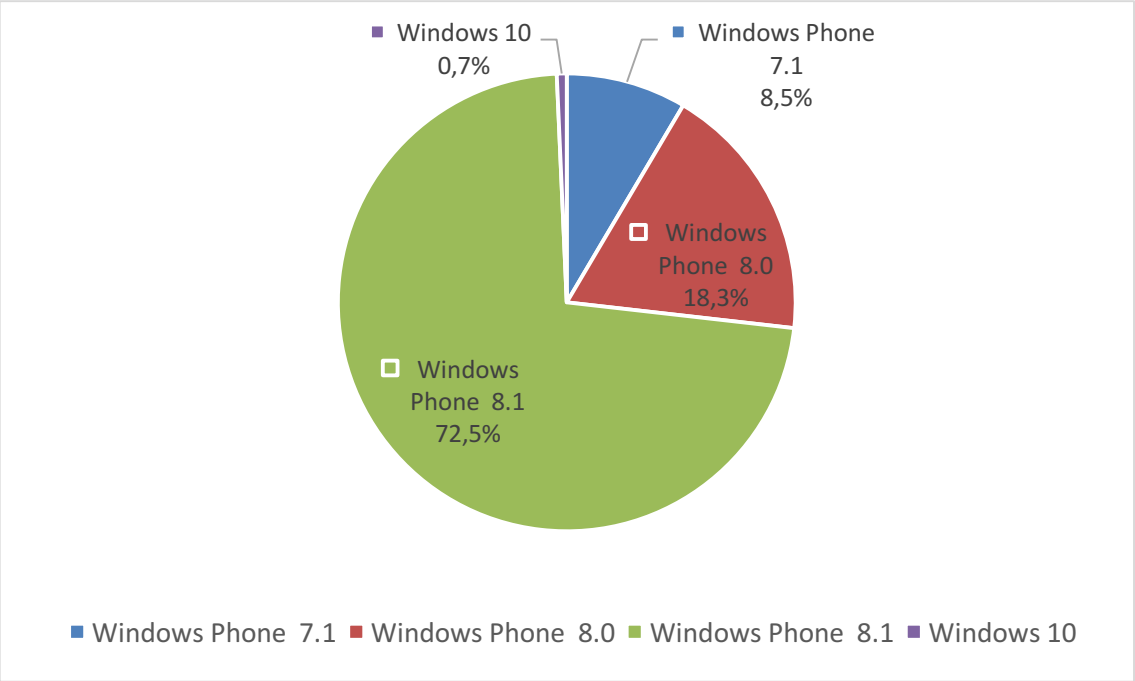
podrobnosti o bezpečnostných zraniteľností, ktoré ovplyvňujú zariadenia (Android, 2016).

Google do novších verzií taktiež pridáva funkciu "always-on VPN" kde budú mať používatelia možnosť byť stále pripojený prostredníctvom VPN a na ten spôsob si zachovať anonymitu na webe. Vedľa webu funkcia by mala spolupracovať aj so všetkými aplikáciami, ktoré majú prístup k internetu. Pokiaľ by došlo k prerušeniu VPN komunikácia by prestála a údaje by sa prestali odosielať (Sacco, 2016).

Pri verzii 6.0 používateľom nainštalované certifikáty nie sú už považované za dôveryhodné. Android bude používať iba jednu certifikačnú autoritu naprieč všetkými zariadeniami, takže výrobcovia nebudú môcť pridať ďalšie certifikáty v rôznych krajinách. To by malo zabezpečiť, že Android zariadenia budú mať rovnakú úroveň dôvery všade (Armasu, 2016).

1.4.3 Windows Phone

Spoločnosť Microsoft siaha svojou výrobou operačného systému pre mobilné zariadenia ešte do roku 1996, kde ho vyrábala pre vreckové počítače. Najprv to bola platforma pre PDA zariadenia, ktoré vyrábal Microsoft ale aj ďalší výrobcovia ako sú Asus, Dell, HP, Motorola a iné. Išlo o zariadenia, ktoré mali veľkosť telefónov ale fungovali ako počítače a aj platforma na ktorej pracovali sa podobala operačnému systému na počítačoch (Evers, 2005). Verzia 6.0 bola prvou verziou, ktorá mala podobu operačného systému pre telefóny a používala ju firma HTC. Následne túto platformu začala používať aj firma Nokia do svojej série mobilov Lumia, ktorú následne odkúpil Microsoft a dnes ju vyrába pod svojím menom. V roku 2010 Microsoft zmenil meno platformy na Windows Phone a začal vyrábať iba systém pre telefóny a tablety spolu si operačným systémom pre počítače, ktoré sú si podobné vzhľadom. V roku 2015 bola vydaná verzia 10, ktorá je aj aktuálnou verziou platformy a vlastní ju podľa Grafu 5, na ktorom sú zobrazené verzie platformy, iba 0,7 % používateľov. Podobne ako pri verziách na Androide aj pri Windows Phone, staršie telefóny nie sú podporované novším systémom a väčšina používateľov nevlastní aktuálnu verziu platformy (Savov, 2015).



Graf 5 Podiel inštalovaných verzií platformy Windows Phone[7]

Microsoft si svojím systémom nikdy neosvojil trh, aj napriek tomu že telefóny s týmto systémom boli lacnejšie oproti konkurentom a tak sa vždy dostál na nižšie percento na trhu vedľa Androidu a iOSu. Na druhej strane je Windows Phone bezpečnejší ako ostatné platformy o čom svedčia každoročné testovania firiem, ktoré sú zamerané na bezpečnosť platforiem. Napríklad spoločnosť Kaspersky uvádza, že Windows 10 je verzia, v ktorej sú sprísnené pravidla v bezpečnosti a tým robí platformu oveľa bezpečnejšou oproti ostatným (Bamburic, 2015).

Mobilné telefóny pomáhajú používateľom aby boli produktívnejší a výkonnejší, ale tieto mobilné zariadenia tiež vyžadujú zvýšenú bezpečnostnú ostražitosť. Preto aj Microsoft každou novou aktualizáciou platformy vylepšuje okrem iného bezpečnosť zariadenia. Windows Phone využíva najnovšie bezpečnostné hardvérové komponenty založené na štandardoch, ktoré pomáhajú chrániť zariadenia a informácie uložené na nich. Identita a riadenie prístupu sú základnou súčasťou bezpečnostného plánu akejkoľvek organizácie. Microsoft používa identifikáciu MFA s virtuálnymi čipovými kartami aby udržoval dôverné informácie v bezpečí (Microsoft, 2016).

UEFI je moderná, na štandardoch založené náhrada za tradičný BIOS. Implementácia UEFI umožňuje spustiť kontrolu na vnútornej integrite, na overenie digitálneho podpisu firmware pred jeho spustením. Tieto kontroly sa rozšíria na

[7] Zdroj grafu 5: http://www.slideshare.net/adduplex/adduplex-windows-phone-device-statistics-for

prípadné ďalšie ROM zložky na zariadení. Pretože len výrobca hardvéru zariadenia má prístup k digitálnym certifikátom UEFI chráni certifikát pred zneužitím.

Čip TPM je bezpečnostný procesor odolný proti neoprávnenej manipulácii, schopný vytvárať a chrániť šifrovacie kľúče a hodnoty hash. Okrem toho TPM môže digitálne podpísať dáta pomocou súkromného kľúča, od ktorých softvér nemôže získať prístup. Windows Phone používa čip TPM pre kryptografické výpočty a chráni kľúče pre šifrovanie BitLocker skladovania, virtuálnych čipových kariet a certifikátov (Lich, 2016).

Windows Phone používa niektoré z rovnakých technológií, ktoré vo verzii 8.1 využíva na zabezpečenie Boot procesu UEFI a jeho komponentov. Secure Boot je funkcia UEFI, ktorá pomáha chrániť zariadenie pred škodlivým softvérom alebo inej manipulácii v priebehu procesu spúšťania. Ako sme už spomínali Secure Boot overí, že vstup je dôveryhodný a potom následne Trusted Boot chráni zvyšok procesu spustenia overením, že všetky komponenty spusteného systému majú celistvosť a sú dôveryhodné. Ďalej overuje digitálny podpis jadra systému pred vložením. Jadro systému, potom overuje všetky ostatné súčasti procesu spúšťania systému, vrátane ovládačov a spustených súborov. Súčasti systému a aplikácií musia byť riadne podpísané pred načítaním systému. Ak sa útočník so zlými úmyslami alebo s manipulovaným kódom dostane neoprávnene do systému, zodpovedajúca súčasť alebo aplikácia nebudú načítané a spustené (Microsoft, 2015).

Vedľa bezpečnosti hardvéru a systému zariadenia, dôležite je ochrániť aj údaje uchované na zariadení. Windows Phone podporuje niekoľko technológií, ktoré pomáhajú chrániť tieto údaje. V novších verziách sa na šifrovanie používa technológia BitLocker a vnútorná pamäť je šifrovaná s AES 128-bitovým šifrovaním. To pomáha zaistiť, že dáta sú vždy chránené pred neoprávnenými používateľmi, aj po krádeži telefónu. Šifrovací kľúč je chránený s TPM aby bolo zabezpečené, že k údajom nemôžu pristupovať neoprávnení používatelia a to aj v prípade, že interné úložné médiá boli fyzicky odstránené zo zariadenia. Ako aj pri Androide aj Windows Phone ma vyriešené šifrovanie údajov aj na pamäťových kartách na zariadení kde aj po výmene karty, údaje zostávajú zašifrované. Útočníci bežne získajú neoprávnený prístup k informáciám odchytením nešifrovanej komunikácie medzi používateľom a druhou stranou. Windows Phone poskytuje niekoľko šifrovacích metód pre ochranu komunikácie medzi

zariadením a službami, ktoré spravujú údajmi. Ide o technológie TLS a SSL a pridávanie koreňových certifikátov do zariadení pre bezpečnostnú komunikáciu

Významné zlepšenie bezpečnosti v systéme Windows Phone 8.1 je podpora pre virtuálne čipové karty, ktoré sú založené na čipovej karty riešené priemyselným štandardom. Virtuálne čipovej karty emulujú funkčnosť tradičných čipových kariet, ale používajú procesor TPM na zariadeniach. Virtuálne čipové karty umožňujú používateľom používať dvojfaktorovú autentizáciu pri prístupe k prostriedkom a pracovať rovnako ako pri fyzické čipových kartách. V mnohých prípadoch používatelia môžu používať rovnaké virtuálne čipové karty na viactich zariadeniach Windows. Môžu ju používať aj pre bezpečné prezeranie a šifrovanie e-mailových správ.

Mnoho aplikácií a riešení vzdialeného pripojenia používajú certifikáty ako dodatočný faktor autentizácie a na podpis. Keď ide o pripojenie do bezdrôtovej sieti, pripojenie je šifrované podľa bežných štandardov WPA a WEP. Tiež je podporovaná aj autentifikácia EAP, ktorá vyžaduje certifikát inštalovaný na zariadení. V prípade nesprávného certifikátu nie je možné pripojiť sa do takejto sieti, čo zvyšuje bezpečnosť sieti.

Windows Phone taktiež podporuje aj pripojenie do privátnej siete pomocou VPN. Okrem poskytovateľov VPN Microsoft, podporované sú aj iné spoločnosti, ktoré zabezpečujú takýto typ pripojenia. Na zariadení je možnosť aby si používateľ inštaloval potrebný plugin pre pripojenie (Microsoft, 2014).

2 CIELE DIPLOMOVEJ PRÁCE

Hlavným cieľom diplomovej práce je otestovať mobilné zariadenia a ich dátovú prevádzku po pripojení do lokálnej siete. Ďalším cieľom je analyzovať získané pakety prostredníctvom zvoleného nástroja a vyhodnotiť činnosť jednotlivých mobilných zariadení.

Podciele:

- vyhľadať odborné a aktuálne zdroje k danej téme a rozpracovať ich obsah,
- vypracovať teoretickú časť práce s kompiláciou bibliografických zdrojov,
- zvoliť si funkčný nástroj na vytvorenie prístupového bodu,
- vykonať testovanie komunikácie mobilných zariadení so sieťou,
- analyzovať získané informácie z prístupového bodu,
- vyhodnotiť výsledky praktickej časti diplomovej práce.

3 METÓDY RIEŠENIA PROBLÉMU

Výrobcovia operačných systémov pre mobilné zariadenia si uvedomujú všetky riziká spojené s ochranou súkromia používateľa a do svojich operačných systémov zakomponovávajú stále novšie techniky ako toto súkromie chrániť. Problémom je, že mobilné zariadenia, ktoré sa dostávajú na trh majú tento operačný systém upravený rôznymi nadstavbami výrobcov mobilného zariadenia a je otázne, ako sa tieto nadstavby správajú pri zabezpečení súkromia používateľa. Našim cieľom je zistiť, aké údaje a kam prenáša mobilné zariadenie pri jeho prvom zapnutí a pripojení k internetu. Metodika testovania mobilného zariadenia pozostáva s nasledovných krokov:

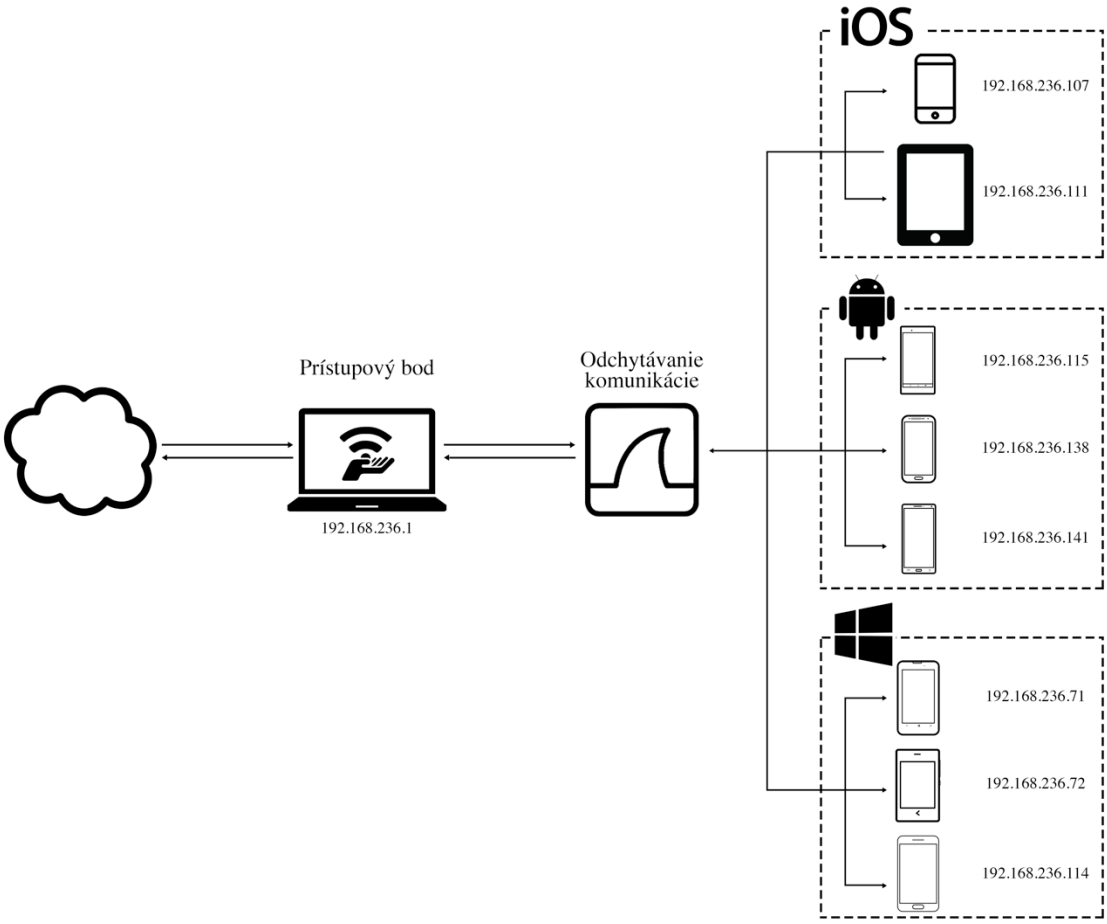
1. Zvoliť zariadenia na testovanie,
2. zatriediť testované zariadenia do skupín podľa operačného systému,
3. navrhnúť sieťové zapojenie jednotlivých zariadení,
4. vybrať nástroj na odchytávanie sieťovej prevádzky,
5. nastaviť mobilné zariadenia do výrobných nastavení,
6. odchytiť a uložiť odchytenú komunikáciu,
7. analyzovať a vyhodnotiť odchytenú komunikáciu.

3.1 Otestované mobilné zariadenia

Na úvod sme si stanovili, ktoré mobilné zariadenia budú otestované. Zariadenia sme si rozdelili do troch skupín na základe platformy na ktorej pracujú. Každé zariadenie pracovalo na inej verzii operačného systému a obsahovalo iba aplikácie, ktoré už boli vopred nainštalované. Zariadenie sme následne rozdelili do jednotlivých skupín na základe platformy na ktorej pracovali. Do prvej skupiny patrili zariadenia Apple a to iPhone 4S a iPad Mini. Zariadenia pracujúce na platforme Android, Samsung Galaxy Grand Prime, Sony Xperia Z1 Compact a Samsung J7. Tretiu skupinu tvorili zariadenia pracujúce na operačnom systéme od Microsoftu - Nokia 610, Samsung Ativ S a Microsoft Lumia 435.

3.2 Sieťové zapojenie zariadení

V ďalšom kroku sme použili nástroj, pomocou ktorého sme vytvorili prístupový bod, na ktorý sme následne pripájali jednotlivé zariadenia. Na porovnanie kvality pripojenia použili sme dva nástroje, ktoré sme inštalovali na dvoch rozdielnych operačných systémoch.



Obrázok 3 Sieťová topológia[8]

Na obrázku 3 je znázornené zapojenie jednotlivých komponentov – mobilné zariadenia, zariadenie na vytvorenie pripojenia do siete a nástroj, ktorý má poskytnúť odchytenie a analýzu komunikácie. Pre zaručenie komunikácie so sieťou sme potrebovali pripojenie k internetu. Keďže v učebniach univerzity sú bežné zariadenia ako sú prepínač a prístupový bod blokované nemohli sme ich použiť pri testovaní, keďže neumožnili aj pripojenie do internetu. Ako prístupový bod sme použili notebook, ktorý už bol pripojení v káblovej sieti, kde sme následne inštalovali nástroj, ktorý umožňoval vytvorenie hotspotu. Porovnali sme niekoľko nástrojov na operačných systémoch Windows a KaliLinux a ako najvhodnejší sa ukázal Connectify. Tento nástroj je bežne používaný na zdieľanie pripojenia a preto sme ho zahrnuli do testovania. Na operačnom systéme KaliLinux otestovali sme nástroj GhostPhisher, ktorý je už súčasťou tejto distribúcie Linuxu. Zistili sme, že pri dlhšom časovom intervale nástroj prestal

[8] Zdroj obrázku 3: Autor práce

fungovať a zariadenie bolo odpojené zo siete a z toho dôvodu sme následne používali iba nástroj Connectify.

3.2.1 Connectify

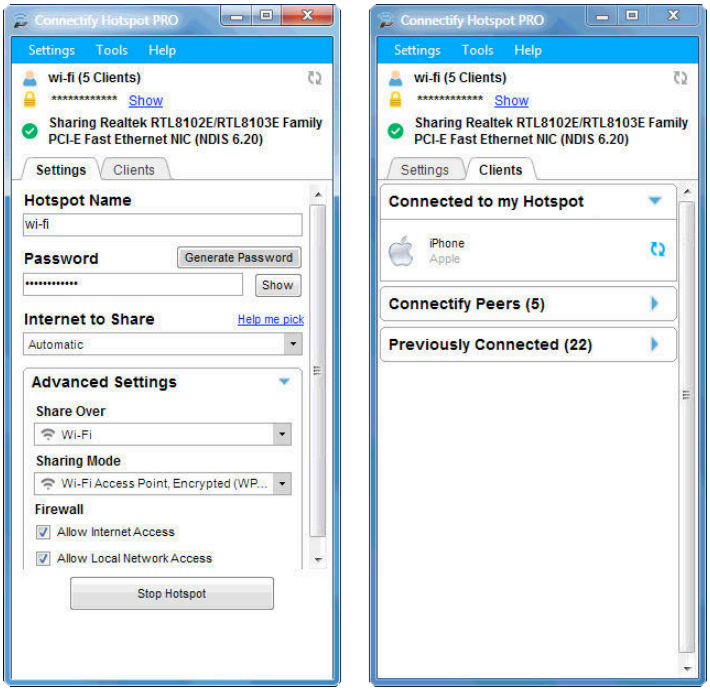
Connectify Hotspot je nástroj na pripojenie zariadení na WiFi hotspot a na zdieľanie internetu počítača medzi ostatnými pripojenými počítačmi. Je to nástroj, ktorý pomocou káblového pripojenia do internetu dokáže zdieľať pripojenie ďalej.

Okrem štandardného WiFi pripojenia nástroj ponúka aj vytvorenie 3G alebo 4G sietí. Vytvorené pripojenie je zabezpečené s WPA2 šifrovaním pre bezpečnostnú komunikáciu. Aktuálna verzia aplikácie obsahuje možnosť monitorovania prevádzky v reálnom čase a grafické zobrazenie informuje o množstve stiahnutých a odoslaných dát pre jednotlivé pripojené zariadenia (Connectify, 2017).

Tento nástroj sme použili na vytvorenie prístupového bodu, ktorý sme použili na otestovanie bezpečnosti zariadení. Inštalovali sme bezplatnú verziu aplikácie na operačnom systéme Windows 7. Inštalácia prebiehala v niekoľkých jednoduchých krokoch.

Týmto nástrojom sme vytvorili virtuálny prístupový bod, podobajúci sa skutočnému zariadeniu, ktorý ma totožné nastavenia a vlastnosti ako bežne používané zariadenie.

Ako pri bežnom prístupovom bode aj teraz bolo potrebné zvoliť si meno a heslo siete a typ šifrovania. Následne sme si zvolili káblové pripojenie, ktoré sme použili ako zdroj internetu. Ako vysielač sme použili externú sieťovú kartu aby sme zaistili stabilnejšie pripojenie. Po pripojení do siete v položky klienti, ktorú môžeme vidieť na Obrázku 4 sa zobrazilo pripojené zariadenie a odpočúvanie sme spustili v nástroji Wireshark. Tento nástroj nám poslúžil ako prepojenie zariadenia a nástroja na analýzu komunikácie.



Obrázok 4 Pracovné prostredie nástroja Connectify[9]

3.2.2 Ghost Phisher

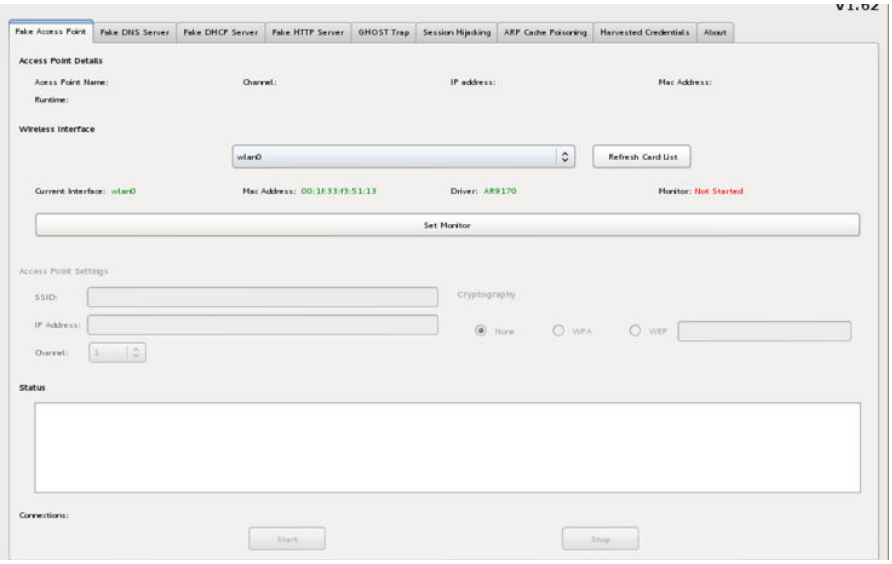
Ďalší nástroj, ktorý sme použili na vytvorenie prístupového bodu bol Ghost Phisher, ktorý sme otestovali na operačnom systéme KaliLinux. Ide o nástroj káblového a bezdrôtového bezpečnostného auditu určený na rôzne testovania siete. Aplikácia je napísaná v jazyku Python a nástroj je schopný simulovať prístupový bod. Okrem tejto funkcie nástroj podporuje aj vytvorenie HTTP, DNS a DHCP servera. Tiež na vytvorenie početných útokov ako sú ARP útok, metasploit alebo SQL Injection (Kali, 2014).

Keďže je nástroj už súčasťou operačného systému, nebolo potrebné ho inštalovať alebo konfigurovať. Nástroj sme zapli cez príkazový riadok príkazom *ghost-phisher*. Aplikácia obsahuje niekoľko kariet, zobrazených na Obrázku 5, v ktorých sú zaradené jednotlivé sieťové testovania. My sme použili položku Fake Acess Point, ktorá bola hneď prvá v poradí.

Ako prvé zvolili sme si sieťové rozhranie prostredníctvom, ktorého sme vysielali signáli na pripojenie do siete kde sa nám vypísali informácie o zvolenom rozhraní ako sú fyzická adresa, typ ovládača a monitorovací režim. Následne sme si zvolili meno a heslo bodu a spôsob kryptovania komunikácie. Tiež sme si zvolili aj kanál na ktorom bude pracovať prístupový bod odlišný od ostatných aby sa zaistila kvalita pripojenia. Po nakonfigurovaní bodu, stlačili sme tlačidlo štart a v okne status boli vypísane informácie, či

[9] Zdroj obrázku 4: Autor práce

bolo pripojené úspešne vytvorené a spustené a tiež informácie o pripojených zariadeniach. Ako aj pri nástroji Connectify, aj v tomto prípade sme ďalej pokračovali v analýze komunikácie v nástroji Wireshark.



Obrázok 5 Vytvorenie prístupového bodu v nástroji Ghost Phisher[10]

3.3 Odchytenie sieťovej prevádzky

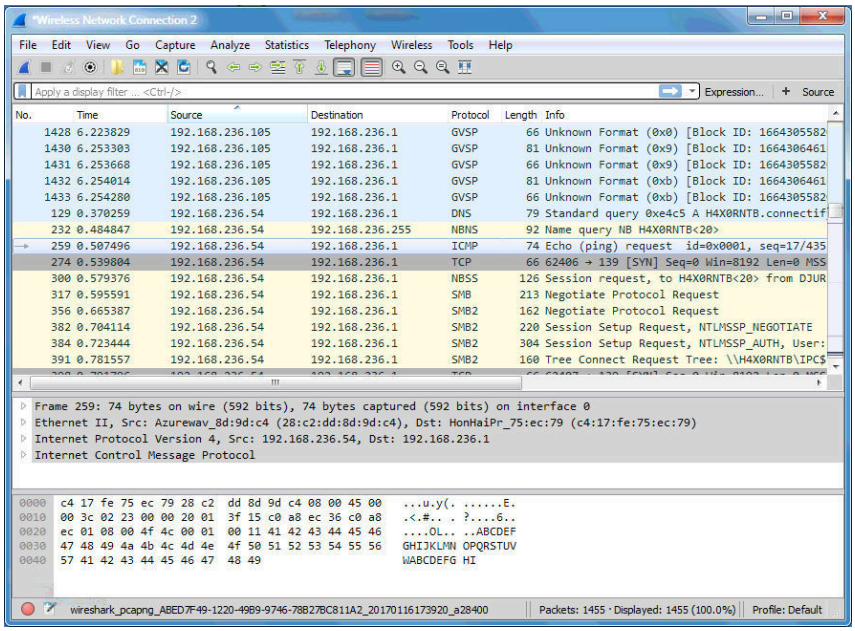
Po vytvorení prístupového bodu sme pripájali zariadenia do nami vytvorenej bezdrôtovej siete a sledovali ich správanie a činnosť pomocou nástroja určeného na analýzu a odchytenie komunikácie. Na odchytenie a analýzu dát použili sme nástroj WireShark. Ide o nástroj, ktorý dokáže po nastavení odsledovať celkovú komunikáciu pre nastavený sieťový adaptér. Zvolili sme si ho z toho dôvodu, že poskytuje priehľadnú analýzu paketov s rôznymi nastaveniami. Tiež obsahuje funkciu „Follow stream“, ktorá poskytuje detailnejšie a hlbšie nahliadnutie do jednotlivých paketov.

3.3.1 Wireshark

Po pripojení zariadenie do siete, použili sme nástroj WireShark s ktorým sme odsledovali komunikáciu a správanie sa zariadenia na sieti. WireShark je aplikácia, ktorá po pripojení do zvolenej siete umožňuje odpočúvanie sieťovej komunikácie. Dokáže odchytiť pakety prenášané sieťou a podporuje veľké množstvo sieťových protokolov, ktoré sa používajú. Za pomoci nástroj WireShark môže používateľ sledovať celú detailnú komunikáciu siete. Aplikácia poskytuje zobrazenie informácii o odchytených paketoch, podobne ako na Obrázku 6, rôzne štatistiky, ktoré sa môžu

[10] Zdroj obrázku 5: Autor práce

odfiltrovať. Nástroj umožňuje tiež exportovanie jednotlivých dát do štandardných formátov ako sú CSV alebo textový (WireShark, 2017).



Obrázok 6 Zoznam skenovaných paketov v nástroji WireShark[11]

3.3.1.1 Sieťové protokoly nástroja Wireshark

Wireshark v svojom prostredí zobrazuje zoznam odchytených paketov pri komunikácii zariadenia v sieti. Pri každom pakete sú rôzne parametre ako sú zdrojová a cieľová IP adresa, dĺžka paketu, bližší informácie o pakete ako aj druh protokolu. Protokol nám bližšie hovorí o aký paket ide. V zozname sa nachádzal protokol ARP, ktorý slúži na preklad IP adresy na adresu fyzickú. Ďalej sa nachádzal protokol DHCP, ktorý poskytoval IP adresu pre zariadenie pripojujúce sa do siete. HTTP protokol, ktorý transportuje dokumenty medzi serverovou a používateľskou službou WWW. Ktorý je zároveň primárny spôsob transferu informácii na internete.

TCP protokol slúži na vytváranie a udržiavanie sieťovej komunikácie, prostredníctvom, ktorej si aplikácie môžu vymieňať údaje. TCP spolupracuje s protokolom IP, ktorý definuje ako budú zariadenia odosielať pakety dát. Ide o protokol, ktorý je orientovaný na pripojenie, čo znamená že pripojenie je vytvorené a udržiavané pokiaľ sa na oboch koncoch nedokončí výmena správ, čiže poskytuje bezchybné spojenie. Umiestnení je medzi transportnou a relačnou vrstvou v OSI. TCP protokol používa porty, napríklad FTP, ktorý je pod číslom 21, Telnet 23, alebo HTTP 80 (Rouse, 2014).

[11] Zdroj obrázku 6: Autor práce

3.4 Analýza odchytenej komunikácie

Všetky otestované zariadenia sme nastavili do výrobných nastavení, z dôvodu aby sme čo najpresnejšie určili, ktoré pakety zariadenia odosielajú a na aké servery sa pripájajú. V nástroji WireShark sme si zvolili vytvorené pripojenie a odfiltrovali sme požiadavky, ktoré smerovali zo zariadenia do siete. Každé zariadenie sme otestovali zvlášť, kvôli lepšej prehľadnosti. Súbor s odchytenými paketmi sme následne zachovali pre ďalšiu analýzu.

Odchytené pakety smerované do internetu sme potom v nástroji analyzovali a porovnávali sme s ostatnými verziami platformy. Výsledky získané z praktickej časti sme interpretovali v nasledovnej kapitole.

3.5 Postup testovania zariadení

Pred samotným otestovaním správania sa zariadenia po pripojení do siete, každé použité zariadenie sme nastavili do továrenského nastavenia. To sme vykonali prostredníctvom nastavenia zariadenia v záložky reset. Išlo o proces, ktorý bol pomerné rovnaký pri všetkých platformách. Po resetovaní, zariadenie neobsahovalo nič okrem aplikácií, ktoré sú inštalované spolu s operačným systémom. Zariadenia sme resetovali z toho dôvodu aby sa pri odosielaní paketov nezobrazovali aj pakety aplikácií, ktoré boli inštalované neskôr, tým pádom sme mohli zistiť čo robí mobil, ktorý nebol pripojený do siete. Ďalší dôvod bol aby sa v pamäti nenachádzal uložený prístupový bod, ktorý sme použili na vytvorenie pripojenia. Po zapnutí zariadenia, najprv sme otestovali zariadenia bez prihlásenia. Neprihlasovali sme sa na Google účet pri Androide, resp. Microsoft alebo Apple pri iných platformách, aby sme zachovali anonymitu zariadenia. Následne sme otestovali aj zariadenia po prihlásení, pre porovnanie, či zariadenie poskytuje aj nejaké iné údaje o používateľovi.

Skôr ako sme vytvorili prístupový bod na počítači museli sme zaistiť aby bol počítač pripojení do siete prostredníctvom kábla. Počas testovania v učebniach na katedre informatiky, museli sme nastaviť fyzickú adresu totožnú z niektorým počítačom v učebni aby fungovalo pripojenie. Následne sme inštalovali nástroj pomocou ktorého sme vytvorili prístupový bod. Porovnali sme niekoľko nástrojov a z pohľadu stability použili sme nástroj Connectify. Tiež sme použili nástroj GhostPhisher na operačnom systéme Linux. Zistili sme, že nástroj GhostPhisher nebol stabilný a častokrát zrušil spojenie, tak sme pri väčšine zariadení použili Connectify. Inštalácia nástroja bola štandardná ako pri ostatných aplikáciách a nebolo potrebné nič dodatočne nastavovať.

Po naštartovaní nástroja museli sme byť pripojení do siete prostredníctvom kábla aby sme mohli pripojenie odosielať bezdrôtovo. Ďalej sme si zvolili bezdrôtovú sieťovú kartu, ktorá mala za úlohu odosielať signál a poskytnúť pripojenie pre zariadenie. Ako sieťovú kartu zvolili sme *TP-LINK TL-WN722N,* ktorú sme prepojili pomocou USB rozhrania. Zvolili sme si preto, lebo v porovnaní so zabudovanou sieťovou kartou mala vyšší výkon a lepšie pripojenie. Tiež bolo potrebné nastaviť meno, heslo a spôsob šifrovania komunikácie. Po nastavení parametrov, nástroj sme mohli spustiť.

Keď nástroj Connectify bol aktívny, naštartovali sme nástroj Wireshark. Ako prvé pozreli sme si na ktorom rozhraní bežala komunikácia, v našom prípade to bolo pripojenie *Wireless Network Connection 2*, pripojenie, ktoré sme si vopred vytvorili. Zvolili sme si pripojenie a stačili na tlačidlo na spustenie odchytávania. Nástroj začal zachovávať všetky pakety, ktoré boli prenášané cez naše pripojenie.

Po naštartovaní nástroja a keď sme si overili jeho správnosť fungovania, pripojili sme zariadenie do siete. Aby sme mali lepší prehľad medzi paketmi na sieti bolo pripojené iba testované zariadenie. Keďže zariadenie bolo resetované a na továrenskom nastavení, pripájalo sa do novej siete takže bolo potrebné zadať zadefinované heslo. Keď DHCP server pridelil IP adresu zariadeniu, čo sme videli aj v hlavnom pracovnom okne a zariadenie sa pripojilo do siete, začal sa zväčšovať počet paketov a na ten spôsobom sme zistili, že je zariadenie korektne pripojené. Aby sme získali iba informácie o tom, čo zariadenie robia bez nášho vedomia, neinštalovali sme žiadne dodatočné aplikácie, ktoré by potrebovali pripojenie do internetu a nechali sme zariadenie uzamknuté. Testovanie sme nastavili na čas 5 minút, z toho dôvodu, že sme zistili že to je dostatočne dlhý časový interval aby zariadenie vykonalo potrebné úlohy. Po nastavenom časovom intervale sa jednotlivé pakety opakovali.

Po uplynutí nastaveného času, pozastavili sme skenovanie komunikácie a zachovali sme zachytené pakety. Rovnaké testovanie sme uskutočnili pre všetky zariadenia oddelene v novom súbore. Po otestovaní všetkých zariadení, analyzovali sme každý súbor zvlášť. Orientovali sme sa a pre nás boli dôležité pakety, ktoré obsahovali zdrojovú alebo cieľovú adresu totožnú z IP adresou zariadenia. Ďalej sme analyzovali jednotlivé pakety a zistili sme že pri všetkých zariadeniach bolo najviac paketov s TCP a DNS protokolom. Na tieto dva pakety sme následne aj upriamili najväčší dôraz. Detailnú analýzu každého paketu pre všetky zariadenia sme popísali v pokračovaní tejto kapitole.

3.6 Zariadenia pracujúce na platforme iOS

Keďže operačný systém iOS vlastnia iba zariadenia od firmy Apple, porovnali sme dve zariadenia rovnakého výrobcu. Aby nešlo iba o smartfóny, použili sme aj tablet. Otestovali sme iPhone 5S, ktorý na sebe obsahoval aktuálnu verziu iOS, 10.2.1. iPhone sme resetovali a neinštalovali sme ďalšie aplikácie. Avšak aby sme ho mohli použiť, museli sme zadať prihlasovacie údaje. Ako tablet sme použili iPad Mini pracujúci pod verziou 7.1.2. Pre porovnanie čo zariadenia robia, tento tablet obsahoval aj Jailbreak.

3.6.1 iPhone 5S

Ako prvé zariadenie otestovali sme iPhone 5S. Zariadenie bolo nastavené ako nové a neobsahovalo žiadne dodatočné aplikácie. Pri aktivácii museli sme sa prihlásiť na Apple účet. Zariadeniu bola pridelená IP adresa *192.168.238.107*. Po prihlásení do vytvorenej sieti, videli sme, že zariadenie požiadalo systém DNS o IP adresu servera *captive.apple.com*.

```
43 12.621441   192.168.236.107   192.168.236.1   DNS   77 Standard query 0x2e57 A captive.apple.com
```

Ide o server, ktorý slúži na zadanie údajov pri prihlasovaní do verejnej bezdrôtovej siete, ktorý na zariadenie odoslal link na stránku s formulárom na prihlasovanie. Keďže sme v našom prípade zadávali iba heslo siete stránka sa nezobrazila. Následne bolo požiadané o adresu stránky výrobcu *apple.com*.

V pokračovaní vidíme žiadosť o adresu servera *api-aka.smoot.apple.com*. Na tomto serveri sa zhromažďujú všetky slová, ktoré sme vnášali pri vyhľadávaní a na zariadenie sa sťahovali slová, ktoré by uľahčili vyhľadávanie. Keďže zariadenie bolo prvýkrát pripojené do internetu, zistili sme že si sťahovalo väčšie množstvo údajov, čiže databázu pomocných slov.

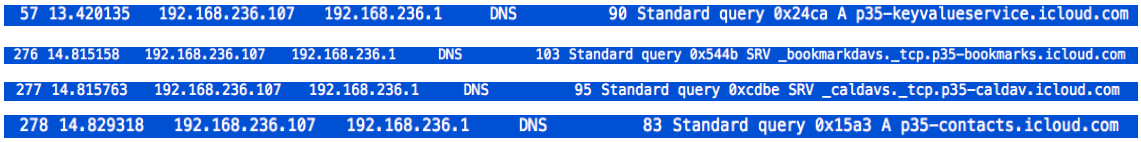
```
56 13.418935   192.168.236.107   192.168.236.1   DNS   83 Standard query 0xbf41 A api-aka.smoot.apple.com
```

Zariadenie sa taktiež pripojilo na server *p35-ckdatabase.icloud.com*. Tento server slúži na ukladanie údajov do Cloudu. Následne na základe TCP paketov sme si všimli, že prebehla synchronizácia a v prípade že by sa niektoré údaje nenachádzali v Cloude, začali by sa odosielať v našom prípade k tomu nedošlo keď neobsahoval nič.

```
52 13.417428   192.168.236.107   192.168.236.1   DNS   85 Standard query 0x9b2c A p35-ckdatabase.icloud.com
```

Okrem tohto Cloudového serveru zariadenie sa pripojilo aj na ďalšie. Ide o servery, ktoré sú rozdelené podľa kategórií a to na základe čo sa odosiela.

```
54 13.418190   192.168.236.107   192.168.236.1   DNS   80 Standard query 0xd18c A p35-imap.mail.me.com
55 13.418560   192.168.236.107   192.168.236.1   DNS   82 Standard query 0x8198 A p35-content.icloud.com
```



Sú to servery *imap.mail.me.com,* ktorý zálohuje emailové správy, *content.icloud.com* určený na zálohovanie dokumentov ako sú fotografie, notes a iné. *keyvalueservice.icloud.com* slúži na zálohovanie hesiel webových stránok a kreditných kariet z aplikácii Wallet. *bookmarks.icloud.com* je zálohovanie uložených stránok v prehliadači Safari, *caldav.icloud.com* zálohuje uložené udalosti v aplikácii kalendár a reminders. Server *contacts.icloud.com* ukladá kontakty zo zariadenia, či už telefóne alebo emailové. Prítomnosť týchto serverov sa môže odlišovať na jednotlivých zariadeniach v závislosti, ktoré položky majú zaškrtnuté v nastavení iCloudu. Pri továrenskom nastavení zaškrknuté sú všetky položky.

Po synchronizácii s iCloudom zariadenie požiadalo o pripojenie na server *lcdn.locator.apple.com.*

Ide o server na ktorom sa aktualizujú informácie o lokalite kde sa zariadenie nachádza. Pomocou aplikácii Find My iPhone môžeme zistiť kde presne sa zariadenie nachádza a v prípade straty alebo krádeží môžeme zariadenie lokalizovať.

Okrem iCloud serverov, spoločnosť Apple používa aj úložiská od spoločnosti Amazon, *s3.amazonaws.com.*

Spoločnosť Apple vlastní aj úložiskové centrá od iných spoločností ako sú Amazon alebo Microsoft kvôli rozmiestnenú serverov na rôznych lokalitách s dôvodu aby dosahovali rýchlejšie pripojené s najmenšou odozvou. Konkrétne otestované zariadenie sa pripojilo na server umiestnení v Írsku.

Ďalej zariadenie zosynchronizovalo údaje so serverom *blobstore.apple.com*.

Blobstore je server, ktorý ma na starosti údaje týkajúce sa s aplikáciou iTunes. Idem o aplikáciu, ktorá slúži na prehrávanie hudby alebo filmov. Multimédia sa do iTunesu môže kopírovať za pomoci počítača. Taktiež existuje možnosť zakúpenia si hudby alebo filmov a pokiaľ sa nachádzajú na účte prepojenom so zariadením, prebehne synchronizácia.

Zariadenia iPhone poskytujú vývojárom možnosť zasielať rôzne notifikácie používateľovi pomocou Apple push notification.

Zariadenie sa pripojilo na server *courier.push.apple.com* za účelom aby si stiahlo notifikácie, ktoré sú smerovane zo strany spoločnosti Apple.

Taktiež sa počas testovania zariadenie pripojilo aj na *server albert.apple.com.*

Albert je server, ktorý slúži na synchronizáciu aktivácie pre zariadenia Apple. Pokiaľ je zariadenie stratené alebo odcudzené existuje možnosť aby sa nastavilo do strateného režimu. Ak by sa zariadenie nachádzajúce v stratenom režime pripojilo na internet, automatický by používateľovi zaslalo správu kde sa nachádza a na zariadení by sa zobrazili vopred zadefinované informácie, napr. údaje o používateľovi.

Zariadenia si vyžiadalo IP adresu aj od servera *mesu.g.aaplimg.com*.

Je to server na ktorom sú uložené údaje, čiže aplikácie, ktoré sú dostupné na sťahovanie v „obchode“ Appstore. Prostredníctvom Appstoru aplikácie sa aj aktualizujú a preto sa aj testované zariadenie zosynchronizovalo so serverom aby sa v prípade potreby aktualizovali inštalované aplikácie.

3.6.2 iPad Mini

Ďalšie otestované zariadenie, ktoré pracovalo na platforme iOS bolo iPad Mini. Ide o prvú generáciu tabletu v zmenšenej sérii. Aby sme porovnali dva rozdielne verzie platformy, tablet pracoval na verzii 7.1.2. Keďže ide o staršiu verziu operačného systému, bolo možné inštalovať aj Jailbreak. Inštalovali sme ho z toho dôvodu aby sme porovnali či sa zariadenie pod vplyvom Jailbreaku pripája aj na iné servery vzhľadom k otestovanému zariadeniu iPhone. Tablet po pripojení do siete vlastnil adresu *192.168.236.111*.

Ako aj pri iPhone aj iPad väčšinou komunikovalo so servermi výrobcu za účelom synchronizácie niektorých údajov. Zariadenie sa najprv pripojilo na server *captive.apple.com*, kvôli zobrazeniu formuláru na prihlásenie do siete. Keďže sieť bola rovnaká ani v tomto prípade sa stránka s formulárom nezobrazila. Po úspešnom pripojení do siete, zariadenie požiadalo adresu od servera *guzzoni.apple.com*.

Server guzzoni je určený pre osobnú asistentku *Siri*. Ide o funkciu, ktorá bola prvýkrát inštalovaná na zariadenie iPhone 4S. Používateľ môže tak po stlačení domovského tlačidla hlasom zadať úlohu asistentke. Do tejto funkcie sa často pridávajú nové gestá, pre iné aplikácie a preto sa musí zosynchronizovať so zariadením.

Následne navštívilo stránku výrobcu a napojilo sa na server *init-p01st.push.apple.com* a 8-*courier.push.apple.com.*

Tento server slúži na odosielanie „push“ notifikácií na zariadenia. Pri porovnaní od iPhonu, ktorý sa tiež pripojil na podobný server, adresy sa odlišovali čo naznačuje že pre niektoré časti sa servery líšia na základe verzie platformy.

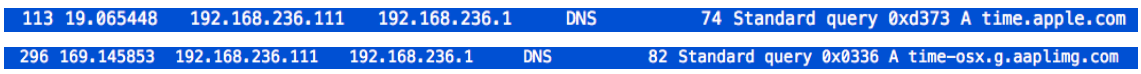
Každé zariadenie obsahuje už inštalovanú aplikáciu Mail, ktorá podporuje najznámejšie mailové účty medzi, ktoré patrí aj Outlook.

Počas testovania sa zariadenie pripojilo na server *eas.outlook.com* a na tablete sa zobrazil formulár na vnesenie prihlasovacích údajov. Okrem Outlooku Apple podporuje tiež Gmail a Yahoo mail, ktoré sa totiž počas testovania nezobrazili.

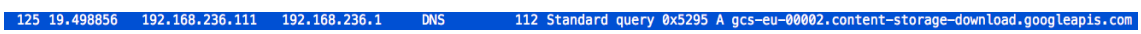
Potom ako aj pri predchádzajúcom testovaní prebehla synchronizácia so servermi iCloud.

Boli to serveri *streams.icloud.com*, úložiskový server pre ukladanie fotografii, ktoré sú ukladané prostredníctvom služby iCloud. Server *content.icloud.com*, ktorý v prípade iOS 7 slúžil na úschovu ďalších údajov ako sú kontakty, zápisnice a iné. Tiež server *keyvalueservice.icloud.com*, na ktorom sa nachádzajú chránené heslá z webových stránok a aplikácií na platenie online pomocou aplikácie Apple Pay. Všimli sme si že pri nižšej verzii platformy, sa niektoré iCloudové servery nezobrazili, ale sú prepojené do jedného spoločného serveru, ako napríklad server *content.icloud.com,* ktorý v sebe zahrnul niekoľko ďalších serverov.

Okrem údajov zariadenie si zosynchronizovalo tiež dátum a čas s NTP serverom *time.apple.com* a následne na ďalší podobný server,
time-osx.g.aaplimg.com.



Tiež sme si všimli, že okrem serverov výrobcu, iPad sa pripojil aj na server spoločnosti Google, *content-storage-download.googleapis.com* a server *sr.symcd.com*, ktorý patri spoločnosti Symantec.



Ako ďalšie servery aj tieto sú určené ako úložiskové servery. Server *symcd* je definovaný ako všeobecný úložiskový server, zatiaľ čo server spoločnosti Google slúži ako zdroj odkiaľ sa sťahujú videa a hudba, ktorú je možné zakúpiť si ju prostredníctvom

aplikácie iTunes Store. Ďalší server, ktorý pracuje s aplikáciou iTunes je *upp.itunes.apple.com*.

Na základe TCP paketov sme zistili, že si z tohto serveru zariadenie sťahovali autorizačný certifikát, pomocou ktorého by sa mohol prihlásiť do iTunes predajni, za účelom nákupu rôznych multimédií.

Aj napriek tomu, že otestovaný model iPadu nemal v sebe zabudovaný GPS modul, po pripojení do siete odoslal na server *gs-loc.apple.com* lokalitu tom kde sa nachádza.

3.7 Zariadenia pracujúce na platforme Android

Na otestovanie bezpečnosti platformy Android sme si zvolili tri zariadenia, Samsung Galaxy Prime Grand a Sony Xperia Z1 Comapact pracujúcej na rovnakej verzii platformy a Samsung J7, ktorý obsahoval aktuálnu verziu operačného systému. Ako pri ostatných testovaných smartfónoch, aj tieto zariadenia boli resetované do továrenského nastavenia a neobsahovali žiadne nakopírované údaje.

3.7.1 Sony Xperia Z1 Compact

Ako prvé otestované zariadenie sme si zvolili smartfónov značky Sony. Zariadenie na sebe obsahovalo verziu 5.1.1 známu pod názvom „Lollipop“. Akonáhle sme vniesli heslo siete a pripojili sa, DHCP server poskytol adresu *192.168.236.115.*

Ako prvé sme si všimli, že zariadenie sa pripojilo na server *connectivitycheck.android.com.*

Tento server je podobný serveru *captive,* ktorý sa zobrazil na zariadeniach Apple a slúži aby zariadenie otestovalo či pripojenie funguje.

Po úspešnom pripojení, zariadenie si ako prvé aktualizovalo dátum a čas so servermi *ntp.nict.jp* a *time.gpsonextra.net.*

V porovnaní s ostatnými zariadeniami, prvýkrát sa stretáme, že smartfón použil iný ntp server od výrobcu. Okrem synchronizácii času, prebehla aj synchronizácia emailového klienta. Akonáhle sa zobrazil paket so žiadosťou o adresu klienta *imap.gmail.com,* zobrazil sa aj formulár na prihlásenie, keďže zariadenie bolo resetované.

Zariadenie sa ďalej počas testovania pripojilo aj na niekoľko serverov výrobcu *idd.sonymobile.com, udl-api.sonymobile.com* a *updatesec.sonymobile.com* odkiaľ si stiahlo aktualizácie systémového softvéru.

```
 49 6.081513    192.168.236.115   192.168.236.1     DNS          78 Standard query 0x389c A idd.sonymobile.com

1050 48.462246   192.168.236.115   192.168.236.1     DNS          82 Standard query 0xf755 A udl-api.sonymobile.com

1217 248.202114  192.168.236.115   192.168.236.1     DNS          84 Standard query 0xf3fc A updatesec.sonymobile.com
```

Tiež sme si všimli, že navštívilo aj stránku *google.com* a *news.google.com* aj napriek tomu, že bolo nastavený slovenský jazyk a krajina Slovensko.

Synchronizácia prebehla aj prostredníctvom serverov *android.cliennts.google.com* a *googleapis.com.*

```
 97 7.647295    192.168.236.115   192.168.236.1     DNS          86 Standard query 0x2ca1 A android.clients.google.com

221 12.791675   192.168.236.115   192.168.236.1     DNS          78 Standard query 0xa22b A www.googleapis.com
```

Potom sa zariadenie pripojilo na server aplikácie obchodu Play odkiaľ sa aktualizujú všetky aplikácie.

```
669 28.410845   192.168.236.115   192.168.236.1     DNS          79 Standard query 0x63ad A play.googleapis.com
```

A následne sa aktualizovali inštalované aplikácie, napr. Mtalk alebo Google Tag Manager a ďalšie, pretože sa zariadenie následne pripojilo na servery *mtalk.google.com* a *googletagmanager.com.*

Ďalej sme si mohli všimnúť, že sa zariadenie pripojilo aj na Cloudový server *cloudconfig.googleapis.com.*

```
116 8.073229    192.168.236.115   192.168.236.1     DNS          86 Standard query 0x94b2 A cloudconfig.googleapis.com
```

Keďže každé Android zariadenie vlastní priestor na GoogleDrive, v prípade že by obsahovalo nejaké údaje a bol by prihlásený používateľ, automatický by začalo odosielať údaje na server.

Aj zariadenia Android si po pripojení do siete stiahli SSL certifikáty, konkrétne otestované zariadenie sa pripojilo na servery *ssl.google-analytics.com* a *ssl.gstatic.com*

```
166 10.918928   192.168.236.115   192.168.236.1     DNS          84 Standard query 0x1c9a A ssl.google-analytics.com

362 15.382871   192.168.236.115   192.168.236.1     DNS          75 Standard query 0xd06f A ssl.gstatic.com
```

Medzi DNS paketmi sa nachádzala aj žiadosť o server *xtra3.gpsonextra.net.*

```
545 25.680613   192.168.236.115   192.168.236.1     DNS          80 Standard query 0x4877 A xtra3.gpsonextra.net
```

Keď sme analyzovali IP adresu servera a prefiltrovali sme TCP pakety, zistili sme, že si zariadenie stiahlo súbor, ktorý napomáha aby si GPS modul rýchlejšie odhalil presnú

lokalitu kde sa nachádza. V prípade, že by bolo zariadenie registrované pomocou Google účtu, lokalita by sa automaticky odosielala na server.

Smartfón si ešte počas testovania zosynchronizoval údaje so serverom *safebrowsing.google.com*

```
661 28.296457   192.168.236.115   192.168.236.1   DNS   83 Standard query 0x2211 A safebrowsing.google.com
```

Safe Browsing, je funkcia vyvíjaná spoločnosťou Google a napomáha zvýšiť bezpečnosť pri prehľadávaní webu, tým spôsobom, že keď by sa používateľ dostál na ohrozenú stránku, prehliadač by prístup zamedzil a vypísal hlášku a hroziacom nebezpečenstve.

3.7.2 Samsung Galaxy Prime Grand

Ďalšie otestované Android zariadenie bol smartfón značky Samsung. Podobne ako aj predchádzajúce zariadenie, aj toto pracovalo na verzii 5.0. Počas testu mu bola pridelená adresa *192.168.236.138.* V nástroji Wireshark sme si všimli, že sa jednotlivé pakety podobajú paketom zariadenia Samsung J7, ktoré pracovalo na aktuálnej verzii platformy, preto sme bližšie popísali iba jedno zvolené zariadenie.

Veľká väčšina paketov bola totožná s paketmi zariadenia Sony, keďže sa obe pripájali na servery Googlu (ktoré sú opísané pri predchádzajúcom zariadení), odlišovali sa tým, že pri tomto zariadení boli pakety smerované aj na Samsungove servery.

Na začiatku sme videli, že si zariadenie aktualizovalo aplikáciu Swype prostredníctvom serverov *api-samsung.swypeconnect.com, cdn-docs.swypeconnect.com* a *cdn.hotwords.swypeconnect.com.*

```
37 43.984231   192.168.236.138   192.168.236.1   DNS   88 Standard query 0x51db A api-samsung.swypeconnect.com

343 47.360936   192.168.236.138   192.168.236.1   DNS   85 Standard query 0xe80c A cdn-docs.swypeconnect.com

480 48.630073   192.168.236.138   192.168.236.1   DNS   89 Standard query 0xd046 A cdn-hotwords.swypeconnect.com
```

Ide u aplikáciu, ktorá podporuje ľahšie ovládanie klávesnice počas písania. Prostredníctvom tohto servera si aplikácia sťahuje všetky potrebné údaje.

Počas testovania do zariadenie sa stiahli aj licenčné zmluvy prostredníctvom servera *ospserver.net.* Na synchronizáciu dátumu a času zariadenia používajú server *pool.ntp.org.*

Synchronizáciu platformy zariadenie realizovalo pomocou serverov *api-diagmon.samsungdm.com, api.spd.amsungdm.com* a ďalších.

```
727 59.965072   192.168.236.138   192.168.236.1   DNS   85 Standard query 0x83ff A api-diagmon.samsungdm.com

822 64.589185   192.168.236.138   192.168.236.1   DNS   81 Standard query 0x9471 A api.spd.samsungdm.com
```

Okrem synchronizácii platformy, prebehla aj synchronizácia inštalovaných aplikácií, na ktorú boli použité servery *hub-odc.samsungapps.com, sk-odc.samsungapps.com* a iné.

```
877 67.095835   192.168.236.138   192.168.236.1   DNS   83 Standard query 0x1f2c A hub-odc.samsungapps.com

885 68.769159   192.168.236.138   192.168.236.1   DNS   82 Standard query 0xbac8 A sk-odc.samsungapps.com
```

Samsung umožňuje aj používanie funkcie MDM (správy mobilných zariadení), ktorá ponúka prepojenie viacerých zariadení spolu s počítačmi, ktorá môže byť implementovaná v iných aplikáciách. Zariadenie si zo servov *secb2b.com* stiahla potrebné údaje pre danú funkciu.

```
3724 76.996974   192.168.236.138   192.168.236.1   DNS   83 Standard query 0xa188 A eu-prod-bulk.secb2b.com

4081 77.885772   192.168.236.138   192.168.236.1   DNS   75 Standard query 0xe880 A gslb.secb2b.com

4400 78.610717   192.168.236.138   192.168.236.1   DNS   82 Standard query 0xcbc3 A eu-segd-api.secb2b.com
```

3.8 Zariadenia pracujúce na platforme Windows Phone

Pri platforme Windows Phone (mobile) sme otestovali tri zariadenia. Jedno zariadenie bolo od výrobcu Samsung a druhé dve od výrobcu Nokia, čiže Microsoft. Na každom zariadení bola iná verzia platformy, pričom každé zariadenie bolo nastavené na továrenské nastavenia a nebolo nič ďalšie inštalované. Windows Phone ponúka možnosť používať zariadenia aj bez prihlásenie s účtom Microsoft, takže zariadenia neboli prihlasované.

3.8.1 Samsung Ativ S

Najprv sme otestovali zariadenie Samsung Ativ S. Ide o smartfónov pracujúci na verzii 8.1. Po prihlásení do siete bola mu pridelená adresa *192.168.236.72*. Podobne ako pri ostatných zariadeniach pri platforme Windows Phone, zariadenie po pripojení do siete požiadalo o adresu pre stránku *www.msftncsi.com*.

```
13 0.179974   192.168.236.72   192.168.236.1   DNS   76 Standard query 0xf81a A www.msftncsi.com
```

Je to stránka, ktorú vlastní Microsoft a používajú ju všetky zariadenia pracujúce na tejto platforme aby vyskúšali či je pripojenie do sieti funkčné. Keďže v zariadení nebol prihlásení žiadny používateľ, pripojilo sa na server *discoveryservice.windowsphone.com*

```
19 0.543284   192.168.236.72   192.168.236.1   DNS   93 Standard query 0x8e62 A discoveryservice.windowsphone.com
```

Na tomto serveri sa nachádzajú autorizačné certifikáty, ktoré umožňujú bezpečné sa prihlásenie na konto Microsoft a poskytujú používateľovi chránenú komunikáciu v sieti. Ďalej sa zariadenie pripojilo na stránku aplikácie Bing Translator a prebehla synchronizácia.

```
70 5.391086   65.52.0.186     192.168.236.72   TCP    66 80 → 49152 [SYN, ACK] Seq=0 Ack=1 Win=8192 Len=0 MSS=1440 WS=256 SACK_PERM=1
```

Na základe TCP protokolov sme zistili, že do aplikácie sa sťahovali rôzne fotografie. Okrem aplikácie Bing Translator, synchronizácia prebehla aj pre WNS.

```
57 5.240555   192.168.236.72   192.168.236.1   DNS    84 Standard query 0x3685 A winphone.wns.windows.com
```

WNS je funkcia podobná Apple Push Notification, ktorá umožňuje vývojárom aplikácii používať vlastne Cloudové servery, napríklad pre aktualizáciu alebo rôzne informácie, ktoré sú zobrazované v aplikáciách. Ďalej sa počas testovania zariadenie pripojilo na server *settings.live.net.*

```
223 220.087003  192.168.236.72   192.168.236.1   DNS    84 Standard query 0xc365 A bn1305.settings.live.net
```

Odkiaľ si stiahlo potrebné certifikáty a na obrazovky sa zobrazil formulár na prihlásenie pre emailovú aplikáciu Outlook. Z dôvodu aby sa vo Wiresharku nezobrazili ďalšie pakety súvisiace s aplikáciu, formulár sme vypli. Taktiež požiadalo aj o získanie informácii o aktualizáciách na serveri *ctldl.windowsupdate.com.*

```
233 220.544376  192.168.236.72   192.168.236.1   DNS    83 Standard query 0x1628 A ctldl.windowsupdate.com
```

Windows používa spoločný server, na ktorom sú umiestnené všetky verzie platformy s aktualizáciami, keďže na rozdiel od ostatných platformách umožňuje aj inštalovanie staršej verzie platformy bez akéhokoľvek dodatočných nástrojov. Počas testovania sme zistili, že sa zariadenie pripojilo na sever *ocsp.omniroot.com*.

```
239 220.642931  192.168.236.72   192.168.236.1   DNS    77 Standard query 0x9dcf A ocsp.omniroot.com
```

Z uvedeného serveru si zariadenie stiahlo dodatočné bezpečnostné certifikáty keďže ide o OSCP server. Na základe IP adresy servera, sme zistili že Microsoft ma odkúpené servery od spoločnosti Verzion. Okrem serveru OSCP, aj zo servera *cdp1-public-trust.com* a *ocsp.msocsp.com* bol stiahnuté ďalšie bezpečnostné certifikáty.

```
253 220.999777  192.168.236.72   192.168.236.1   DNS    81 Standard query 0xa1b1 A cdp1.public-trust.com

261 221.313690  192.168.236.72   192.168.236.1   DNS    75 Standard query 0xb186 A ocsp.msocsp.com
```

Certifikáty sú podobné predošlému a sú určené na zabezpečené surfovanie internetom, podporované protokolmi 443 a 80. Na záver bolo ešte stiahnutých niekoľko SSL certifikátov zo servera mscrl.microsoft.com

```
273 221.429227  192.168.236.72   192.168.236.1   DNS    79 Standard query 0xe25c A mscrl.microsoft.com
```

3.8.2 Nokia 610

Veľkú väčšinu zariadení obsahujúcich platformu Windows Phone vyrobila spoločnosť Nokia, ktorú následne prebral Microsoft. Najprv sme otestovali starší model, Nokia 610. Toto zariadenie pracovalo na verzii 7.5 a v teste bolo pod IP adresou *192.168.236.114.* Testovanie prebehlo rovnakým spôsobom ako aj ostatné a zariadenie tiež bolo rovnako nastavené. Počas priebehu testu sa zo zariadenia neodoslal žiadny

DNS paket, ktorý by žiadal preklad adresy nejakého servera. Aby sme porovnali resetované zariadenie od zariadenia bežného používateľa, prihlásili sme sa pomocou účtu Microsoft a kopírovali sme niekoľko údajov, ako sú fotografie kontakty a pod. Testovanie sme zopakovali a zistili sme, že aj napriek osobným údajom nachádzajúcich sa na zariadení, neovplyvnili aby ich zariadenie odosielalo do Cloudu, v prípade Microsoftu prostredníctvom aplikácie One Drive. Aby sme potvrdili funkčnosť nástrojov a samotnej siete, navštívili sme stránku.*ki.fpv.ukf.sk*, kde sa následne zobrazil paket DNS, ktorý požiadal o IP adresu stránky.

3.8.3 Microsoft Lumia 435

Na porovnanie správania sa zariadení rovnakého výrobcu pracujúcich na odlišných platformách, otestovali sme aj zariadenie, ktoré obsahovalo aktuálnu verziu Windows 10 mobile. Išlo o model Lumia 435 kde bol ako výrobca označený Microsoft. Zariadenie bolo otestované pod IP adresou *192.168.236.71*.

Väčšina paketov boli totožne s paketmi zariadenia Samsung Ativ S. Išlo prevažne o pakety ktorými boli prenášané SSL certifikáty. Ako prvé na zariadení prebehla synchronizácia aktualizácií platformy a boli stiahnuté údaje zo serverov *sls.update.microsoft.com*, *ctldl.windowsupdate.com, go.microsoft.com, licensing.mp.microsoft.com, fe3.delivery.mp.microsoft.com* a *tsfe.trafficshaping.dsp.mp.microsoft.com.*

```
 52 9.480338   192.168.236.71  192.168.236.1   DNS   84 Standard query 0x603c A sls.update.microsoft.com
 59 10.206524  192.168.236.71  192.168.236.1   DNS   83 Standard query 0x72b9 A ctldl.windowsupdate.com
 465 20.414865 192.168.236.71  192.168.236.1   DNS   76 Standard query 0xd127 A go.microsoft.com
 664 26.904031 192.168.236.71  192.168.236.1   DNS   86 Standard query 0x1d1d A licensing.mp.microsoft.com
 817 29.007669 192.168.236.71  192.168.236.1   DNS   89 Standard query 0x120a A fe3.delivery.mp.microsoft.com
3576 194.649278 192.168.236.71 192.168.236.1   DNS  100 Standard query 0xb3ed A tsfe.trafficshaping.dsp.mp.microsoft.com
```

Po pripojení na severy, na zariadení sa aktualizovali niektoré už inštalované aplikácie a počas testovania sa sťahoval veľké množstvo údajov. Ide o servery, ktoré nevplývajú na činnosť zariadenia a na druhej strane dokážu sledovať aktivitu používateľa a zo zariadenia uberať aj súkromné informácie.

Ďalej sa zobrazil DNS so serverom *fs.microsoft.com.*

```
 88 11.613703  192.168.236.71  192.168.236.1   DNS   76 Standard query 0x8f90 A fs.microsoft.com
```

Server totožný serveru pri Androide určený na MDM, ktorý sa používa na ukladanie a zdieľanie informácií o identite medzi dôveryhodnými partnermi, cez službu extranet.

Ide o službu podobnú VPN, ktorá umožňuje pripojenie sa do rôznych webových aplikácií ostatných partnerov. Táto funkcia je zabezpečená a pri pripojení overuje každého používateľa.

Podobne ako pri zariadení Samsung, aj pri tomto teste sa na obrazovke zobrazil formulár pre prihlásenie do Microsoft účtu, *login.live.com*. Na rozdiel od prechádzajúceho zariadenia, v tomto prípade sa najprv zariadenie pripojilo na server *displaycatalog.mp.microsoft.com*.

```
117 13.789441   192.168.236.71   192.168.236.1   DNS   91 Standard query 0xa39f A displaycatalog.mp.microsoft.com
```

Displaycatalog je proxy server, ktorý poskytuje anonymné prihlásenie sa a poskytuje tunel, ktorý skrýva celý proces, ide o zámenu služby VPN.

Okrem serverom Verzion, Microsoft používa aj servery spoločnosti Symantec, *s2.symcb.com*.

```
126 14.618487   192.168.236.71   192.168.236.1   DNS   72 Standard query 0x2d04 A s2.symcb.com
```

Podobne ako aj server Verzion, aj na servery Symantec sú umiestené ďalšie certifikáty.

Verzia 10 platformy obsahuje tiež osobného asistenta *Cortanu*, ktorého údaje sú uložené na servery *storeedgefd.dsx.mp.microsoft.com*.

```
374 17.831984   192.168.236.71   192.168.236.1   DNS   92 Standard query 0xeb54 A storeedgefd.dsx.mp.microsoft.com
```

Taktiež sa na tomto servery umiestené údaje, ktoré používa aplikácia Skype, ktorá je tiež vopred inštalovaná.

Zariadenie sa pripojilo aj na server *clientconfig.passport.net*

```
483 20.716047   192.168.236.71   192.168.236.1   DNS   85 Standard query 0x5723 A clientconfig.passport.net
```

Podľa prijatých paketov ide o CRM server, ktorý slúži na komunikáciu s používateľom, pokiaľ by došlo do nejakého problému, či už zo strany používateľa alebo zariadenia.

Ďalšie pakety, ktoré sa zobrazili vo Wiresharku obsahovali adresy serverov *settings-win.data.microsoft.com* a *v10.vortex-win.data.microsoft.com*.

```
643 26.431101   192.168.236.71   192.168.236.1   DNS   91 Standard query 0xe3c2 A settings-win.data.microsoft.com

645 26.442837   192.168.236.71   192.168.236.1   DNS   93 Standard query 0x0df4 A v10.vortex-win.data.microsoft.com
```

Zistili sme, že sú to ďalšie servery na ktorých sa nachádzajú SSL certifikáty, ktoré slúžia na bezpečné stihnutie a inštaláciu aktualizácií platformy.

Aby prebehla aktivácia zariadenia a overenie prihlásenie používateľského konta, zariadenie si vyžiadalo adresu servera *pruchase.mp.mictosoft.com*.

```
1046 32.475146   192.168.236.71   192.168.236.1   DNS   85 Standard query 0x657a A purchase.mp.microsoft.com
```

Je to aktivačný server, ktorý legitimuje nové zariadenie prvýkrát pripojené do siete.

4 VÝSLEDKY RIEŠENIA A ICH ZHODNOTENIE

V predchádzajúcej kapitole sme popísali test ôsmych zariadení rozdelených do troch kategórii podľa platformy na ktorej pracovali. Zariadenie, ktoré sme použili na vytvorenie prístupového bodu sa používa aj pri bežnom poskytovaní bezdrôtového pripojenia, čo bol dôvod, že zariadenia mali rozlične pridelené IP adresy.

V štvrtej kapitole bližšie uvedieme dosiahnuté výsledky jednotlivých testovaní. Vyhodnotíme nástroje, ktoré sme použili pri praktickej časti, tiež popíšeme výhody a nevýhody použitých nástrojov. Ďalej zhodnotíme otestované platformy a zariadenia, ako aj dosiahnuté výsledky testov. Na záver na základe zistených výsledkov, navrhli sme metódy a odporúčania na čo by mali používatelia dávať pozor pred pripojením do siete a tiež sme popísali aplikáciu, ktorá poskytuje anonymitu v sieti.

4.1 Vyhodnotenie platformy iOS

Na otestovanie platformy iOS použili sme dve zariadenia. Aby sme porovnali v čom sa odlišujú telefón od tabletu použili sme iPhone a iPad. Tiež sme použili aj dve odlišné verzie platformy aby sme zistili či sa odlišujú zo pohľadu bezpečnosti.

Zariadenia si líšili aj tým, že jedno obsahovalo Jailbreak. Test v oboch prípadoch prebehol rovnakým spôsobom. Obe zariadenia vo väčšine prípadov komunikovali so servermi výrobcu alebo so servermi, ktoré ma Apple zakúpené z dôvodu lepšieho umiestnenia serverov na všetkých kontinentoch.

Keď ide o iCloudové servery, zistili sme že pri novšej verzii platformy je väčší počet serverov, ktoré sú rozdelené do viacerých kategórií. V prípade bezpečnosti ide o lepší prístup keďže by sa útočníkovi zväčšil počet paketov smerovaných na rôzne serveri, ale z druhej strane by mu bol poskytnutí akýsi filter a mal by lepší prehľad o odoslaných paketov. Zariadenia sa počas testu nepripojili na žiadny podozrivý server a neodosielali údaje smerované na iné miesta. V prípade druhého zariadenia, ktoré obsahovalo Jailbreak, neodhalili sme žiadne podozrivé správanie po pripojení do siete. Pakety sa neodlišovali od paketov iPhonu, ale na druhej strane zariadenie obsahovalo neaktuálnu verziu platformy, ktorá ma rôzne systémové diery, ktoré znižujú bezpečnosť.

Všimli sme si, že pri továrenskom nastavení, zariadenie odosiela všetky údaje, niektoré súkromné do iCloudu. V prípade útoku man-in-the-middle, útočník by získal všetky odoslané údaje. Pre zvýšenie bezpečnosti je preto potrebné zhodnotiť si či je

potrebné aby boli zapnuté služby iCloudu, alebo používať spôsob zálohovania údajov pomocou USB kábla. Tiež je potrebné zamedziť možnosť zdieľania lokality pre ostaté aplikácie. Taktiež je dôležité neignorovať informáciu o aktualizácii platformy iOS, ktorá zaručuje vyššiu bezpečnosť čo sme zistili aj pri testovaní. Ďalšie všeobecné odporúčania týkajúce sa všetkých otestovaných zariadení sme uviedli v nasledujúcej podkapitole.

4.2 Vyhodnotenie platformy Android

Bezpečnosť platformy Android sme otestovali pomocou troch zariadení, pričom sme použili dvoch odlišných výrobcov a dve odlišné verzie platformy. Pomocou nástroja určeného na analýzu paketov zistili sme, že všetky zariadenia bez ohľadu na výrobcu sa pripájali na servery výrobcu platformy, čiže Google. Tiež sme si všimli, že zariadenia pracujúce na platforme Android na synchronizáciu času a dátumu nepoužívajú vlastné servery. Každý výrobca vlastní aj vlastné servery na, ktoré sa jednotlivé zariadenia pripájajú a odosielajú určité informácie. Preto kvôli zvýšeniu bezpečnosti, treba obmedziť jednotlivé nastavenia aby sa určité údaje po pripojení do siete automaticky neukladali na dané servery.

Prvé otestované zariadenie bolo Sony. Komunikácia zariadenia so serverom prebiehala podobným spôsobom ako aj pri ostatných zariadeniach. Keďže zo zariadenia bolo všetko vymazané, najprv sa stiahli potrebné aktualizácie platformy a potom aj všetkých aplikácií, ktoré sa nachádzali na zariadení. Aj napriek tomu, že zariadenie nič neobsahovalo v pamäti, prihlásilo sa na úložiskový server. Taktiež sa zariadenie pripojilo na niekoľko serverov výrobcu ale nepodarilo sa podrobne zistiť aké všetky údaje zariadenie odosiela. Keďže si avšak stiahlo súbor, ktorý napomáha zrýchliť zistenie lokality zariadenia, je možné že odosiela údaje o tom kde sa nachádza.

Nasledovné zariadenia boli od výrobcu Samsung. Z bezpečnostného dôvodu sme porovnali dve odlišné verzie platformy, dospeli sme k tomu, že aj napriek aktuálnejšej verzie platformy, zariadenie v sieti konalo rovnako. Obe zariadenia podobne ako predchádzajúce komunikovali so servermi výrobcu, odkiaľ sťahovali potrebné údaje. Oproti smartfónu Sony, zariadenia neboli pripojené na žiadny Cloudový server. Tiež neboli zobrazené pakety súvisiace s lokalitou. Avšak na rozdiel od zariadeniach výrobcu Apple, ktorého servery boli rozdelené do kategórií, v tomto prípade bol menší počet serverov a keďže jednotlivé odoslané pakety boli zašifrované nemohli sme zistiť čo presne obsahujú.

4.3 Vyhodnotenie platformy Windows Phone

Pri platforme Windows Phone otestovali sme tri zariadenia. Na porovnanie čím sa odlišujú od rôznych výrobcov požili sme zariadenia Samsung a Nokia. Ďalej aby sme zistili či sú nejaké zmeny vo verziách platformy, otestovali sme tri rôzne verzie. Počas testovania sme zistili, že všetky zariadenia sa väčšinou pripájali na servery výrobcu platformy čiže Microsoftu.

V prípade zariadenia Nokia 610, sme došli k uzáveru, že ide o bezpečné zariadenie nakoľko sa nepripojilo na žiadny server, neodosielalo a neprialo žiadne pakety. Aj napriek tomu, že sme následne nakopírovali určité údaje do zariadenie, výsledky testov boli nezmenené, čo svedčí o tom, že ide o zariadenie vhodné na používanie bez myšlienky, že sa osobné údaje niekam ukladajú. Na druhej strane zariadenie pracovalo na staršej verzii platformy, ktorá už nie je podporovaná pre bežne aplikácie čo obmedzuje použiteľnosť tohto zariadenia.

Pri ďalších dvoch zariadeniach sme si všimli, že boli aktívnejšie po pripojení do siete. Zariadenie Samsung Ativ S po pripojení sťahovalo aktualizácie platformy a aplikácii. Ďalej sa pokúsilo pripojiť do emailového klienta a stiahlo niekoľko bezpečnostných certifikátov. Neboli odoslané žiadne údaje na Cloudové úložiská OneDrive. V nasledujúcej časti testu sme zopakovali proces ako pri predchádzajúcom zariadení a pridali sme údaje. Tiež sa potvrdilo, že zo zariadenia neunikajú žiadne údaje aj napriek tomu, že sú pridávané následne. Keďže ide o zariadenie, ktoré vlastní verziu platformy 8.1, všetky aplikácie boli podporované, takže môžeme tvrdiť, že ide o bezpečné zariadenie, ktoré sa môže uplatniť v každodennom použití.

Posledné otestované zariadenie pracovalo na aktuálnej verzii 10. Pomocou paketov sme prišli po výsledky, ktoré boli do určitej miere totožne so zariadením Samsung. Avšak ďalej počas testovania sa začali zobrazovať servery, ktoré odosielali veľké množstvo údajov na zariadenie. Prevažne išlo o aktualizácie aplikácií a doplnkov. Zaznamenali sme, že ide o servery, ktoré majú schopnosť sledovať prácu zariadenia, ktoré podľa práv odškrtnutých pri aktivácii zariadenia Microsoftu povoľujú. Aby sme zamedzili sledovanie zariadenia, potrebovali sme do systémového súboru *hosts,* skopírovať všetky adresy serverov a označiť ich za localhost. Týmto by sme znížili sťahovanie údajov do zariadenia a znemožnili sledovanie zo strany Microsoftu a potrebné aktualizácie aplikácií by sme vykonávali manuálne.

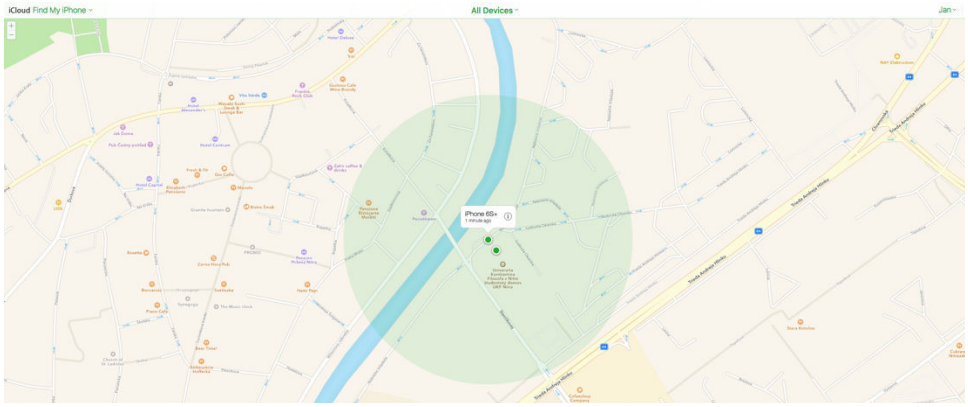
4.4 Metódy a odporúčania pre zvýšenie bezpečnosti zariadení

Po otestovaní všetkých zariadení na základe odchytených paketov sme zistili na čo by si mali používatelia dávať pozor. V tejto časti by sme chceli bližšie uviesť metódy a odporúčania, ktoré sú jednoduché na vykonanie aj pre priemerného používateľa. Medzi prvé odporúčanie by sme zaradili aby si používateľ nenechával zapnuté WiFi pripojenie. V pamäti zariadenia sú uložené všetky prístupové body na ktorých bolo pripojené. Akonáhle sa zariadenie vyskytne v blízkosti tohto bodu automatický sa pripojí, pokiaľ nie je vypnuté automatické pripojenie, čo tiež môže byť užitočné. Na tento spôsob sa používateľ bez svojho vedomia môže stáť obeťou útoku.

Ďalej by si mal dať používateľ pozor na to, aké aplikácie používa po pripojení do verejnej siete. Napríklad aplikácie v ktorých sa nachádzajú súkromné informácie, ako sú elektronické bankovníctvo, aplikácie spoločnosti, nakupovanie v e-shope platobnou kartou a pod. Údaje z takýchto aplikácií, ktoré nie sú dostatočné zabezpečené útočník môže ľahko odchytiť a získať.

Niektoré aplikácie medzi ktoré patria aj sociálne siete, po inštalovaní vyžadujú od používateľa aby povolil brať informácie alebo aj hardvér zariadenia, ako sú kamera alebo mikrofón. Používateľ by mal zvážiť, pre ktorú aplikáciu čo povolí, aby sa jeho údaje nedostali von zo zariadenia. Na všetkých zariadeniach sme otestovali a zistili, že aj na aplikáciách, ktoré boli skorej inštalované existuje možnosť tie povolenia zamedziť.

Väčšina zariadení obsahuje GPS modul určený pre navigáciu. Po resetovaní zariadenia, táto možnosť bola automatický zapnutá. Väčšina aplikácií tento modul využíva aby sme mali možnosť zdieľať kde sa nachádzame, pri platforme iOS spoločnosť Apple používa nástroj *Find My iPhone* ktorý je znázornený na Obrázku 7. Modul sa taktiež využíva aby sme mali GPS koordináty pre fotografiu, ktorú sme vytvorili. Pri testovaní sme zistili že zariadenia aj bez nášho vedomia odosielali údaje kde sa nachádzajú. Z hľadiska bezpečnosti je lepšie zamedziť túto možnosť iba pri niektorých aplikáciách, pretože by táto funkcia mohla poslúžiť v prípade keď by sme zariadenie stratili.



Obrázok 7 Vzhľad nástroja Find My iPhone[12]

Mnohí používatelia na svojich zariadeniach používajú Jailbreak v prípade iPhonov alebo Rooting v prípade Android zariadení. Ide o nástroj ktorým sa odblokujú mnohé funkcie, ktoré výrobca uzamkol. Po odblokovaní zariadenia touto technikou máme prístup väčšine systémových častí a môžeme inštalovať aplikácie, ktorými zmeníme vzhľad zariadenia, aplikácie určené na testovanie, ovládanie senzorov a iné. Tieto nástroje sú vyvíjané programátormi, ktorí sa snažia odhaliť zraniteľné miesta systému a na ten spôsob aby mohli vniknúť do vnútra jadra. Pri používaní týchto nástrojov môžeme poškodiť ale aj znížiť bezpečnosť zariadenia, na ten spôsob, že nástroje sú funkčné iba na niektorých verziách platformy a po aktualizácii systému nástroj už nefunguje. Preto je z hľadiska bezpečnosti účinnejšie mať aktuálnu verziu platformy ako používať podobné nástroje.

4.4.1 Úložiskové aplikácie na zálohovanie údajov

Všetky platformy, ktoré sme otestovali obsahovali už vopred inštalovaný nástroj na ukladanie dát do Cloudu. Po vnesení prihlasovacích údajov pre konkrétne účty v závislosti od platformy, tieto úložiská sa automatický nakonfigurujú. Vo Wiresharku sme skonštatovali, že zariadenia navštevovali servery úložísk. Akonáhle dostali odpoveď automaticky začali odosielať údaje a vykonávať backup. Na tieto úložiska sa zvyčajne zálohujú fotografie, kontakty, správy, hovory a ďalšie súkromné údaje. V prípade útoku, útočník by sa pri zálohovaní mohol ľahko dostať k zálohovaným údajom.

Pre zvýšenie bezpečnosti zariadenia, lepšie riešenie by bolo zálohovať si veci doma ručne, čiže pripojením zariadenia do počítaču pomocou USB kábla. Výrobcovia

[12] Zdroj obrázku 7: Autor práce

obsahujú špeciálne aplikácie, ktoré sú určené na zálohovanie a synchronizáciu zariadení. Skúšali sme, či existuje možnosť nastavenia času kedy by sa určité údaje zálohovali, aby sa napríklad zálohovanie zaplo keď by bol používateľ pripojení do vlastnej siete. Výrobcovia ponúkajú iba nastavenie čo chceme zálohovať pokiaľ sa časovo obmedziť nedalo.

4.5 Použitie VPN nástroja pre anonymnú komunikáciu

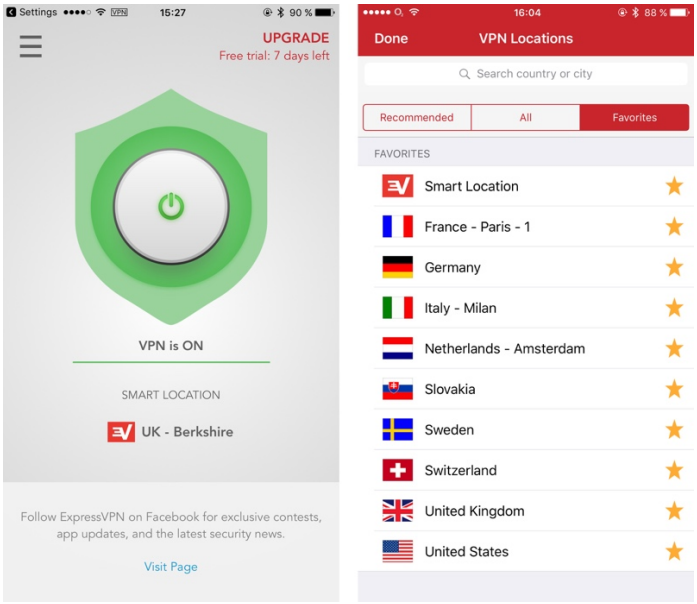
Väčšina používateľov sa okrem prostredia doma alebo v práci, pripája aj do verejnej bezdrôtovej siete, či sa už nachádza v nejakom podniku, kaviarni alebo v nákupnom centre. Akonáhle sa pripojí do takejto siete, existuje riziko že môže byť narušená bezpečnosť zariadenia a zároveň údajov nachádzajúcich sa v zariadení používateľa. Mnoho používateľov sa tento problém neuvedomuje a prihlási sa do takej nezabezpečenej sieti. Môže existovať riziko, že sieť do ktorej sa pripojil nie je vo vlastníctvu inštitúcie. Ide o podobne vytvorenú sieť, ako čo sme vytvorili v praktickej časti, z účelom odchytávania údajov zo strany útočníka, ktorý na ten spôsobom môže vykonať útok Man-in-the-middle. Keďže používateľ videl podobne nazvanú sieť iba s minimálnou úpravou, nemôže vedieť že ide o útok. V prípade že na zariadení používania sú zapnuté rôzne aplikácie, ktoré po pripojení do siete zdieľajú mnohé údaje, ako sú kontakty, správy, či fotografie sa môžu ľahko dostáť do rúk útočníka, ktorý ich môže zneužiť.

Jeden zo spôsobov ako predísť takémuto útoku je použitie VPN nástroja. Ide o technológiu, ktorá vytvára šifrované spojenie cez sieť. Výhodou použitia VPN je to, že zabezpečuje primárnu úroveň zabezpečenia pripojených zariadení, pokiaľ samotná sieť nie je dostatočne zabezpečená. VPN sa obvykle používa aby sa používatelia, ktorí nie sú fyzický na určenom mieste, dostali bezpečne k tomu miestu aj keď sú pripojení do verejnej siete. Používateľovi potom stačí na pripojenie po VPN bránu iba adresa VPN servera a prihlasovacie údaje.

Ďalší spôsob použitia VPN, ktorí sme použili aj my je tunelovanie. Je to prenos údajov v rámci súkromnej siete cez verejnú sieť tým spôsobom, že smerovacie uzly vo verejnej sieti nevedia, že ten prenos ide prostredníctvom verejnej siete. Využívajú sa tunely medzi koncovými zariadeniami privátnej sieti, v rámci ktorých sa prenášajú samotné údaje a tým sa ochraňujú od útokov smerovaných zvonku. Na otestovanie správnosti tunelovania sme použili aplikácie, ktoré sme inštalovali na zariadenia.

4.5.1 ExpressVPN

Prvý nástroj, ktorý sme použili bol ExpressVPN. Tento nástroj sme použili pri všetkých zariadeniach keďže aplikácia podporuje všetky platformy vrátane aj operačných systémov na počítačoch. Zvolili sme si tento nástroj, pretože na základe testovaní viacerých inštitúcii a recenzií dosahoval najvyššie ocenenie z hľadiska bezpečnosti.



Obrázok 8 Pracovné prostredie nástroja ExpressVPN[13]

Nástroj sme stiahli z predajní aplikácii pri oboch operačných systémoch. Inštalácia pozostávala zo štandardných krokoch. Po naštartovaní aplikácie museli sme najprv vytvoriť účet na základe čoho sme dostáli 7 dňové bezplatné použitie, po uplynutí spoločnosť ponúka mesačné predplatné ktorého cena závisí od dĺžky zvolenej licencie. Následne sme museli povoliť aplikácii aby nakonfigurovala údaje pre VPN, ktoré uskutočnila automatický, takže sme údaje nemuseli vnášať manuálne. Po nastavení VPN mali sme možnosť zvoliť si našu virtuálnu lokalitu. Aplikácia ponúka možnosť *Smart location*, kde nám na základe fyzickej vyberie najlepšiu lokalitu ktorá nebude mať veľkú odozvu. Tiež ponúka veľký výber z viac ako 130 lokalít, ktoré sú zachytené na Obrázku 8, medzi ktorými sa nachádza aj Slovensko. Keď sme si zvolili lokalitu, nástroj sme zapli veľkým tlačidlom. Po pripojení na zvolenú lokalitu nástroj sa spustil čo sme mohli vidieť v hornej časti zariadenia kde zasvietila ikonka VPN. Keď sme overili našu IP adresu, dostáli sme odpoveď že sa nachádzame v tom štáte kde je

[13] Zdroj obrázku 8: Autor práce

umiestnení aj server. Spoločnosť zaručuje vysokú bezpečnosť, pretože všetky údaje sú kryptované 256 bitovým zabezpečením. Pri testovaní sme zistili že aplikácia je stabilná a počas používania sa nestalo že prestála fungovať. Veľkou výhodou oproti iným aplikáciám je možnosť využívania služby bez dátového obmedzenia, takže nie je potrebné ju vypínať.

Aj napriek tomu, že nástroj ktorý by používateľom mal poskytovať anonymitu po pripojení do verejnej siete a ochrániť ich údaje pred útočníkom, existuje hrozba, že všetky odoslané a prijaté údaje, môže ukladať prevádzkovateľ aplikácie. Preto by si používatelia počas inštalácie mali prečítať všetky podmienky a zmluvy, s ktorými po zaškrtnutí súhlasí. V prípade nástroj ExpressVPN, prevádzkovateľ v zmluve píše, že všetky súkromné údaje používateľov žiadnym spôsobom neukladá a nevyužíva ich. V každom prípade by používatelia po pripojení do verejnej siete nemali používať aplikácie ktoré odosielajú súkromné informácie, alebo obmedziť ich použitie.

ZÁVER

Hlavnou témou diplomovej práce bolo otestovať bezpečnosť mobilných zariadení, po pripojení do bezdrôtovej siete pracujúcich na najzastúpenejších platformách. Na základe vykonaných testov sme mohli porovnať bezpečnosť zvolených platforiem medzi sebou a skonštatovať stupeň bezpečnosti.

Za účelom lepšieho a detailnejšieho porovnania použili sme zariadenia viacerých výrobcov, tiež rôzne verzie platforiem ako aj nastavenia a ďalšie zmeny vykonané priamo na zariadení. Pre samotné vytvorenie prístupového bodu porovnali sme dva nástroje pracujúce na odlišných operačných systémoch. V tomto prípade sa lepšie ukázal operačný systém Windows, ktorý ponúka oproti Linuxu veľký počet nástrojov používajúcich sa na tieto účely. Nástroj Connectify prejavil najlepší výkon aj na základe bežného používania a preto sme po využili aj pri tomto testovaní. Podobne ako nástroj Connectify, vysokú funkčnosť prejavil nástroj Wireshark, ktorý sme použili v druhej časti praktickej časti, pre odchytenie a analýzu sieťových paketov.

Každé zariadenie sme otestovali samostatne pri zvolenom časovom intervale. Po pripojení do siete všetky zariadenia začali aktívne komunikovať, odosielať a prijímať pakety, avšak na rozdiel od zariadenia výrobcu Nokia, pracujúca na platforme Windows Phone, ktorá počas testovania nepreukázala žiadnu aktívnu komunikáciu so sieťou. Väčšina paketov smerovaných na serveri bola totožná pri všetkých výrobcov, kde sa jednotlivé zariadenie pripájali na serveri výrobcov platformy alebo zariadenia. Pakety smerované na zariadenia boli v podobe bezpečnostných certifikátov, ktoré poskytovali bezpečný prenos, ako aj aktualizácie platformy, či aplikácií. Na druhej strane TCP pakety smerované zo zariadenia boli údaje v podobe médií odosielané do Cloudu. Keďže celý prenos paketov bol šifrovaný nebolo možné detailnejšie analyzovať o aké údaje išlo, ale na základe DNS požiadaviek zo strany zariadenia sme bližšie určili odoslané údaje.

Existuje mnoho metód a nástrojov, ktoré napomáhajú k zvýšeniu bezpečnosti zariadení. Najúčinnejším spôsobom je použitie VPN nástroja, ktorý pomocou tunelov a proxy serverov zabezpečuje anonymnú komunikáciu. Ďalším spôsobom ochrany údajov na zariadení je nastavenie Cloudových aplikácií aby automaticky neodosielali údaje po pripojení do siete, ale aby to používateľ manuálne vykonal po pripojení do bezpečnej siete, buď bezdrôtovo alebo za pomoci dátového kábla. Pri analýze paketov sme zistili, že niektoré zariadenia po pripojení do siete sťahovali a odosielali veľké

množstvo údajov, aby zamedzili nadbytočnú spotrebu dát na zariadení by nemalo byť vždy zapnuté bezdrôtové pripojenie, čo zároveň napomáha aj zníženiu pravdepodobnosti že by sa zariadenie mohlo stať cieľom rôznych útokov.

Každé zariadenie pracujúce na otestovaných platformách obsahuje nejakú časť čo znižuje bezpečnosť, buď sú to odosielané údaje, ktoré môže odchytiť útočník alebo rôzne povolenia zo strany platformy či aplikácií, ktoré môžu taktiež pristúpiť k rôznym častiam. Zistili sme, že zariadenia pracujúce na platforme Windows Phone sú najbezpečnejšie z hľadiska siete a preto by používatelia mali zvážiť aj túto platformu pri kúpe zariadenia. Pri platformách Android a iOS, ktoré sú aj najpoužívanejšie, preukazovali určitý stupeň ohrozenia, keďže automatický bez vedomia používateľa odosielali súkromné údaje. Avšak pri akceptovaní upozornení a aplikovaní navrhnutých bezpečnostných metód a nástrojov, každé zariadenie sa stáva tým najbezpečnejším.

ZOZNAM BIBLIOGRAFICKÝCH ODKAZOV

ADLI, M. K., NIYA, J. 2016. *Security bootstrapping of mobile ad hoc networks using identity-based cryptography*. Security and Communication networks. WILEY-BLACKWELL. 2016. ISSN 1939-0114.

ALISON. 2016. *Bezpečnosť mobilných zariadení*. Alison. 2016. [online]. [cit. 2016-09-17]. Dostupné na internete: <http://alison-group.sk/riesenia/bezpecnost/bezpecnost-mobilnych-zariadeni/>.

ALLIANCE, O. H. 2007. *Industry Leaders Announce Open Platform for Mobile Devices*. Open Handset Alliance. 2007. [online]. [cit. 2016-11-02]. Dostupné na internete: <http://www.openhandsetalliance.com/press_110507.html>.

AMERAH, A. A KOL. 2014. *Enhancing security of cookie-based sessions in mobile networks using sparse caching*. International journal of internet security. SPRINGER. 2014. ISSN 1615-5262.

ANDORID. 2016. *Verified Boot*. Android. 2016. [online]. [cit. 2016-02-11]. Dostupné na internete: <https://source.android.com/security/verifiedboot/index.html>.

ANDROID. 2016. *Android Security 2015 Year In Review*. Google. 2016. [online]. [cit. 2016-11-02]. Dostupné na internete: <https://static.googleusercontent.com/media/source.android.com/en//security/reports/Google_Android_Security_2015_Report_Final.pdf>.

ANDROID. 2016. *Android Security Bulletin-September 2016*. Android. 2016. [online]. [cit. 2016-09-06]. Dostupné na internete: <https://source.android.com/security/bulletin/2016-09-01.html>.

APPLE. 2016. *iOS Security*. Apple Inc. 2016. [online]. [cit. 2016-09-17]. Dostupné na internete: <http://www.apple.com/about/>.

APPLE INC. 2012. *802.1X Authentication*. Apple Technical White Paper. 2012. [online]. [cit. 2016-10-23]. Dostupné na internete: <http://training.apple.com/pdf/WP_8021X_Authentication.pdf>.

ARMASU, L. 2016. *All The New Security Improvements In Android N*. Tom's hardware. 2016. [online].[cit. 2016-11-02]. Dostupné na internete: <http://www.tomshardware.com/news/google-android-n-securityimprovements,31846.html>.

BAMBURIC, M. 2015. *Windows Phone security is top notch, says Kaspersky*. Beta news. 2015. [online]. [cit. 2016-11-03]. Dostupné na internete: <http://betanews.com/2015/06/11/windows-phone-security-is-top-notch-says-kaspersky/>.

BATES, P. 2016. *What Is The Most Secure Mobile Operating System?*. Make use of. 2016. [online]. [cit. 2016-10-15]. Dostupné na internete: <http://www.make useof.com/tag/secure-mobile-operating-system/>.

BICAKCI, K. A KOL. 2014. *Mobile Authentication Secure Against Man-In-The-Middle Attacks.* 9th International Conference on Future Networks and Communications. ELSEVIER SCIENCE BV. 2014. ISSN 1877-0509.

BURGESS, B. 2014. *What is Apple's iCloud Keychain and how do I use it?*. New atlas. 2014. [online]. [cit. 2016-10-23]. Dostupné na internete: <http://newatlas.com/ apple-icloud-keychain-ios7/30301/>.

CHORAS, M., KOZIK, R. 2013. *Evaluation of Various Techniques for SQL Injection Attack Detection.* 8th International conference on computer recognition systems cores. Springer INT. publishing AG. 2013. ISBN 978-3-319-00969-8.

CIRCLE, S. 2016. *A Eulogy: PrivatOS. June 1, 2014 - June 30, 2016 - Privacy Delivered*. Silent Circle. 2016. [online]. [cit. 2016-10-15]. Dostupné na internete: <https://www.silentcircle.com/blog/an-epitaph-privatos-june-1-2014-june-30-2016-privacy-delivered/>.

CSIRT.SK. 2016. *Bezpečnosť mobilných aplikácií*. CIRT. 2016. [online]. [cit. 2016-09-17]. Dostupné na internete: <https://www.csirt.gov.sk/bezpecnostnastudovna/ aplikacna-bezpecnost/bezpecnost-mobilnych-aplikacii-878.html>.

CONNECTIFY. 2017. *Connectify Hotspot*. Connectify. 2017. [online]. [cit. 2017-01-14]. Dostupné na internete: <http://www.connectify.me/hotspot/>.

COONEY, M. 2012. *10 common mobile security problems to attack*. PCworld. 2012. [online]. [cit. 2016-08-29]. Dostupné na internete: <http://www.pcworld.com/ article/2010278/10-common-mobile-security-problems-to-attack.html>.

CSSCORP. 2016. *Mobile Security Services*. CSS Corp. [online]. [cit. 2016-08-25]. Dostupné na internete: <https://www.csscorp.com/support-services/infra-support/mobility-services/mobile-security-services>.

DAR, M., PARVEZ, J. 2014. *Smartphone Operating Systems: Evaluation & Enhancements*. International Conference on Control, Instrumentation, Communication and Computational Technologies. IEEE. 2014. ISBN 978-1-4799-4190-2.

DEBIAO, H. A KOL. 2013. *Anonymous Two-factor Authentication for Consumer Roaming Service in Global Mobility Networks*. IEEE Transactions on Consumer Electronics. IEEE-INST ELECTRICAL ELECTRONICS ENGINEERS INC. 2013. ISSN 0098-3063.

DZYRE, N. 2016. *10 Tips To Tighten Security On Your Android Device*. Hongkiat. 2016. [online]. [cit. 2015-09-01]. Dostupné na internete: <http://www.hongkiat.com/blog/protect-your-android-device/>.

EVERS, J. 2005. *Microsoft to phase out Pocket PC, Smartphone brands*. InfoWorld. 2005. [online]. [cit. 2016-11-03]. Dostupné na internete:<http://www.infoworld.com/article/2668041/computer-hardware/microsoft-to-phase-out-pocket-pc--smartphone-brands.html>.

FALCONI, A. A KOL. 2016. *ECG Authentication for Mobile Devices*. IEEE Transactions on Instrumentation and Measurement. IEEE-INST ELECTRICAL ELECTRONICS ENGINEERS INC. 2016. ISSN 0018-9456.

FORREST, C. 2015. *Everything you need to know about Apple Airdrop*. TechRepublic. 2015. [online]. [cit. 2016-10-23]. Dostupné na internete:<http://www.techrepublic.com/article/everything-you-need-to-know-about-apple-airdrop/>.

GOODRICH, R. 2012. *5 Best Ways to Protect Your Smartphone*. TopTenReviews. 2012. [online]. [cit. 2016-09-01]. Dostupné na internete:<http://www.toptenreviews.com/software/articles/5-best-ways-to-protect-your-smartphone/>.

GOOGLE. 2016. *Google Inc.* [online]. [cit. 2016-09-17]. Dostupné na internete: <https://www.google.com/intl/en_rs/about/company/>.

GUZMAN, A. A KOL. 2016. *Network activity monitoring against malware in android operating system*. International Journal of Electrical and Computer Engineering. Institute of Advanced Engineering and Science. 2016. ISBN 20888708.

HARDWICK, T. 2016. *Zero-Day Acquisition Platform Triples iOS 10 Bug Bounty to $1.5 Million*. MacRumors. 2016. [online]. [cit. 2016-10-23]. Dostupné na internete: <http://www.macrumors.com/2016/09/30/zerodium-triples-ios-10-bug-bounty-to-1-5-million/>.

HEVESI, P. 2016. *Mobile Device Security: A Comparison of Platforms.*Gartner. 2016. [online]. [cit. 2016-09-10]. Dostupné na internete: <https://www.gartner.com/doc/3276422/mobile-device-security-comparison-platforms>.

HOFFMAN, C. 2016. *How to Encrypt Your Android Phone (and Why You Might Want to)*. How to geek. 2016. [onlne]. [cit. 2016-11-02]. Dostupné na internete: <http://www.howtogeek.com/141953/how-to-encrypt-your-android-phone-and-why-you-might-want-to/>.

HOLMES, M. 2013. *12 Ways to Protect Your Smartphone from Cyber Attacks*. Small Business trends. 2013.[online]. [cit. 2016-09-01]. Dostupné na internete: <http://smallbiztrends.com/2013/01/protect-smartphone-cyber-attack.html>.

JATINDER, S. A KOL. 2016. *Twenty Security Considerations for Cloud-Supported Internet of Things*. IEEE Internet of Things Journal. IEEE-INST ELECTRICAL ELECTRONICS ENGINEERS INC. 2016. ISSN 2327-4662.

JAYAPRAKASH, G. A KOL. 2015. *Forensic ready Secure iOS apps for jailbroken iPhones. ADVANCES IN DIGITAL FORENSICS XI*. SPRINGER-VERLAG BERLIN. 2015. ISBN 978-3-319-24123-4.

KALI. 2014. *Ghost Phisher*. Kali Tools. 2014. [online]. [cit. 2017-01-17]. Dostupné na internete: <http://tools.kali.org/information-gathering/ghost-phisher>.

KATINA, M., CLARKE, R. 2013. *Location and tracking of mobile devices: Uberveillance stalks the streets.* Computer Law & Security Review. ELSEVIER ADVANCED TECHNOLOGY. 2013. ISSN 0267-3649.

KENG-BOON, O., TAN, GHW. 2016. *Mobile technology acceptance model: An investigation using mobile users to explore smartphone credit card.* Journal of Service Management. PERGAMON-ELSEVIER SCIENCE LTD. 2016. ISSN 0957-4174.

KIM, S. A KOL. 2015. *Certificate sharing system for secure certificate distribution in mobile environment.* Expert Systems with Applications. PERGAMON-ELSEVIER SCIENCE LTD. ISSN 0957-4174.

KUDAKWASHE, M. A KOL. 2015. *Mobile Security Threats: A Survey of how Mobile Device Users are Protecting Themselves From new Forms of Cybercrimes*. 10th International Conference on Cyber Warfare and Security. ACAD CONFERENCES LTD. 2015. ISBN 978-1-910309-97-1.

LASTOVKA, Š. 2016. *8 jednoduchých krokov ako zvýšiť bezpečnosť mobilných zariadení*. Security news: 2016. [online]. [cit. 2016-09-01]. Dostupné na internete: <http://www.securitynews.sk/clanok/151_8-jednoduchych-krokov-ako-zvysit-bezpecnost-mobilnych-zariadeni>.

LICH, B. 2016. *Trusted Platform Module Technology Overview*. Microsoft. [online]. [cit. 2018-11-03]. Dostupné na internete: <https://technet.microsoft.com/en-us/itpro/windows/keep-secure/trusted-platform-module-overview>.

MARIANTONIETTA, L. P. A KOL. 2013. *A Survey on Security for Mobile Devices*. IEEE Communications Susrveys and Tutorials. IEEE-INST ELECTRICAL ELECTRONICS ENGINEERS INC. 2013. ISSN 1553-877X.

MICROSOFT. 2014. *Windows Phone 8.1 Security Overview*. Microsoft. 2014. [online]. [cit. 2016-11-03]. Dostupné na internete: <https://download.microsoft.com/download/B/9/A/B9A00269-28D5-4ACA-9E8E-E2E722B35A7D/Windows-Phone-8-1-Security Overview.pdfa_LHA&bvm=bv.137132246,d.bGg&cad=rja>.

MICROSOFT. 2015. *Secure the Windows 8.1 boot process*. Microsoft 2015. [online]. [cit. 2016-11-03]. Dostupné na internete: <https://technet.microsoft.com/en-us/windows/dn168167.aspx>.

MICROSOFT. 2016. *Multi-Factor Authentication*. Microsoft Azure. 2016. [online]. [cit. 2016-11-03]. Dostupné na internete: <https://azure.microsoft.com/en-us/services/multi-factor-authentication/>.

PHAM, M. 2015. *Under Attack: An interview with a hacker*. What mobile. 2015. [online]. [cit. 2016-10-15]. Dostupné na internete: <http://www.whatmobile.net/features/under-attack-an-interview-with-a-hacker/>.

PING, Y. A KOL. 2013. *An Intrusion Prevention Mechanism in Mobile Ad Hoc Networks*. Ad Hoc & Sensor Wireless Networks. OLD CITY PUBLISHING INC. 2013. ISSN 1551-9899.

ROEMMELE, B. 2013. *What is Apple's new Secure Enclave and why is it important?* Quora. 2013. [online]. [cit. 2016-10-23]. Dostupné na internete: <https://www.quora.com/What-is-Apple%E2%80%99s-new-Secure-Enclave-and-why-is-it-important>.

ROUSE, M. 2014. *TCP (Transmission Control Protocol).* Tech Target. 2014. [online]. [cit. 2017-02-03]. Dostupné na internete: <http://searchnetworking.techtarget.com/definition/TCP>.

SACCO, A. 2016. *Google details security features in Android 7.0 'Nougat'*. CIO. 2016. [online]. [cit. 2016-11-02]. Dostupné na internete: <http://www.cio.com/article/3108382/android/google-details-security-features-in-android-7-0-nougat.html>.

SAVOV, V. 2015. *Windows 10 makes its phone debut*. The Verge. 2015. [online]. [cit. 2016-11-03]. Dostupné na internete: <http://www.theverge.com/2015/1/21 /7865923/microsoft-windows-10-mobile-os>.

SHABTAI, A. A KOL. 2014. *Mobile malware detection through analysis of deviations in application network behavior*. Computers & Security. ELSEVIER ADVANCED TECHNOLOGY. 2014. ISSN 0167-4048.

SHELDON, R. 2016. *How Apple iOS encryption and data protection work*. Search Mobile Computing. 2016. [online]. [cit. 2016-10-23]. Dostupné na internete: <http://searchmobilecomputing.techtarget.com/tip/How-iOS-encryption-andata-protection-work>.

SHEN, J. 2016. *Orders for iris recognition chips to boost Xintec 2017 revenues, says report*. Digitimes. 2016. [online]. [cit. 2016-09-01]. Dostupné na internete: <http://www.digitimes.com/news/a20160830PM202.html>.

SIMS, G. 2012. *How secure is Android?*. Android authority. 2012. [online]. [cit. 2016-11-02]. Dostupné na internete: <http://www.androidauthority.com/secure-android-90523/>.

SMARTCEO. 2016. *Which mobile OS is most secure?*. SmartCEO. 2016. [online]. [cit. 2016-10-15]. Dostupné na internete: <http://www.smartceo.com/nextlogik-which-mobile-os-is-most-secure-ios-android-or-windows/>.

TECH4TEA. 2012. *BlackBerry OS vs iOS vs Windows Phone vs Android.* Tech4tea. 2012. [online]. [cit. 2016-10-15]. Dostupné na internete: <http://tech4tea.com /blog/2012/04/16/blackberry-os-vs-ios-vs-windows-phone-vs-android/>.

TIAGO, O. A KOL. 2016. *Mobile payment: Understanding the determinants of customer adoption and intention to recommend the technology*. *C*omputers in Human Behavior. PERGAMON-ELSEVIER SCIENCE LTD. 2016. ISSN 0747-5632.

WAGONER, A. 2014. *10 best ways to secure your smartphone*. Androidcentral. 2014. [online]. [cit. 2016-09-01]. Dostupné na internete: <http://www.androidcentral .com/10-best-ways-secure-your-smartphone>.

WIRESHARK. 2017. *About Wireshark*. WireShark. 2017. [online]. [cit. 2017-01-16]. Dostupné na internete: <https://www.wireshark.org/about.html>.

WRAY, R. 2010. *Google forced to delay British launch of Nexus phone.* The Guardian. 2010. [online]. [cit. 2016-11-02]. Dostupné na internete: <https://www.theguardian.com/technology/2010/mar/14/google-mobile-phone-launch-delay>.

YANRONG, L. A KOL. 2016. *Robust anonymous two-factor authenticated key exchange scheme for mobile client-server environment*. Security and Communication Networks. WILEY-BLACKWELL. 2016. ISSN 1939-0114.

ZIBREG, C. 2014. *An in-depth look at how Touch ID, A7, and Secure Enclave boost iOS security*. iDownloadBlog. 2014. [online]. [cit. 2016-10-23]. Dostupné na internete: <http://www.idownloadblog.com/2014/02/26/apple-ios-security-touch-id-specifics/>.

ZOZNAM PRÍLOH NA CD

Príloha A – Diplomová práca vo formáte .pdf

Príloha B – Abstrakt vo formáte .pdf

Príloha C – Nástroje Connectify a Wireshark

Príloha D – Súbor otestovaných zariadení v nástroji Wireshark