Univerzita Pardubice
Fakulta ekonomicko-správní
Ústav systémového inženýrství a informatiky

Bezpečnost mobilních zařízení

Aleš Hrdlička

Bakalářská práce
2017

Univerzita Pardubice
Fakulta ekonomicko-správní
Akademický rok: **2016/2017**

ZADÁNÍ BAKALÁŘSKÉ PRÁCE

(PROJEKTU, UMĚLECKÉHO DÍLA, UMĚLECKÉHO VÝKONU)

Jméno a příjmení:	**Aleš Hrdlička**
Osobní číslo:	**E13209**
Studijní program:	**B6209 Systémové inženýrství a informatika**
Studijní obor:	**Informační a bezpečnostní systémy**
Název tématu:	**Bezpečnost mobilních zařízení**
Zadávající katedra:	**Ústav systémového inženýrství a informatiky**

Zásady pro vypracování:

Bakalářská práce se zabývá zhodnocením bezpečnosti mobilních zařízení.

Zásady pro vypracování:
Popis současného stavu (základy mobilní bezpečnosti, bezpečnost jednotlivých operačních systémů, bezpečnostní software mobilních zařízení, bezpečnost mobilních aplikací, bezpečnost komunikačních přenosů, bezpečnost soukromých a firemních mobilních zařízení).
Komparace bezpečnosti mobilních zařízení či případová studie.
Formulace závěrů.

Rozsah grafických prací:

Rozsah pracovní zprávy: **cca 35 stran**

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

Seznam odborné literatury:

ALLEN, Grant. Android 4: průvodce programováním mobilních aplikací. Vyd. 1. Brno: Computer Press, 2013, 656 s. ISBN 978-80-251-3782-6.
ANDROULIDAKIS, Iosif I. Mobile phone security and forensics: a practical approach. New York: Springer, c2012, xi, 105 p. SpringerBriefs in electrical and computer engineering. ISBN 1461416493.
BITTO, Ondřej. Šifrování a biometrika aneb tajemné bity a dotyky. Vyd. 1. Kralice na Hané: Computer Media, 2005, 168 s. ISBN 80-86686-48-5.
MAISNER, Martin. Základy softwarového práva. Vyd. 1. Praha: Wolters Kluwer Česká republika, 2011, 339 s. Právní monografie (Wolters Kluwer ČR). ISBN 978-80-7357-638-7.
MAISNER, Martin a Zdeněk VANÍČEK. Odpovědnost za obsah přenosu v elektronických komunikacích. Vyd. 1. Praha: Wolters Kluwer Česká republika, 2012, xiv, 133 s. Právní monografie (Wolters Kluwer ČR). ISBN 978-80-7357-964-7.
MLÝNEK, Jaroslav. Zabezpečení obchodních informací. Vyd. 1. Brno: Computer Press, 2007, 154 s. ISBN 9788025115114.
PUŽMANOVÁ, Rita. Bezpečnost bezdrátové komunikace: jak zabezpečit wi-fi, bluetooth, GPRS či 3G. Vyd. 1. Brno: Computer Press, 2005, 179 s. ISBN 80-251-0791-4.
VÁVRŮ, Jiří. IPhone: vývoj aplikací. Vyd. 1. Praha: Grada, 2012, 179 s. Průvodce (Grada). ISBN 978-80-247-4457-5.
VÁVRŮ, Jiří. JQuery Mobile. Vyd. 1. Brno: Computer Press, 2013, 247 s. ISBN 978-80-251-3811-3.
Zdroje Internetu.

Vedoucí bakalářské práce: **Ing. Miloslava Kašparová, Ph.D.**
Ústav systémového inženýrství a informatiky

Datum zadání bakalářské práce: **4. září 2016**

Termín odevzdání bakalářské práce: **28. dubna 2017**

doc. Ing. Romana Provazníková, Ph.D.
děkanka

L.S.

doc. Ing. Pavel Petr, Ph.D.
vedoucí ústavu

V Pardubicích dne 4. září 2016

PROHLÁŠENÍ

Prohlašuji, že jsem tuto práci vypracoval samostatně. Veškeré literární prameny a informace, které jsem v práci využil, jsou uvedeny v seznamu použité literatury.

Byl jsem seznámen s tím, že se na moji práci vztahují práva a povinnosti vyplývající ze zákona č. 121/2000 Sb., autorský zákon, zejména se skutečností, že Univerzita Pardubice má právo na uzavření licenční smlouvy o užití této práce jako Školního díla podle § 60 odst. 1 autorského zákona, a s tím, že pokud dojde k užití této práce mnou nebo bude poskytnuta licence o užití jinému subjektu, je Univerzita Pardubice oprávněna ode mne požadovat přiměřený příspěvek na úhradu nákladů, které na vytvoření díla vynaložila, a to podle okolností až do jejich skutečné výše.

Beru na vědomí, že v souladu s § 47b zákona č. 111/1998 Sb., o vysokých školách a o změně a doplnění dalších zákonů (zákon o vysokých školách), ve znění pozdějších předpisů, a směrnicí Univerzity Pardubice č. 9/2012, bude práce zveřejněna v Univerzitní knihovně a prostřednictvím Digitální knihovny Univerzity Pardubice.

V Pardubicích dne 28. 4. 2017 Aleš Hrdlička

PODĚKOVÁNÍ:

Tímto bych rád poděkoval své vedoucí práce Ing. Miloslavě Kašparové Ph.D. za její odbornou pomoc, cenné rady a poskytnuté materiály, které mi pomohly při zpracování bakalářské práce.

ANOTACE

Mezi nepostradatelné pracovní nástroje současné doby patří chytré mobilní telefony a tablety. Umožňují nám rychlejší a efektivnější komunikaci a mobilní přístup k informacím. V současné době tato zařízení nahrazují do značné míry dříve nezbytné osobní počítače. Proto i u těchto mobilních zařízení, stejně tak jako u počítačů a notebooků, je vhodné zajistit bezpečnost a ochranu uživatele, určit správný způsob, jak zařízení nastavit, jak zabezpečit zařízení proti neoprávněnému vstupu, nebo přístupu jiných uživatelů prostřednictvím sítě nebo aplikací.

KLÍČOVÁ SLOVA

Mobilní zařízení, Bezpečnost, Operační systém, Firmware

TITLE

Mobile device security

ANNOTATION

In this work, I aim to highlight that smartphones and tablets are included amongst the most indispensable working tools. They allow us faster and more efficient communication and mobile access to information. Nowadays, these devices are replacing, to a large extent, the necessity of having personal computers. Accordingly, for these mobile devices as well as PCs and notebooks, it is appropriate to provide the user safety and security, to determine the correct way to secure the device against unauthorized entry, or access by other users over a network or application.

KEYWORDS

Mobile device, Security, Operating system, Firmware

OBSAH

SEZNAM TABULEK

SEZNAM OBRÁZKŮ

SEZNAM ZKRATEK A ZNAČEK

AES	Advanced encryption standard
AP	Access point
API	Application programming interface
APK	Android application package
ARM	Advanced RISC machine
ASLR	Address space layout randomization
BT	Bluetooth
BYOD	Bring you own device
CA	Certificate authority
CE	Consumer electronics
DES	Data encryption standard
DSA	Digital signature algorithm
ECID	Exclusive (or Electronic) chip identifier
EDGE	Enhanced data rates for GSM evolution
FBI	Federal bureau of investigation
FISH	Fibonacci shrinking
GID	Group identifier
GPRS	General packet radio service
GPS	Global positioning system
GSM	Groupe special mobile
HSPA	High speed packet access
HTTPS	Hypertext transfer protocol secure
HW	Hardware
IDEA	International data encryption algorithm
IMEI	International mobile equipment identity
IP	Internet protocol
IPC	Inter-process communication
IPS	In-plane switching
IPsec	Internet protocol security
IR	Infra-red
IS	Informační systém
IT	Informační technologie
JVM	Java virtual machine

L2TP	Layer 2 tunnel protocol
LCD	Liquid crystal display
LLB	Low level bootloader
LTE	Long term evolution
MDM	Mobile device management
MIPS	Microprocessor without interlocked pipeline stages
MMS	Multimedia messaging service
MT	Mobilní telefon
NFC	Near field communication
NT	New technology
OS	Operační systém
OTA	Over the air
OWASP	Open web application security project
PBKDF	Password base key derivation function
PC	Personal computer
PDA	Personal digital assistant
PIE	Position independent executable
PIN	Personal identification number
PPTP	Point to Point Tunneling Protocol
PUK	Personal unlocking key
RAM	Random access memory
RC4	Rivest Cipher 4
RFID	Radio-frequency identification
RISC	Reduced instruction set computing
RNG	Random number generator
ROM	Read-only memory
RSA	Rivest Shamir Adleman
SD	Secure digital
SE	Second edition
SHA	Secure hash algorithm
SIM	Subscriber identity module
SIP	Session initiation protocol
SMS	Short message service
SQL	Structured Query Language

SSL	Secure socket layer
SW	Software
TKIP	Temporal key integrity protocol
TLS	Transport Layer Security
UI	User interface
UID	Unique identifier
USA	United States of America
USB	Universal serial bus
VGA	Video graphics array
VOIP	Voice over internet protocol
VPN	Virtual private network
WEP	Wired equivalent privacy
WPA	Wi-Fi protected access
WVGA	Wide video graphics array
XNU	X is not UNIX

ÚVOD

Bezpečnost v oblasti IT, tedy i mobilních zařízení, je z části i mou pracovní náplní. Firma, ve které pracuji, má v této oblasti velmi vysoké nároky. Proto neustále vyhledávám články týkající se novinek o bezpečnosti, případných rizikách, bezpečných i nebezpečných aplikací, komplexní bezpečnosti mobilních zařízení i konkrétních verzí mobilních operačních systémů.

Během několika posledních let narostl několikanásobně objem mobilních zařízení, která naše firma využívá. Je nutné zaměřit se na jejich potenciální hrozby. Mezi nejčastější patří neoprávněné zneužití, odcizení, únik citlivých informací, nedůvěryhodné zařízení v podnikové síti, zařízení zapojená do nedůvěryhodné sítě, instalace nedůvěryhodných aplikací v zařízeních, ukládání dat do nedůvěryhodných uložišť.

Součástí mé pracovní náplně je také vytvoření konceptu bezpečnosti mobilních zařízení. Tento koncept nám nabídne konkrétní opatření, která mohou zcela či částečně eliminovat hrozby. Zvýší se tak především podniková bezpečnost. Zároveň s ním bude zaveden účinný systém správy mobilních telefonů „mobile device management“ (MDM), podpora BYOD (Bring You Own Device – přines si své vlastní zařízení), autentizace těchto vlastních mobilních zařízení pomocí aplikací správy mobilních zařízení do firemní sítě. Přínosem opatření je centralizovaná správa mobilních zařízení s plnohodnotnou kontrolou, monitorování všech firemních zařízení z jedné konzole v reálném čase, vzdálené ovládání či konfigurace mobilních zařízení, eventuální smazání jejich obsahu, ochrana firemních informací, zabezpečený přístup k sdíleným datům organizace a v podstatě také řízení jejich celého životního cyklu.

Cílem mé práce je zhodnocení bezpečnosti a komparace konkrétních mobilních telefonů. Přes teorii bezpečnosti v úvodní kapitole přejdu k bezpečnosti již konkrétních mobilních operačních systémů v kapitole druhé. Pomocí metody SWOT provedu ve druhé kapitole analýzu silný a slabých stránek, rizik a hrozeb. Ve třetí kapitole komparuji konkrétní zařízení zastupující dané operační systémy.

Součástí mé práce jsou přílohy popisující vývoj mobilních telefonů a operačních systémů od počátků až po současnost.

1 TEORIE BEZPEČNOSTI

V této kapitole se zaměřím na teorii bezpečnosti. První vysvětlím pojmy jako je bezpečnost, informační bezpečnost, řízení přístupu k informacím, škodlivý kód. Popíši základní teorii kryptografických nástrojů, hesel, pinů a biometrie. Budu se věnovat bezpečnosti bezdrátové komunikace, projektu OWASP Mobile Security a charakteristice analýzy SWOT.

1.1 Bezpečnost

Bezpečnost je stav, kdy je systém schopen odolávat známým a předvídatelným vnějším i vnitřním hrozbám, které mohou negativně působit proti jednotlivým prvkům nebo i celému systému tak, aby byla zachována struktura systému a jeho stabilita, spolehlivost a chování v souladu s cílovostí. Je to míra stability systému a jeho primární a sekundární adaptace.

Pro vymezení systému na podmínky státu je obsah bezpečnosti uveden v ústavním zákoně č. 110/1998 Sb., o bezpečnosti České republiky. V tomto případě používáme pojem vnější a vnitřní bezpečnost státu. [12]

1.2 Informační bezpečnost

V současné době patří zpracované, přenášené i uložené informace mezi nejcennější aktiva obchodních společností, výrobních firem, státní správy i ostatních společností. Firmy se snaží zajistit jejich důvěrnost, dostupnost i obsahovou neporušitelnost (integritu). V rámci platné legislativy, závazků vyplývajících ze smluv, je každá firma povinna chránit své informace. Je ale i v jejím vlastním zájmu tyto informace ochraňovat. Zabezpečení informací se nejčastěji provádí v rámci informačního systému (IS), který daná organizace užívá. V IS je integrována informační základna (data), technické i programové vybavení, interní předpisy a návody pro uživatele i správce. [21][30]

Chráněny jsou informace uložené nejen v informačních systémech, ale i informace vytištěné, psané, nebo jen uložené v něčí mysli. Je důležité zachovat bezpečnostní funkce, jako je důvěrnost, celistvost i dostupnost chráněných informací a zrovna tak i potřebné bezpečnostní mechanismy fyzického, logického, technického a administrativního charakteru. [21]

Bezpečnostními mechanismy fyzického charakteru jsou například zámky, trezory, bezpečnostní služba či alarmy, klimatizace, záložní zdroje a také protipožární ochrana.

Mechanismy logického charakteru jsou také nazývané jako software. Jsou jimi aplikace pro řízení přístupu, kryptografické služby, digitální podpisy, antivirové aplikace, firemní doménové účty, brána firewall v operačním systému, zálohovací systém a další.

Mezi mechanismy technického charakteru, též uváděné jako hardwarové, patří vstupní identifikační karty, autentizační kalkulátory pro zabezpečený přístup (např. do bankovnictví), firewall, konfigurovatelný switch s centrální správou, zálohovací fyzická média dat i aplikací.

Bezpečnostní mechanismy administrativního charakteru jsou bezpečnostní školení, postupy pro přijímání a propouštění zaměstnanců, autorizační postupy pro přístup do firemní sítě, konfigurace systému, právní normy, vyhlášky, zákony, dodržování licenční politiky. Patří sem také konkurenční zpravodajství, sběr a analýza rizik a statistik.[21][30]

1.3 Řízení přístupu k informacím

Řízení přístupu k informacím se zabývá vztahem mezi pasivními prvky informačního systému neboli objekty – uživateli, programy, procesy a aktivními prvky a subjekty – soubory, databázemi, záložními médii.

Zahrnuje identifikaci, autentizaci a autorizaci subjektu. Pod identifikací si můžeme představit zadání uživatelského jména do přihlašovací úvodní obrazovky informačního systému nebo mailové schránky. Zadáním hesla provedeme autentizaci. Je-li heslo správné, přihlásíme se do systému (schránky), tímto bude provedena autorizace.[21]

U bezpečnosti mobilních zařízení se setkáváme s autentizací pomocí grafických hesel, pinu, hesla, NFC technologie nebo také technologie BT, kontrolních otázek, biometrie (otisku prstu), rozpoznávání obličeje, rozpoznání hlasu, skrytých znaků v obrázcích.

1.4 Škodlivý kód

Stejně, jako u osobních počítačů a serverů, také u mobilních zařízení existuje zákeřný software, který je určen k vniknutí do operačního systému, konkrétní aplikace. Obecně se označují anglickým názvem malware. Mezi malware patří viry, trojské koně, reklamní bannery či celé aplikace, značené jako adware, nebo také programy (části aplikací), sloužící pro odesílání statistik a konkrétních požadovaných dat bez vědomí uživatele, označovaný jako spyware. [21]

Důvod, proč vlastně tento škodlivý kód stále putuje světem v našich zařízeních, je různý. První z nich je bezpečnost státu. Za bezdůvodného škůdce můžeme označit programátora,

který tak vyjadřuje nesouhlas s určitou situací, nebo je ovlivněn jakousi komunitou. Také se objevují jedinci, kteří si ověřují své schopnosti, a individua, jež se rozhodla obohatit na neznalosti jiných lidí. Psychickým nátlakem se snaží z nich vylákat peníze. Někdy může být škodlivý kód vyvíjen pro účely diskreditace platformy. Ta tak ztrácí zájemce, není považována za dostatečně bezpečnou.

Je vždy potřeba zvažovat otevírání neznámých mailů, odkazů, cizích (nedůvěryhodných) webových stránek. Doporučuje se stahovat aplikace jen z ověřených zdrojů, obchodů daných platforem. Zde jsou veškeré aplikace testovány a certifikovány. Zásadní je zajímat se o stav našeho zařízení, stahovat a instalovat aktualizace firmware a hlavně zálohovat. Antivirové firmy nabízí verze mobilních antivirů, které mohou pomáhat v rozpoznání potenciálně nebezpečné aplikace. Je možné je stáhnout v bezplatných i placených verzích z oficiálních obchodů.

1.5 Kryptografické nástroje

Kryptografické nástroje se užívají především k zajištění důvěrnosti, integrity a autentičnosti informací, jejich nepopiratelnosti původu (nelze posléze autorem popřít autorství), autentizaci entit (uživatelé IS, počítače, počítačové aplikace).

Kryptografie (tvoření bezpečnostních algoritmů) je součást vědního oboru kryptologie, který zahrnuje rovněž oblast kryptoanalýzy (analýza bezpečnostních algoritmů). Kryptoanalýza šifrovacích strojů má výrazný podíl na vzniku a následném vývoji elektronických počítačů. S rozvojem výpočetní techniky v druhé polovině 20. století přichází nové možnosti. Moderní kryptografické metody jsou založeny nejčastěji na teorii čísel. Mezi základní nástroje patří jednosměrné funkce, kontrolní součty, šifrovací algoritmy a algoritmy digitálního podpisu.

Obecný šifrovací proces může mít následující kroky. Nejprve je na otevřený text aplikován uživatelem algoritmus s využitím klíče. Vznikne tak šifrovaný text, který může cestovat otevřeným kanálem k příjemci. Ten na text aplikuje dešifrovací postupy s využitím klíče a získá otevřený text. Podle toho, zda jsou klíče obou stran stejné či nikoliv, rozlišujeme symetrickou a asymetrickou kryptografii. Dále rozlišujeme šifry proudové (kryptografie probíhá po jednotlivých bitech) a blokové (rozšíření předchozí metody s rozdělením na bloky s pevně stanoveným počtem bitů). Mezi nejznámější patří FISH, RC4, DES, Triple DES, IDEA, Blowfish. Problematika kryptografie je podrobněji popsána například v knize Bruce Scheiera – Applied Cryptography.[13][44]

1.6 Hesla, PIN a biometrie

Hesla jsou obecným prostředkem autentizace uživatele, kterým nemusí být pouze člověk. Uživatel je pokládán za oprávněného, prokáže-li znalost hesla. Bezpečnost autentifikace pomocí hesla je závislá na síle hesla, zabezpečení na straně uživatele i systému během jeho ověřování.

PIN (Personal Identification Number) neboli osobní identifikační číslo je další možností autentizace uživatele. Jedná se o posloupnost číslic volně definovatelnou uživatelem. Bývá obvykle čtyřciferný, ale může mít i více míst. Používá se nejčastěji u platebních karet, vstupních kódů, přihlašování do Windows, v mobilních telefonech apod. U SIM karet je v případě opakovaného špatného zadání PIN kódu vyžadováno zadání následného PUK (Personal Unlocking Key) osobního odblokovacího klíče.

Ověření identity pomocí biometrie nabízí výrazně vyšší úroveň bezpečnosti v porovnání s tradičními metodami. Pro autentizaci otisků prstů se užívá několik metod. Obraz detekcí teplotních rozdílů, přímý optický snímek nebo měření nepatrné změny elektrického náboje na povrchu prstu. Uživatel přejede prstem po čidle, který je tvořen jedním mikročipem. Pokrývá jej teplotně citlivá vrstva sestavená z 14 000 zobrazovacích prvků. Čip konvertuje zaznamenané nepatrné teplotní rozdíly na 50 až 100 obrazových řezů, které ukazují charakteristické čáry. Během desetiny sekundy speciální software složí tyto řezy do celkového snímku. Následně je zpracován snímek pomocí složitého algoritmu a vytvořen digitální identifikační kód.[13]

1.7 Bezpečnost bezdrátové komunikace

Bezdrátové sítě jsou všude kolem nás. Jsou využívány v domácnostech, telekomunikačních sítích a společnostech. Spojení je uskutečňováno nejčastěji pomocí elektromagnetických vln. Bezdrátové sítě slouží pro zasílání a sdílení dat i komunikaci online. Podrobnější charakteristiky bezdrátových sítí, způsob jejich zabezpečení a šifrování, je možné získat například z knihy Rity Pužmanové – Bezpečnost bezdrátové komunikace.[39]

1.7.1 Bezdrátové sítě WLAN

Hlavním důvodem využívání bezdrátových sítí je jejich vysoká rychlost za velmi příznivé ceny oproti cenám za připojení mobilních operátorů. V poslední době bývají tyto sítě ve městech poskytovateli často nahrazovány optickou sítí. Ty umožňují stabilnější připojení

s větší propustností dat. Bezdrátové sítě zůstávají přístupovými body uživatelů v domácnostech či firmách.

Ve stávajících řešeních se nejčastěji využívá normy IEEE 802.11(a/b/g/n/y/ac/ad), konkrétně stále nejvíce rozšířené jsou IEEE 802.11b/g/n, a to jak v domácnostech, tak i firmách. Velkým problémem bezdrátových sítí je jejich zabezpečení.

Základní zabezpečení bezdrátové sítě je šifrování WEP (Wired Equivalent Privacy – soukromí ekvivalentní drátovým sítím). Toto zabezpečení, které se používalo od počátků bezdrátových sítí, je již zastaralé. Pracovalo se šifrou RC4. Dnes se již nepoužívá z důvodu snadného prolomení.

Pokročilejším zabezpečením bezdrátové sítě je šifrování WPA (Wi-Fi Protected Access). Bylo náhradou prolomeného zabezpečení WEP. Dalo se využít po pouhé aktualizaci obslužného software na zařízeních, která podporovala šifrování RC4. Pro eliminaci slabých míst obsahoval také protokol TKIP (Temporal Key Integrity Protocol). Ten zabezpečoval komunikaci mezi klientem a bodem nejen na začátku komunikace, ale i během ní. Ani toto šifrování není považováno za bezpečné. Autentizace klienta je pro WPA navržena s použitím předsdílené fráze (Pre-shared key) nebo s autentizačním serverem (typicky RADIUS). Po prolomení šifrování WPA a vydání WPA2 s protokolem Advanced Encryption Standard (AES), byl tento protokol doplněn i k šifrování WPA.

Šifrování WPA2 s protokolem AES je stále považováno za bezpečné. Je důležité použít silného hesla proti napadení hrubou silou, které je jeho slabinou. Šifrování protokolem AES je stále využíváno například na šifrování disků aplikací TrueCrypt. Stále je světově uznávaným šifrovacím standardem, který byl akceptován i US vládou.

Běžně doporučované šifrování je kombinované šifrování WPA-WPA2-PSK (TKIP/AES), které nové prvky také podporují. Poskytuje maximum kompatibility s historickými zařízeními. Nabízí však útočníkovi možnost prolomit síť pomocí nejslabšího článku šifrovacího obvodu. Proto, máme-li moderní síťové prvky, preferujeme bezpečné šifrování WPA2-PSK(AES).[39]

1.7.2 Mobilní datová síť

První, a také nejpomalejší z dostupných datových sítí, je síť GSM (Global System for Mobile Communication). Nabízí jen velice pomalé datové spojení rychlostí 9,6 + 9,6 kb/s. Dnes se tato síť stará jen o hlasové služby. Pokročilejší službou, s označením 2,5G s propustností 50 + 25 kb/s, je GPRS (General Packet Radio Service). V dnešní době je použitelná v podstatě jen na malé maily a velmi pomalé surfování. Je dostupná všude tam, kde je pokrytí signálem

GSM. Další, mírně upravenou verzí služby GPRS, je služba EDGE. Nabízí teoretickou rychlost až 238,6 + 119,3 kb/s. Ani EDGE není dnes použitelná pro běžné surfování a vyřizování pošty větších objemů dat. Občas bývá označována jako 2,75 generace. První použitelnou datovou sítí je síť 3. generace, označována jako 3G. Ta nám umožňuje bezdrátový přenos hlasu a dat, video telefonii i mobilní televizi s rychlostí vyšší než 200 kb/s. Následníkem této sítě je síť 3,5G nebo 3,75G označována jako HSPA (High Speed Packet Access). Její teoretická rychlost je v řádu jednotek Mb/s. Novější variantou služby je služba HSPA+. Teoretická propustnost na stahování dat je 84,4 - 168 Mb/s a odesílání 22 Mb/s. Aktuální čtvrtou generací datových služeb, je standard 4G označován jako LTE (Long Term Evolution). Její propustnost dat je až 225 Mb/s a rychlost odesílání je 50 Mb/s.[39]

1.7.3 Přístupový bod a hotspot

Přístupový bod označovaný jako AP (Access Point) je připojení drátové či bezdrátové, které umožňuje připojení zařízení do internetu.

Hotspot je fyzické místo, kde se lidé mohou připojit do internetu. Typicky jsou to Wi-Fi sítě. K těmto místům patří například kavárny, hotely, restaurace, obchody. Zde se můžeme zdarma nebo za poplatek připojit k internetu. Je třeba si uvědomit, že připojení nemusí být vždy bezpečné. Je zde riziko monitorování síťového provozu. Může tak dojít k odcizení zadávaných hesel. Existují také možnosti, jak zfalšovat jakýkoliv hotspot. Po připojení k zfalšovanému bodu se nevědomě odevzdáme do rukou útočníka. Osobní hotspot si můžeme vytvořit i v chytrém mobilním telefonu. V případě nastavení vlastního přístupového bodu je nutné dbát na bezpečnost (šifrování, síla hesla).

1.7.4 BLUETOOTH, NFC

Pomocí vlastního telefonu nebo prostřednictvím jiných zařízení je možné zprostředkovat datové spojení technologií BT. Ta má teoretickou propustnost dat rozlišenou dle verzí. Poslední dostupná verze BT v5.0 má, oproti předchozí verzi 4.2, čtyřnásobný dosah a dvojnásobnou propustností dat (cca 2 Mb/s). Tato technologie se využívá především u bezdrátových klávesnic, myší, bezdrátových sluchátek, autorádií, datových přenosů, pro synchronizaci PDA zařízení, připojení na internet, přenos hudby mezi mobilními telefony a moderními přehrávači, které způsob komunikace podporují. Zabezpečení BT je v podstatě jednoduché. Zařízení se páruje na obou stranách proti sobě. K párovanému zařízení není možné se připojit, dokud na tomto zařízení nebude povoleno párování. Po aktivaci funkce párování je limitován čas,

po který je zařízení viditelné okolním zařízením. Spárovaná zařízení komunikují ve skrytém režimu, není již dále viditelné pro ostatní nespárovaná zařízení.

Technologie NFC (Near Field Communication) je využívána na velmi krátkou vzdálenost (do cca 4 cm) s přiblížením přístrojů. Předpokládané a současné využití bylo určeno především k výměně klíčových dat při bezkontaktních finančních transakcích a také jako náhrada starších bezkontaktních RFID čipů.[39]

1.8 OWASP Mobile Security Project

Základem testování bezpečnosti mobilních aplikací je OWASP Mobile Security Project. Je vytvořený neziskovou organizací OWASP. Ta je známa především svou prací v oblasti zabezpečení webových aplikací. Projekt představuje bezplatný a centralizovaný zdroj informací, klasifikuje bezpečnostní rizika mobilních aplikací a dokumentuje postupy pro bezpečný vývoj. Snižuje se tak dopad i pravděpodobnost výskytu zranitelností. Zaměřuje se především na aplikační vrstvu. Nepopisuje bezpečnostní rizika mobilních platforem. Ta nejzávažnější v oblasti bezpečnosti jsou identifikována a kategorizována. Dostupná jsou jako OWASP Top 10 Mobile Risks.[33]

Aktuální verze dostupných rizik naleznete na stránkách společnosti viz obrázek 1.

Obrázek 1: OWASP Mobile Top 10 2016

Zdroj:[33]

M1 - Improper Platform Usage

Tato kategorie se soustředí na zneužití funkcí mobilního operačního systému nebo nedostatku bezpečnostních kontrol platforem Android či iOS. Problémy mohou zahrnovat zneužití Keychain na iOS (více viz kapitola 2.1.2 – Bezpečnostní prvky) nebo Android Intenty (více viz kapitola 2.2.2. – Bezpečnostní prvky).

M2 – Insecure Data Storage

Podle zprávy NowSecure Mobile Security 2016 má 25 procent mobilních aplikací nejméně jedno vysoké bezpečnostní riziko ochrany osobních údajů. Tyto chyby mohou mít za následek únik osobních informací, které mohou být použity k nedovoleným účelům.[1]

M3 – Insecure Communication

Nezabezpečené komunikace zahrnují nechráněná data v tranzitu. Příkladem je odesílání komunikace ve formě prostého textu.

M4 – Insecure Authentication

Mobilní aplikace potřebují bezpečně identifikovat uživatele, zejména pokud uživatelé volají nebo posílají citlivá data jako například finanční informace.

M5 – Insufficient Cryptography

Existují dva typy chyb, které v této kategorii může vést útočník, aby získal přístup k citlivým informacím z mobilní aplikace z důvodu nedostatečné ochrany osobních údajů. Zranitelnost může ovlivnit proces šifrování/dešifrování, anebo slabý algoritmus šifrování/dešifrování.

M6 – Insecure Authorization

Nezabezpečené autorizace, které se liší od M4, se vztahují k selhání serveru v řádném vynucení identity a oprávnění, jak je vyžadováno mobilní aplikací. Zatímco M4 se týká ověření uživatele v rámci aplikace, M6 pokrývá autorizaci komunikace mezi aplikací a back-end servery. Například k tomu může dojít, pokud server umožňuje slepě mobilní aplikaci podávat žádosti.

M7 – Client Code Quality

Do této kategorie patří riziko vyplývající ze zranitelností, jako je přetečení vyrovnávací paměti, formátování řetězců zranitelnosti a různé další chyby kódu na úrovni, kde může být díky zranitelnosti vykonán kód na mobilním zařízení. Dle OWASP umožňuje špatný kód útočníkům zneužít obchodní logiky a potenciálně obejít bezpečnostní kontroly vynucené na zařízení.

M8 – Code Tampering

Útočníci mohou instalovat zadní vrátka (backdoor) nebo je jinak manipulovat a následně znovu podepsat a publikovat aplikace třetích stran se škodlivým kódem. Takové útoky jsou typicky zaměřovány na oblíbené aplikace a finanční aplikace. Vývojáři by měli využívat

techniky proti neoprávněné manipulaci a neoprávněnému zásahu detekcí a ochranou provádění nelegitimních aplikací.

M9 – Reverse Engineering

Pokud útočník může snadno použít reverzní inženýrství na aplikace, znamená to, že může analyzovat zdrojový kód aplikace, knihovny, algoritmy a další. S hlubší znalostí aplikace, jak funguje, může útočník mnohem jednodušeji identifikovat nedostatky, které může zneužít.

M10 – Extraneous Functionality

Vývojáři často používají zadní skrytá vrátka nebo bezpečnostní kontroly, které jsou užitečné v průběhu fáze vývoje, ale nemají je v plánu uvolnit do výroby. Pokud je tato funkce omylem spuštěna, mohou útočníci kompromitovat aplikaci. Příkladem může být zablokování dvoufázové autentifikace v průběhu testování.

Seznamy podobné OWASP Mobile Top 10 nebo NowSecure – Secure Mobile Development Best Practices, jsou dobrými zdroji aktuálně největších bezpečnostních problémů. Jsou to silné základní minimální kontrolní seznamy, které lze použít při tvorbě programu bezpečnosti mobilní aplikace. Existuje mnoho dalších nebezpečí, která v nich nejsou uvedena. Přesto si jich odborníci na bezpečnost musí být vědomi.[33]

1.9 Analýza SWOT

Tato analýza se využívá ke zmapování všech faktorů, na kterých při boji s konkurencí můžeme stavět a které nám jsou překážkou. Zkratka SWOT je odvozena z anglických názvů Strengths (silné stránky), Weaknesses (slabé stránky), Opportunities (příležitosti) a Threats (hrozby). Ty značí také jednotlivé kvadranty, které si musíme určit.[19][47]

V rámci druhé kapitoly provedu SWOT analýzu bezpečnosti operačních systémů.

Silné stránky

Identifikují oblasti, v nichž jsme obecně lepší než konkurence. Patří sem schopnosti, dovednosti, znalosti, zdroje, potenciál, dosažené úspěchy (unikátní know-how), silná značka, certifikace jakosti či vysoce kvalitní produkt nebo služba. Skutečnou silnou stránkou je to, čím vybočujeme z průměru. Mezi silné stránky patří také zavedený produkt, významné postavení na světovém trhu kladné reference zákazníků, škálovatelnost produktu (schopnost přizpůsobit se rychle a pružně požadavkům zákazníka) a technologické know-how.

Slabé stránky

Slabé stránky jsou opakem silných. Jsou jimi oblasti, ve kterých si firma, produkty nebo služby vedou hůře než konkurence. Mezi ně patří vysoké náklady a nedostatek marketingových zkušeností a další. Platí pravidlo, že naše silné stránky jsou slabinami konkurence a naopak. Mezi slabé stránky patří špatná distribuce, specializace na střední firmy, firma nedostatečně využívá marketingu k získávání nových zákazníků, nebo má nedostatečné výrobní kapacity.

Příležitosti

Příležitosti představují skutečnosti, které mohou firmám přinést úspěch, dokážou-li je najít a využít. Mezi ně patří technologický vývoj, nenaplněné potřeby zákazníků, módní trendy, nové trhy, pokračovat v expanzi do dalších zemí, nové segmenty trhu, zajištění dlouhodobé věrnosti zákazníků, neustálé zkvalitňování výrobků. K dalším příležitostem řadíme náskok před konkurencí, spolupráce s partnery na vývoji, nové technologie, dotační programy na technologie a vzdělávání.

Hrozby

Hrozby jsou skutečnosti, které mohou mít za vliv snížení poptávky, způsobují nespokojenost zákazníků, ohrožují ekonomickou stabilitu firmy. Mezi typické hrozby patří aktivity konkurentů, změny zákaznických preferencí, živelné pohromy nebo regulační opatření a obchodní bariéry. Jsou to také bariéry vstupu, nutnost certifikací, patenty konkurence, kurzy měn, přístup k novým technologiím, zlepšení nabídky ze strany stávající konkurence.[19][47]

2 BEZPEČNOST OPERAČNÍCH SYSTÉMŮ iOS A ANDROID

V této kapitole se zaměřím na bezpečnost jednotlivých operačních systému iOS a Android. Popíši jejich architekturu a bezpečnostní prvky.

2.1 Bezpečnost operačního systému iOS

Operační systém iOS firmy Apple byl vyvinut tak, aby maximálně ochraňoval uživatele. Přitom ho jen minimálně omezoval v jeho práci a chránil, jak jen je možné, jeho data. Šifrování dat zařízení iPhone, iPAD či iPOD je implicitní a není jej možné v zařízeních konfigurovat. V podstatě se nepředpokládá, že by uživatel, který chce svá data chránit, používal zařízení se systémem iOS bez nastaveného vstupního hesla nebo otisku prstu. Uživateli nechráněného zařízení nezáleží na jeho vlastní bezpečnosti, ochraně dat, zabezpečení proti krádeži a ztrátě.

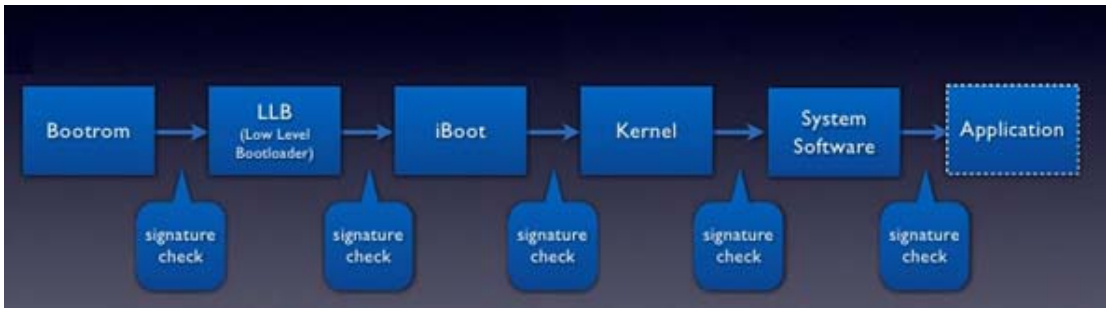
2.1.1 Architektura operačního systému iOS

Systém iOS je pevně spjat se zařízeními společnosti Apple. Díky tomu dochází k těsné integraci software s hardware. Je tak možné používat všechny ověřovací vrstvy daných zařízení. Po spuštění boot-up procesu dojde k ověření základních parametrů zařízení, jako například UID přístroje a následně dále v jednotlivých krocích najíždí systém. Každý krok je analyzován a prověřen z hlediska důvěryhodnosti. Po naběhnutí systému se o jeho bezpečnost i důvěryhodnost stará XNU (X is not UNIX – jádro operačního systému vyvíjené společností Apple). Za běhu vyhodnocuje bezpečnost a je důvěryhodné pro všechny ověřovací vrstvy, funkce i aplikace. [22]

Secure Boot Chain

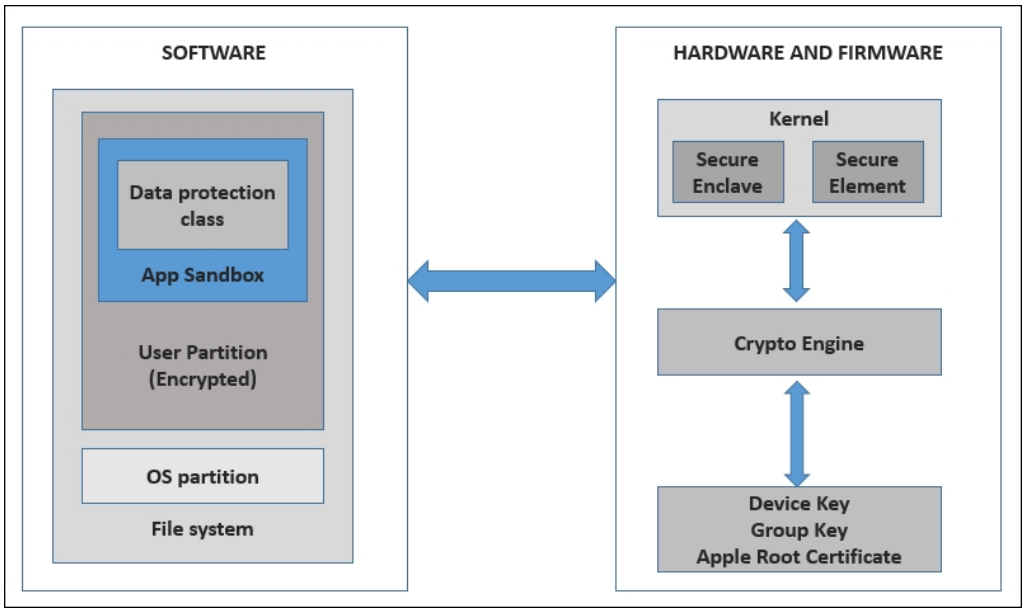
Boot-up proces obsahuje pouze komponenty odepsané společností Apple a probíhají řetězcem důvěry. Řetězec obsahuje základní zavaděče, jádro i s rozšířením a firmware. První kontrolou prochází Boot ROM kód, který je uložen v paměti. Ten je přístupný pouze pro čtení (read-only), je nezměnitelný, součástí čipu. Implicitně je nastaven jako důvěryhodný. Jeho obsahem je veřejný klíč (Apple Root CA), který se používá při ověřování LLB (Low level Bootloader), prvního kroku ověřovacího řetězce. Dalším krokem je „iBoot", který ověřuje a zabezpečuje, že není za provozu manipulováno s nejnižšími úrovněmi software a také tento systém není spouštěn na nepodporovaných zařízeních. Je-li vše v pořádku, dojde ke spuštění jádra systému, následně systému software i aplikací. Neověří-li systém některý z kroků zaváděcích procesů, nabíhání zařízení se zastaví. Zařízení informuje o nestandartním chování, potřebou obnovy systému do továrního nastavení. Vše je názorně

zobrazeno na obrázku 2, který popisuje řetězec bezpečného načtení systému. Obrázek 3 popisuje bezpečnost systému iOS.[22]



Obrázek 2: Popis řetězce bezpečného načtení systému

Zdroj:[10]



Obrázek 3: Popis modelu bezpečnosti systému iOS

Zdroj:[37]

Proces aktualizace software zařízení

Systém je díky aktualizacím neustále vylepšován. Opravují se objevené bezpečnostní díry. Aktualizace jsou vydávány na všechna podporované zařízení najednou. Instalují se díky aplikaci iTunes nebo také přímo v telefonu. Po vydání aktualizace informuje zařízení o její dostupnosti. Po souhlasu uživatele s jejím stažením sám vyzve k aktualizaci. Při spuštění aktualizace se zařízení připojí na server Apple a zašle kryptografický seznam pro všechny její části instalace. Server provede porovnání této verze s dostupnými verzemi. Prověří podepsání instalačního balíku výrobcem i s potřebným povolením ECID. Takto vytvořená,

schválená konečná sada se následně do zařízení stáhne a nainstaluje. Díky tomu nemůže být na těchto zařízeních instalován jiný operační systém než dodávaný výrobcem.[22]

2.1.2 Bezpečnostní prvky

Mezi bezpečnostní prvky patří podepisování aplikací společností, prověřování bezpečnosti běžících procesů, šifrování souborů, ochrana dat, vstupní hesla, třídy, keychain data protection a keybags a zabezpečení sítě.

Podepisování aplikací společností

Všechny aplikace, které lze instalovat do systému iOS, musí obsahovat spustitelný kód ověřený společností Apple. Aplikace třetích stran používají pro ověření důvěryhodnosti certifikát vydaný společností Apple. Toto je jediná možnost instalace aplikací do zařízení. Není možno spouštět nebo instalovat aplikace z webu, spouštět stažené aplikace a nedůvěryhodný kód. Certifikát ověření pravosti aplikací vývojáře vydává sama společnost Apple po registraci uživatele do vývojářského programu. Po ověření vývojáře je vydán certifikát, na jehož základě může vystavovat aplikace přes App Store. I přesto jsou zde aplikace testovány a ověřovány pro co nejvyšší možnou bezpečnost. Firmy mají ještě jeden způsob označovaný jako in-house (v domě). Po registraci a následném prověření společnosti může firma instalovat do zařízení profil, který umožní instalovat a spouštět vlastní vyvinuté aplikace bez potřeby je vystavovat a instalovat přes App Store. [22]

Prověřování bezpečnosti běžících procesů

Přestože jsme nainstalovali ověřenou aplikaci z důvěryhodného zdroje, prochází vynuceně nadále sledováním operačním systémem. Ten má za úkol zajistit vzájemnou bezpečnost mezi aplikacemi a celým systémem. Aplikace třetích stran jsou striktně omezovány na přístup k datům zařízení a mají také velmi malá práva k provádění změn na zařízení. Aplikace nemohou shromažďovat, nebo jakkoliv měnit data o jiných aplikacích. Každá aplikace má vytvořenou složku samostatně a také do ní si ukládá veškeré své soubory. V případě požadavku mimo adresář musí tato aplikace využít služeb poskytovaných systémem právě k tomu určených. Systémové složky jsou chráněny, oddíl systému krom několika nástrojů je připojen pouze pro čtení, což znemožňuje změny v souborech. [22]

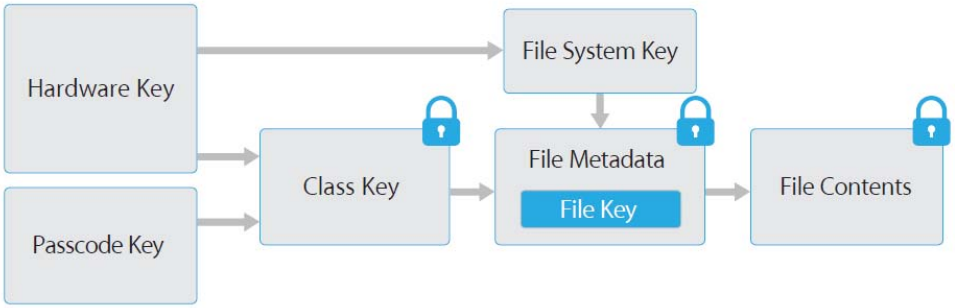
Šifrování souborů

Kromě ochrany počátečními bezpečnostními prvky jako „Secure boot chain“ či „Runtime process“ obsahuje systém iOS i další bezpečnostní prvky ochrany uživatelských dat. Mezi tyto prvky patří šifrování souborů a zabezpečení různými typy klíčů. Umožňují

je integrované vrstvy softwarových a hardwarových technologií. Šifrovací neboli kryptografické operace jsou velice náročné na početní výkon zařízení. To vede ke snižování výkonu zařízení a také výdrže baterií, které jsou pro mobilní zařízení jedním z nejdůležitějších parametrů a je potřeba je efektivně využívat. Každé zařízení má jedinečné ID (UID – unit ID) a šifrovací 256bitový AES klíč vytvořený již při výrobě samotného čipu. Umožňuje tak data šifrovat s vazbou na konkrétní zařízení. V případě přemístění paměťového čipu do jiného zařízení budou data nečitelná. Dalším je GID (Group IDentifier) - identifikační číslo celé skupiny zařízení. Obě tyto ID nelze vyčíst pomocí software nebo úpravou firmware, zobrazují se pouze výsledky šifrování/dešifrování. Také se v zařízeních vytváří další klíče pro šifrování, a to pomocí generátoru náhodných čísel RNG (Random Number Generator). Systém taktéž disponuje službou zaměřenou na bezpečné mazání nepoužívaných klíčů. Je důležité, aby byl klíč bezpečně odstraněn a nemohlo dojít k jeho zneužití. [22]

Ochrana dat

Tato technologie byla vyvinuta speciálně pro mobilní zařízení. Neustále se připojují k internetu. Uskutečňují telefonní hovory, zpracovávají krátké textové zprávy či emaily. Proto bylo nutné vytvořit technologii reagující na události bez potřeby dešifrování citlivých dat, dodatečného stahování nových informací, a to i přes zamčené zařízení. Data jsou rozdělena do tříd dle jejich citlivosti. Každá třída má vlastní zabezpečení. Vytváří se 256bitový klíč pro každý nově vytvořený oddíl dat s následným předáním AES, který soubor pomocí tohoto klíče zašifruje. Šifrovací klíč je zabalen společně s dalšími klíči, dle restrikcí k otevření daného souboru a jeho uložení do souborových metadat. Pokud je soubor otevřen, rozbalí se metadata a ta jsou následně dešifrována klíčem systému souborů, hledáním klíče dané třídy souboru. Veškerá metadata jsou také zašifrována náhodným klíčem, generovaným při instalaci systému na zařízení. Nepoužívá se však pro zabezpečení důvěryhodných dat, je uložen přímo v zařízení, a tak by mohlo dojít k jeho zneužití. Je možnost jej však uživatelsky jednoduše a rychle odstranit, a tak se veškeré soubory stanou kryptograficky nepřístupné. Obsah každého souboru je šifrován klíčem vnořeným do třídy klíčů chráněných pomocí UID, někdy navíc i heslem. Chráněný klíč je uložen v metadatech souboru. Ty jsou šifrovány dalším klíčem systému souborů (viz obrázek 4). Hierarchie poskytuje požadovanou flexibilitu i výkon. [22]



Obrázek 4: Schéma architektury kódování

Zdroj:[7]

Vstupní hesla

Po zapnutí zařízení je uživatel vyzván k zadání číselného kódu o minimální délce čtyř znaků. Vložením korektního kódu dojde k odemčení zařízení. Pro hesla lze použít širokou škálu alfanumerických znaků neomezené délky. Kód také poskytuje entropii pro šifrovací klíče, které nejsou uložené v tomto zařízení. Zařízení obsahují technologii zabraňující prolomení pomocí tzv. hrubé síly. Každý neúspěšný pokus prodlužuje interval pro nové zadání vstupního kódu. Lze také nastavit limit počtu chybně zadaných hesel, po jehož překročení dojde ke smazání telefonu. Vstupní heslo můžeme u nových modelů od roku 2013 nahradit následnou registrací a přihlašováním otiskem prstu (funkce „Touch ID“). Neznamená to ale, že by bylo možné vynechat vstupní kód. Při registraci otisku prstu je nutno zadat také bezpečnostní vstupní kód. Přes používání otisku je vstupní heslo vyžadováno například po restartu nebo dlouhodobém nepoužívání zařízení.

Třídy

Každý nově vytvořený soubor má přidělenu příslušnou bezpečnostní třídu. Ty obsahují různé politiky přístupu k těmto souborům.

- **Complete protection** – klíč třídy je chráněn klíčem odvozeným od uživatelského přístupového kódu a UID zařízení. Po uzamčení přístroje jsou veškerá data nepřístupná až do následného odemčení uživatelem. Jedná se o implicitní ochranu zpráv, příloh či obrázků.
- **Protected unless open** – existují i takové soubory, které potřebují zapisovat i při uzamčeném zařízení (např. emaily). Proto je zde vytvořen veřejný a soukromý klíč. Sdílený tajný klíč je vypočítán pomocí soukromého klíče a klíčem třídy, jejíž soukromý klíč je chráněný uživatelským kódem a UID zařízení. Sdílený klíč

chrání vytvořený pár a po ukončení práce se souborem je vymazán společně s veřejným i soukromým klíčem.

- **Protected until first user authentication** – chová se jako třída Complete protection, nemaže však klíč třídy z paměti po uzamčení přístroje.
- **No protection** – tato třída je chráněna pouze pomocí UID zařízení. Je výchozí třídou všech souborů. Klíče potřebné pro dešifrování souborů jsou uloženy v zařízení, mohou být vzdáleně smazány.[22]

Keychain data protection a keybags

Keychain je implementován jako SQL databáze uložená v souborovém systému, který poskytuje bezpečné ukládání klíčů a přihlašovacích údajů. Data typu Keychain jsou chráněna pomocí struktury třídy podobné té souborové. K šifrování a dešifrování používají však jiné klíče a jsou součástí API. Třídy Keychain jsou chráněny pomocí UID, není tedy možné zneužití zálohy v jiném zařízení. Všechny Keychain třídy a jejich klíče, ale i všechny ostatní klíče souborů, jsou spravovány pomocí Keybags. Ty jsou rozděleny do několika hlavních typů.

- **System KeyBag** – obsahuje zabalené třídy klíčů používaných v běžném provozu, např. přístupový kód.
- **Backup KeyBag –** je vytvořen po zašifrování zálohy zařízení pomocí iTunes (KeyBag je chráněn heslem v iTunes), která se uloží následně na počítač. Vytváří se z nové sady klíčů, pomocí nichž mohou být data zpět dešifrována.
- **Escrow KeyBag** – používá se pro synchronizaci iTunes a MDM. Umožňuje zálohovat a synchronizovat zařízení bez nutnosti zadávání hesla.
- **iCloud backup KeyBag –** je podobný Backup KeyBag, ale všechny třídy jsou asymetrické, tzn. že iCloud zálohování lze provádět i na pozadí.[22][49]

Zabezpečení sítě

Jelikož uživatelé mobilních zařízení vyžadují přístup k firemní síti odkudkoliv, je nutné využít maximální možné ochrany. Systém iOS kromě vlastních zabezpečení podporuje i standardní síťové protokoly, nejnovější standardy pro zabezpečení Wi-Fi a mobilní síťová připojení. Jelikož byl omezen poslech na portech, systém nepotřebuje ochranu portů při otevřené komunikaci. Nepotřebuje Telnet ani webový server. Komunikace pomocí služeb jako jsou iMessage, FaceTime a Apple Notification Server je plně šifrována. Podporu SSL

(Secure Socket Layer) a TLS (Transport Layer Security) využívají Safari, Kalendář, Mail a další aplikace. Tyto služby zajišťují šifrovaný komunikační kanál pro bezpečnou komunikaci. Mezi další podporované standardy patří podpora VPN (Virtual private network) pomocí protokolů PPTP, L2TP nebo IPsec. Potřebují jen minimální konfiguraci pro práci se systémem. Další podporované služby jsou iOS Wi-Fi včetně podpory WPA2 Enterprise pro přístup k podnikovým bezdrátovým sítím. Komunikace je šifrována 128bitovým AES šifrováním během přenosu. Standard 802.1X je samozřejmým a používá se pro připojení do veřejných i domácích sítí. Také není opomenuta podpora BT, nejsou zde ale přístupna osobní data.[22]

Bezpečnost aplikací

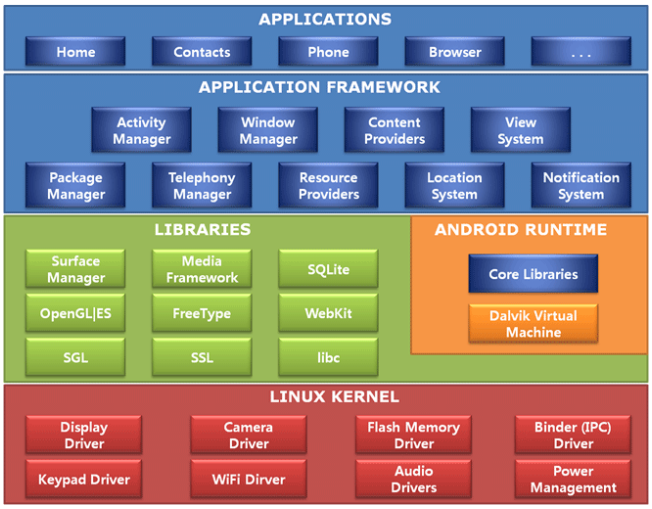
V případě systému iOS je zpřístupnění aplikací třetích stran složitější než u jiných systémů. Chce-li vývojář aplikaci umístit do obchodu AppStore, musí být registrován pod vlastním účtem nejprve v Developer Programu (program pro vývojáře aplikací systému iOS). Po registraci je možné požádat o vlastní certifikát (iPhone distribuce certifikátů). S tímto certifikátem vývojáře je nutné aplikaci připravit a nahrát on-line (distribuce iPhone prováděcí profil). Následně je nezbytné připravit žádost o prodeji. Náklady na zveřejnění aplikace jsou 99 dolarů pro jednotlivce a 299 dolarů pro firmy. Dále je nutné při publikování aplikace vybrat název, ikony a tři ofocené obrazovky z aplikace. Po odeslání žádosti uplyne několik týdnů, než získáme odpověď. V případě správnosti všech požadavků bude aplikace publikována v obchodě AppStore.

2.2 Bezpečnost operačního systému Android

Operační systém Android je otevřenou platformou, která využívá moderní vyspělé technologie. Vývoj se zaměřil na jednoduchost tvorby aplikací. Pro vývojáře je usnadněn flexibilitou bezpečnostních prvků. I bez pokročilých znalostí bezpečnosti OS Android je výchozí nastavení bezpečnosti dostatečně elastické, aby nebylo překážkou vývoje aplikací.[32]

2.2.1 Architektura operačního systému Android

Architektura operačního sytému Android je rozdělena do pěti vrstev. Jádro systému, Android runtime, nativní knihovny, Application Framework a aplikace. Obrázek 5 popisuje strukturu platformy Android.



Obrázek 5: Struktura platformy Android

Zdroj:[14]

Jádro a operační systém

Jádro je nejnižší abstraktní vrstvou. Zprostředkovává komunikaci mezi používaným hardware a zbytkem software. Systém původně vznikl na jádře Linuxu verze 2.6. Android 4x je postaven na jádře Linux 3.x. Linux poskytuje bezpečné a jednoduché uživatelské rozhraní s nutností nastavení oprávnění. Tato oprávnění jsou velmi důležitá z hlediska bezpečnosti systému. Chrání čtení informací z jiných aplikací než té, pro kterou jsou určeny. Hlavní funkcí jádra je komunikace s HW pomocí ovladačů, správa paměti, a síťové spojení.[4]

Android Runtime

Tato vrstva se nachází ve stejné úrovni jako vrstva knihoven a tvoří ji dvě části. První je virtuální stroj Dalvik, na kterém jsou spuštěny všechny běžící aplikace. Je to upravený

JVM (Java Virtual Machine), který se liší architekturou a příponami souborů, jež spouští. Tyto soubory mají příponu (dex) oproti JVM která používá příponu (class). Druhou částí vrstvy jsou systémové knihovny (Core Libraries), které jsou základními knihovnami programovacího jazyka Java. Slouží pro všeobecné programovací rozhraní API (Application Programming interface).[4]

Nativní knihovny

OS Android má sadu nativních knihoven psaných v jazyce C/C++, které využívají jednotlivé komponenty hardware. Vývojáři k těmto komponentům přistupují prostřednictvím nativních knihoven pomocí Application Framework. [4]

Application Framework

Poskytuje bohatou sadu modulů pro vývojáře. Každý z nich nabízí určitou skupinu služeb pro správu systému. Patří sem Aktivity Manager, Package Manager, Resource Manager, Notification Manager.[4]

Aplikace

Aplikační vrstva je nejvyšší vrstvou architektury. Nabízí aplikace, které jsou součástí systému (kalendář, správce kontaktů, webový prohlížeč, SMS klient), nebo aplikace s volitelnou instalací dle uživatele. Jsou psány v kódu Java s příponou (class) a distribuují se prostřednictvím instalačních balíčků s příponou APK (Android Application Package).[4][50]

2.2.2 Bezpečnostní prvky

Bezpečnost OS Android lze rozdělit do čtyř skupin. Jsou jimi bezpečnost systému, šifrování a ochrana dat, bezpečnost aplikací a aktualizace. Tyto skupiny obsahují bezpečnostní prvky na úrovní systému a jádra, jako i na úrovni aplikací.

Bezpečnost systému

Je celkovou ochranou integrity systému. Patří do ní heslo, systémový oddíl, nouzový režim, oprávnění souborového sytému a bezpečnost správy paměti.

Heslo je zásadním uživatelským bezpečnostním prvkem sytému. Využívá se i k jiným funkcím. Po aktivaci hesla je uživatel nucen jej zadávat při každém vstupu do zařízení. Heslo by nemělo být podceňováno svou kvalitou, nebo dokonce uživatelem zcela opomíjeno.

Systémový oddíl obsahuje soubory pro načtení systému. Je nastaven pouze s přístupem pro čtení, tedy do něj není možné zapisovat. Oprávnění souborového systému je nastaveno tak,

že aplikace může číst pouze data svých souborů, a nikoliv jiných aplikací. Je možné, v případě že to aplikace povoluje, využít jejich dat pro aplikace jiné. Nouzový režim systému může být vyvolán uživatelem v případě, kdy je nutné načíst systém pouze s předinstalovanými aplikacemi výrobce. Používá se pro identifikaci a odstranění nežádoucích škodlivých aplikací.[32]

Šifrování a ochrana dat

Oprávnění souborového systému se využívá ve výchozím nastavení tak, že každá aplikace běží v jádru systému pod vlastním jedinečným UID (Unique Identifier). Aplikace se instalují do vlastních adresářů, kam jen ony samotné mají přístup. Tak je zabráněno přístupu jakýchkoliv aplikací k datům jiných aplikací. Přístup je možný jen díky oprávněním v souborovém systému, která musí vývojář předem při tvorbě aplikace nastavit.

Významným přínosem bezpečnosti správy paměti byla technologie ASLR (Address Space Layout Randomization). Tato technologie přichází společně s OS Android 4.0. Slouží k tomu, aby data nahraná do paměti při startu OS byla náhodně rozmístěna, a tudíž nebylo možné zjistit, kde se právě nachází. S verzí Android 4.1 přichází doplněk pro podporu PIE (Position Independent Executable), který umožňuje vykonat strojový kód nezávisle na tom, na jaké adrese v operační paměti se nachází, a to v každém okamžiku, kdy je tento kód vykonán.

Android poskytuje sadu kryptografických metod, které jsou dostupné prostřednictvím API rozhraní. Jsou využívány běžné algoritmy jako AES (Advanced Encryption Standard), RSA (Rivest Shamir Adleman), DSA (Digital Signature Algorithm), SHA (Secure Hash Algorithm), SSL (Secure Sockets Layer) či HTTPS (Hypertext Protocol Secure). Tyto algoritmy využívá pro šifrování souborového systému nebo pro vytvoření šifrované komunikace určitých aplikací. Umožňuje také šifrování síťového provozu prostřednictvím Wi-Fi či BT za pomocí standardních protokolů. Také je možnost vytvářet virtuální privátní sítě VPN (Virtual Private Network).

Od vydání OS Android verze 3.0 je možné šifrovat souborový systém. Používá se symetrických šifer s pevně stanovenou délku klíče pro šifrování i dešifrování. Šifrování probíhá na úrovni jádra. Nástroje jsou implementovány v kryptografické rozhraní API. Pro samotné šifrování se používá algoritmus AES s délkou klíče 128 bitů. Hlavní klíč je chráněn pomocí algoritmu AES128, který je odvozen od uživatelského hesla. Toto heslo zadává uživatel při každém vstupu do zařízení. Proti systematickým útokům hrubou silou a slovníkovým útokům se pro zajištění odolnosti hesla používá tzv. kryptografická sůl.

Několik náhodných bitů se tak doplní dalšími náhodnými bity a při každém opakovaném vstupu do hashovací funkce SHA-1. Tím je zaručeno, že heslo bude mít vždy jiný zakódovaný tvar. K tomu je použito PBKDF2 (Password Base Key Derivation Function) algoritmu. Pro použití internetové asynchronní kryptografie využívá systém Android šifry s veřejným klíčem RSA za použití digitálního podpisu DSA. Tím je zaručena důvěrnost informací i ochrana proti neautorizované modifikaci jinou osobou.[32]

Bezpečnost aplikací

Pro operační systémy Android je povoleno osobám třetích stran vyvíjet a distribuovat aplikace. Aplikace je možné zpřístupnit pomocí Google Play, nebo prostřednictvím vlastních stránek či jiným distribuováním souboru určeného k instalaci.

Poslat žádost o publikování aplikace na OS Android je mnohem jednodušší a levnější než na systému iOS. Stačí se přihlásit do Google Play a následně vstoupit do konzole pro vývojáře. Tam vložíme svou aplikaci (s příponou *.apk) a nahrajeme na server. Žádost je okamžitě testována. Doplníme popis aplikace a v případě kladného vyřízení žádosti je aplikace publikována v rámci obchodu Google Play.

Každá aplikace prochází základním bezpečnostním procesem a musí obsahovat určitá bezpečnostní opatření. Mezi základní prvky ochrany aplikací patří Sandboxing (izolovaný prostor), Application Signing and Verification (podpis aplikací a ověření), Access Permissions API (oprávnění přístupu API) a Google Bouncer (online automatický test aplikací a účtů společnosti Google).

Důležitým a mocným můstkem OS Android mezi jednotlivými stavebními prvky jsou intenty. Intent je jednoduchý objekt, který umí obsáhnout nějaká primitivní data a zařadit je mezi procesy. Můžeme rozlišit dva typy intentů – explicitní a implicitní. Explicitní intenty, kdy systém ví, co chceme spustit. Implicitní intenty popisují záměr, nikoliv přesný způsob, jak ho provést. Umožňují tak značné zjednodušení práce a vzájemnou interoperabilitu aplikací v rámci OS Android.[4][32]

- **Sandboxing**

Je izolovaný prostor, ve kterém běží každá spuštěná aplikace (tzv. Sandbox mód). Občas bývá nazýván také jako aplikační karanténa. Každá aplikace dostane přidělené jedinečné UID a spustí ji v samostatném procesu. Jádro systému pomocí čísla UID rozliší uživatelská oprávnění přiřazené ke každé aplikaci. Díky tomu aplikace nemohou mezi sebou komunikovat a jen omezeně mohou přistupovat k OS. O případnou potřebu komunikace mezi aplikacemi

běžících na různých procesech se stará mezi procesová komunikace označovaná jako IPC (Inter-Process Communication), která je součástí nejnižší vrstvy architektury. Tato komunikace musí být již při vývoji plánovaná tak, aby byla nastavena předem již potřebná oprávnění pro IPC a aplikace tak mohly vzájemně komunikovat.

- **Application Signing and Verification**

Každá aplikace sytému Android vyžaduje autorův digitální podpis, což umožní případnou identifikaci. Díky tomu je možné vytvářet vztahy důvěryhodnosti mezi aplikacemi a jejich aktualizacemi. Digitální podpis aplikací je proveden pomocí certifikátů, jejichž soukromý klíč si generují samotní uživatelé. Certifikát nemusí být podepsán certifikační autoritou. Toto je jedna z největších slabin systému, není totiž zaručena věrohodnost autorů. Je tak možno modifikovat vytvořenou aplikaci, vložit do ní malware a následně podepsat novým certifikátem. Takto upravenou aplikaci vystaví na svých stránkách a zpřístupní pro stažení veřejnosti. Proces ověření podpisu při instalaci aplikace provede modul správy balíčku Package Manager ověření, jestli byl instalační soubor aplikace řádně podepsán. V případě, že aplikace není podepsána autorem, je instalace i její případná distribuce prostřednictvím Google Play obchodu zamítnuta.

Od verze OS 4.2 probíhá online kontrola, která ověřuje prostřednictvím Google serveru potenciální bezpečnost aplikace. Může detekovat škodlivou aplikaci s možností pokračování instalace na přání uživatele, nebo detekuje nebezpečnou aplikaci a samo dojde k automatickému ukončení instalace. Principem této kontroly je porovnání zjištěných hodnot o aplikaci, hodnoty SHA-1, jména, verze aplikace atd.

- **Access Permissions API**

Chceme-li, aby aplikace přistupovala k systémovým prostředkům, je nutné mít definován a naprogramován přístup s potřebnými oprávněními k prostředkům API. Existují jisté výjimky nepodporované systémem (např. přistupování k SIM kartě). Prostředky chráněného API jsou funkce fotoaparátu, SMS a MMS, údaje o poloze GPS, telefonní funkce, bezdrátové komunikace BT, funkce sítí a datového spojení. Při každé instalaci aplikace se zobrazí uživateli seznam oprávnění, které aplikace vyžaduje pro svou instalaci. Veškerá oprávnění aplikace, která může využívat jsou obsažena v souboru *Manifest*, který je součástí instalačního balíčku (*.apk).

- **Google Bouncer**

Je online testovací skener užívaný pro automatické testování aplikací v obchodě Google Play. Ve virtuálním prostředí testuje aplikace a objevuje jakékoliv anomálie, tím odhaluje potenciální škodlivý program. Takovéto aplikace jsou z obchodu ihned vyřazeny.

Dalším úkolem tohoto skeneru je testování nových vývojářských účtů a ochrana před vývojáři, kteří již v minulosti škodlivý software vytvářeli, ti jsou následně blokováni.

- **Aktualizace**

Aktualizace jsou velmi důležité jak pro opravu chyb aplikací třetích stran, tak i chyb v samotném operačním systému. Aktualizace systému může probíhat dvěma způsoby. Prvním z nich je aktualizace přes osobní počítač. Po stažení aktualizace a spuštění v počítači, dojde k ověření její integrity a autentičnosti instalačního balíku, teprve poté k aktualizaci. Druhý způsob aktualizace je prostřednictvím datových služeb nebo bezdrátového připojení, který je označován jako OTA (over the air – vzduchem).[4][11][29]

2.3 Porovnání bezpečnosti operačních systémů

V této kapitole porovnám bezpečnost obou sledovaných operačních systémů na základě silných a slabých stránek a také rizik vyplývajících z analýzy SWOT.

2.3.1 SWOT analýza bezpečnosti OS iOS

Operační systém iOS společnosti Apple je tak specifický, že je obtížné najít potenciální slabé stránky. Prioritou vždy byla bezpečnost, a proto převažují převážně stránky silné.

Silné stránky

Tento OS má v současnosti nejlepší podporu systému i zařízení na trhu. Také je na trhu nejbezpečnějším zařízením současnosti. Jeho bezpečnost není plně pod kontrolou uživatele, systém je uzavřený. Ekosystém zařízení – hardware, firmware i software je řízen společností Apple. Spoléhá na silné šifrovací postupy na celé platformě. Po incidentu s FBI (*The San Bernardino Case*[15]) došlo k posílení šifrování u iCloud a hardware.

Slabé stránky

Mezi slabé stránky iOS patří skryté uživatelské rozhraní. Také bych sem především zařadil uživatele, kteří ať vědomě či nevědomě používají slabých hesel.

Rizika/hrozby

Pro dlouhodobý úspěch produktů Apple je zásadní bezpečnost produktů. Pověstná bezpečnost je jedním z předních rozhodovacích kritérií uživatelů. Jakékoliv narušení bezpečnosti na OS by mohlo způsobit pokles poptávky po jejich produktech. To je důvodem, proč se společnost, zastoupená generálním ředitelem Timem Cookem, brání v kauze šifrování telefonu iPhone proti ministerstvu spravedlnosti. Pokud by společnost Apple souhlasila s vytvořením backdoor procesu šifrování iPhone pro úředníky činnými v trestním řízení, byla by ohrožena bezpečnost a soukromé údaje jejich zákazníků užívajících tato zařízení.[2][5][15]

2.3.2 SWOT analýza bezpečnosti OS Android

Android je nejvíce užívaná mobilní platforma současnosti. Z hlediska bezpečnosti však stále zaostává za OS iOS. Proto je zde stále poměrně dost slabých stránek.

Silné stránky

Operační systém Android je plně otevřený, je kompletně zdarma. Všechna API jsou volně dostupné. Je flexibilní, pracuje na všech zařízeních. Má obrovský trh aplikací a nejlepší

možnosti výběru hardware. Systém je plně konfigurovatelný, uživatel má plnou kontrolu nad nastavením zabezpečení svého soukromí i dalších nástrojů.

Slabé stránky

Multimediální podpora pro mobilní telefony s OS Android je mnohem méně centralizovaná na rozdíl od společnosti Apple, která má centralizované uložiště iTunes. Vzhledem k tomu, že je většina aplikací bezplatná, mají reklamy zobrazené v dolní nebo horní části obrazovky aplikace, případně obsahují vyskakovací okna. To zneklidňuje uživatele a snižuje jejich potěšení z dané aplikace. Systém také neustále odesílá statistiky společnosti Google. Většina aplikací pro OS Android vyžaduje trvalé připojení k internetu, a tak je náchylný externím hrozbám. Je velmi uživatelsky přívětivý, ale může být manipulováno se zdrojovým kódem a aplikace mohou být doplněny o malware.

Rizika/hrozby

Android je silně ohrožen systémem iOS. V případě jeho kompatibility s ostatními zařízeními by jistě došlo k poklesu podílu OS Android na trhu. Android je náchylný k bezpečnostním hrozbám, jako jsou malware a viry. Největším problémem tohoto OS je stahování aplikací z nedůvěryhodných zdrojů.[3][5][46]

3 ZHODNOCENÍ BEZPEČNOSTI MOBILNÍCH ZAŘÍZENÍ

V této kapitole provedu zhodnocení bezpečnosti a komparaci konkrétních mobilních telefonů značek Apple (OS iOS) a Samsung (OS Android). Popíšu podrobněji specifikace telefonů, jejich aktuální verzi software (který se odkazuje na přílohu B), zaměřím se také na funkce usnadnění a jejich bezpečnost. Následně provedu porovnání hardware, software, bezpečnosti a závěrečné hodnocení.

3.1 Zhodnocení bezpečnosti a komparace konkrétních modelů systému iOS a Android

Pro hodnocení bezpečnosti a využité technologie jsem zvolil dva zástupce nejvyšší třídy. Telefony Apple iPhone 7 a Samsung Galaxy S7. Původně jsem zvažoval, zda od firmy Samsung nezvolím Samsung Galaxy Note 7. Avšak po problémech tohoto modelu, které způsobovaly požáry baterie a jeho stažení ze strany výrobce, jsem zvolil model S7. Prodává se sice o pár měsíců déle, ale parametrově je stále největším konkurentem telefonu iPhone 7.

Mezi zásadní kritéria hodnocení komparovaných modelů mobilních telefonů patří:

- výkon hardware zařízení;
- možnosti aktuální verze OS a jejich výhod či nevýhod;
- funkce usnadnění;
- a především jejich bezpečnost.

3.1.1 Apple iPhone 7

Mobilní telefon iPhone 7 (viz obr. 6) byl představen v San Francisku 7. září 2016 jako nástupce modelu 6S.

Obrázek 6: iPhone 7

Zdroj:[8]

Hardware

Tento telefon má celokovové tělo, disponuje IPS LCD displejem o velikosti 4,7 palců s rozlišením 1334 x 750 pixelů a 326 pixelů na palec. Jeho 64-bitový procesor se čtyřmi jádry, kde dvě mají vyšší výkon a dvě nižší, umožňuje efektivně za účelem úspory baterie definovat, který z procesorů dle potřeby daného výkonu bude využit. Telefon nepodporuje paměťové karty, podporu NFC má omezenou pouze pro platby Apple Pay. Je dodáván s 2 GB operační paměti a lze jej koupit ve třech variantách velikosti vnitřní paměti, 32GB,128GB a 256GB. Má dvě kamery, přední 7Mpx a zadní 12Mpx, které umí natáčet videa v kvalitě 4K při 30 snímcích, 1080p při 60 snímcích. Zadnímu fotoaparátu může napomáhat blesk, který tvoří čtveřice led diod. Telefon již nemá „stereo jack“ konektor pro připojení sluchátek. K tomu se využívá konektor Lightning, který je zároveň konektorem datovým i napájecím. Z hlediska konektivity má telefon 4G LTE, GSM, HSPA+, 802.11a/b/g/n/ac (Wi-Fi). Pro lepší zvuk jsou vestavěné stereo reproduktory. O bezpečné přihlášení do zařízení se mimo jiné stará čtečka otisku prstů označovaná jako Touch ID. Ta oproti předchozím verzím není mechanickým tlačítkem. Zařízení obsahuje barometr, tříosí gyroskop, akcelerometr, proximity senzor a senzor okolního světla. Telefon splňuje parametry odolnosti dle IP67 (je odolný vůči jakémukoliv

prachu a ponoření do vody maximální hloubky 1 metru na 30 minut). Telefon obsahuje 1960mAh baterii, jejíž kapacita umožňuje až 14 hodin hovoru v síti 3G.[8][25]

Software

Aktuální verze OS iOS v telefonu je 10.2.1. Vývojáři pracují na nové verzi 10.3. Je možné ji také používat, jestliže se uživatel zaregistruje jako veřejný beta tester nebo jako vývojář. Získá tím možnost testovat novější, občas i nestabilní verze systému dříve, než jsou oficiálně zpřístupněny. Má možnost odladit své aplikace. Následně může zpřístupnit aktualizaci aplikace pro novější verzi systému.

Verze 10.2.1 oproti předchozím přinesla možnost probuzení telefonu pouhým zvednutím telefonu displejem směrem k uživateli. Byly obohaceny notifikace na uzamčené obrazovce. Umožňuje využití interkomu a odemčení vchodových dveří na uzamčené obrazovce, v rámci služby chytré domácnosti. Přibyla rovněž možnost rychlého mazání notifikací pomocí funkce 3D Touch, detekce vody v telefonu na konektoru lightning. Taktéž ovládací panel „Control Center“ vysouvaný zespod obrazovky dospěl značných změn. Byly upraveny možnosti na zamčené obrazovce pomocí nových widgetů, grafická úprava 3D Touch menu, úprava komunikace se Siri a její podpora s aplikacemi třetích stran. Opět byly vylepšeny Apple mapy a navigování v nich, služba Apple Music, služba Apple news, aplikace domácnost, i samotná aplikace telefon (hlasová zpráva je nyní i čitelná, varování u hovorů před potenciálním nevyžádaným hovorem, možnost VOIP či WhatsApp volání přímo u kontaktů). Dále došlo ke zlepšení zpráv, konkrétně byly doplněny nové ikonky emoji a přibyla funkce „Invisible ink“, kdy je zaslán obrázek, který je maskován a po přejíždění prstem po něm je postupně odkryt.

Funkce usnadnění

Patří sem funkce usnadnění přístupu osobám s určitým postižením zraku nebo problémem s dotýkáním se telefonu. Je možno je editovat v záložce nastavení, zpřístupnění. Pro osoby, které mají problém se zrakem, jsou připraveny funkce jako předčítání, zvětšení písma, lupa a přizpůsobení displeje. Je možno volit rychlost předčítání, i nový kvalitnější hlas a případně i druhý alternativní hlas. Můžeme měnit velikost textu, nastavovat tučný, měnit tvary tlačítek, měnit kontrast, snížit průhlednost, ztmavit barvy, omezit pohyb – animaci ikon. Také je zde funkce „Switch Control“, která nám postupně zvýrazňuje položky. Ty je možné aktivovat na dané obrazovce pomocí adaptivního příslušenství. Funkce „AssistiveTouch“ pomáhá lidem, kteří mají problém s dotýkáním se obrazovky, ovládáním myší nebo při užívání adaptivního příslušenství. Nastavení reakce dotyku je také možné přizpůsobit. Je možné změnit nastavení odezvy obrazovky, délky dotyku nebo ignorovat opakování dotyku po určitou dobu,

aby nebyla vyvolána jiná funkce. Zajímavou funkcí nabízenou při prvním spuštění telefonu je volba velikosti displeje. Nabízí zde standardní a zvětšené zobrazení. Podle výběru zobrazení se mění počet ikon na ploše a také velikost fontu písma.

Bezpečnost

Zařízení jsou šifrovaná z výroby. Při prvním spuštění telefonu je nabízen otisk prstu a bezpečnostní heslo pro vstup do telefonu. Je na uživateli, zda nabízené zabezpečení telefonu využije či nikoliv. V případě, že tyto zabezpečení přeskočí a nenastaví, je bezpečnost jeho zařízení na velmi nízké úrovni. Zařízení může otevřít kdokoliv a číst data v něm uložená. Při ztrátě či odcizení není ale schopen útočník telefon smazat, protože je chráněn účtem Apple ID. Dokud je toto zařízení na signálu GSM nebo veřejné Wi-Fi, která byla v telefonu nastavena, může být telefon sledován pomocí služby „hledat iPhone“. Služba umožňuje vyhledání telefonu, prozvonění telefonu, uzamčení nebo i smazání pro případ ztráty či krádeže. V případě, že telefon díky aplikaci hledat iPhone nahlásíme jako ukradený, není možné tento telefon znovu zprovoznit. I za předpokladu pochybení ze strany uživatele, společnost Apple telefon nahlášený jako odcizený pomocí této služby již nikdy znovu nezpřístupní.

Je důležité mít vlastní telefon dostatečně zabezpečený. Navíc výrobce takové zabezpečení doporučuje všem svým uživatelům. Ideální volbou je právě otisk prstu. Společně s ním je nutné vytvořit i bezpečnostní heslo, které slouží jako druhý způsob přihlášení, například v případě nefunkčnosti otisku (např. vlhké ruce nebo odřené polštářky prstů). V případě obnovy zálohy v jiném telefonu bude zařízení ihned po prvním spuštění opět vyžadovat zadání otisku i vstupního hesla. Díky přihlašování pomocí otisku prstu zabráníme sledování zadávaného bezpečnostního hesla pro vstup do zařízení. To může být použito k nákupu aplikací nebo přístupu do zabezpečených aplikací třetích stran. Uzamčený zabezpečený telefon není možné připojit do počítače a vyčíst z něj jakákoliv data. Komunikační port telefonu je uzamčen, odpojen až do odemčení telefonu. Při připojení telefonu do cizího zařízení, je navíc nutné potvrzení důvěryhodnosti tohoto přístroje na svém mobilním telefonu. V případě ztráty či odcizení telefonu je vhodné kontaktovat Policii České republiky a nahlásit ztrátu. Po předložení pořizovacího dokladu (nahlášení IMEI telefonu) bude telefon zablokován pro všechny operátory na území naší republiky.[22][23][26]

3.1.2 Samsung Galaxy S7

Mobilní telefon Samsung Galaxy S7 (obr. 7) byl poprvé představen 11. března 2016.

Obrázek 7: Samsung Galaxy S7

Zdroj:[41]

Hardware

Telefon má 5,1 palců displej s rozlišením 2560 x 1440 pixelů a 577 pixelů na palec. Původně byl prodáván s operačním systémem Android 6, nyní je pro něj již dostupný v poslední aktuální verzi Android 7.0. Tento telefon má slot na paměťovou kartu. Nabízí podporu NFC pro přenos hudby, obrázků a platby. O celkový výkon stroje se stará procesor Qualcomm Snapdragon 820/Samsung Exynos 8890. Tento procesor společnost Samsung vyvíjí sama. Telefon má 4 GB operační paměti a je dodáván ve variantách s 32 GB a 64 GB vnitřní paměti. Obsahuje veškeré další běžné komunikační funkce jako 4G LTE, GSM, HSPA, 802.11 a/b/g/n/ac (Wi-Fi). Má přední 5Mpx kameru a zadní 12 Mpx kameru s možností nahrávání videa až 4K rozlišení při 30 snímcích, 1080p při 60 snímcích. Samozřejmostí je otisk prstu, který je umístěn v tlačítku pod displejem. Zařízení obsahuje barometr, gyroskop, akcelerometr, proximity senzor a monitor snímání srdečního tepu. Telefon je certifikován stupněm krytí IP68, což ho chrání proti prachu a polití vodou. Dle deklarace výrobce a za předpokladu splnění bezpečnostních podmínek těsnosti telefonu, lze telefon ponořit do 1,5 metru na dobu 30 minut. Telefon obsahuje 3000mAh baterii, jejíž kapacita umožňuje až 22 hodin hovoru v síti 3G. [17]

Software

Telefon umožňuje stažení aktuální verze operačního systému Android verze 7.0. Aktualizace jsou stejně jako u společnosti Apple distribuovány ve dvou verzích. Jsou dostupné jako předčasné aktualizace systému pro beta testery a stabilní, oficiálně vydané verze pro koncové uživatele. Proto brzy po vydání této verze byla dostupná první stabilizační aktualizace opravující nedodělky a chyby.

Po aktualizaci OS Android na verzi 7.0 je výchozí rozlišení telefonu nastaveno na FullHD. Je nutné rozlišení přenastavit zpět na nativní. Verze OS Android 7.0 přináší výrazné přepracování vzhledu. Změnila se nadstavba TouchWiz, notifikační lišta s vlastním přizpůsobením vzhledu a možností. Změnou prošlo menu a vzhled nastavení a také prostředí fotoaparátu. Aktualizací prošla aplikace Always On. Objevila se možnost okamžité odpovědi v notifikační liště. Velkou novinkou jsou výkonové režimy telefonu, které lze nastavit v centru „údržba zařízení“. Je možné volit mezi optimalizovaným, herním, zábavním či vysokým výkonem telefonu. To zatím porovnávaná verze OS společnosti Apple nenabízí. Další novinkou je nativní podpora šifrování dat na úrovni souborů pro lepší izolaci a ochranu dat jednotlivých uživatelů zařízení.

Funkce usnadnění

Standardní funkce usnadnění jako jsou zrak, obratnost a interakce je možno definovat již po prvním zapnutí telefonu. Je zde hlasový asistent, možnost změny velikosti písma, možnost zapnutí vysoce kontrastního písma, změna tvarů tlačítek, lupa, stupně šedi, negativní barvy nebo i definice barev. V dalším menu je možné aktivovat snadné zapnutí displeje přejetím rukou přes displej, univerzální přepínač pro připojení externích příslušenství, klepání na obrazovku nebo použití předního fotoaparátů k detekci otáčení hlavy, otevření úst či mrkání očí. Nachází se zde také pomocné menu pro uživatele s omezenou obratností.

Nově ve verzi 7 přibyl filtr modrého světla, který je považován za původce nespavosti pro případ, že uživatel i před spaním v posteli používá telefon, nebo jej používá v noci. Lze nastavit několik úrovní intenzity (lehce až sytě žluté) nebo použít automatického režimu. Intenzitu jasu a nočního režimu lze časovat, používat automatické zapnutí v časového intervalu „od soumraku do úsvitu“ s využitím GPS. Další novinkou je regulace svítilny.

Bezpečnost

Telefon není z výroby šifrován, je možné šifrování zapnout pomocí nastavení. Jakýkoliv zašifrovaný telefon s OS Android však trpí výrazným zpomalením výkonu. Samsung S7 je vybaven otiskem prstu, který nám výrazně usnadní jeho odemčení. Proto je dobré jej využít a nenechat tento telefon high-end třídy nezabezpečený. Telefony s Android 6 a vyšším již není možné při jejich odcizení či ztrátě smazat jinou osobou. Zařízení je spárováno přes účet Google a v případě, že nebude z účtu odebrán, není možné bez tohoto účtu telefon dále provozovat. Smazat telefon lze pomocí kláves při jeho spuštění. Potenciální zloděj či nálezce je schopen tak telefon smazat se ztrátou dat, ale u této nové verze OS jej nepřipojí k jinému účtu Google. Telefon je možné z webu Google na dálku, bude-li zapnut a na síti, prozvonit, uzamknout či vymazat. V případě ztráty či odcizení telefonu je vhodné kontaktovat Policii České republiky a nahlásit ztrátu. Po předložení nákupního dokladu (ověření IMEI telefonu) bude zablokován pro všechny operátory na území naší republiky.

Aplikace Samsung Knox

Výrobce mobilních telefonů Samsung již řadu let nabízí vlastní řešení bezpečnosti pro svá zařízení řady Galaxy. Je jím Samsung Knox (viz obr. 8). Byl vyvinut především pro využití ve firemním prostředí. Aktuální verze 2.6 dosáhla vysokého hodnocení na různých webových stránkách, zabývajících se testováním bezpečnosti jednotlivých platforem. [42]

Obrázek 8: Aplikace Samsung Knox z Google Play

Zdroj:[43]

Jelikož jsem byl zvědavý, jak tato aplikace funguje a nepopisoval pouze teoretické znalosti s danou aplikací dle materiálů, zapůjčil jsem si Samsung Galaxy S6, ve kterém je tuto aplikaci v poslední dostupné verzi možno také nainstalovat. V továrním nastavení telefon nabádá

uživatele k instalaci této aplikace. Instalace je velmi rychlá a následuje nastavení zašifrovaného prostoru pro data aplikace v uložišti telefonu, a to i bez potřeby šifrování celého telefonu. Tento způsob šifrování telefon nijak výrazně nezpomalil. Pro prvotní přihlášení do aplikace je nutná emailová adresa a také jeden ze způsobů zabezpečeného přístupu do aplikace, heslo, otisk, znak nebo pin.

Díky aplikaci Samsung Knox můžeme v telefonu oddělit prostor veřejný a soukromý, nebo pracovní a soukromý, otevřený a zabezpečený. Umí oddělit ty nejdůležitější, nejčastěji používané aplikace jako jsou například kontakty, galerie fotografií, kalendář, mail, stažené aplikace i samotný obchod play, vlastní soubory, internetový prohlížeč a další. Také je možné touto aplikací telefon najít, uzamknout telefon či jej smazat nebo jen uzamknout aplikaci Knox. Obsluha aplikace je velmi snadná. V případě, že si uživatel nezabezpečí telefon samotný, slouží tato aplikace v podstatě pouze k zamezení přístupu k osobním datům uloženým v dané aplikaci. Provedeme-li tovární nastavení telefonu, dojde k odstranění všech dat v telefonu včetně obsahu aplikace Knox. [42]

3.1.3 Porovnání hardware

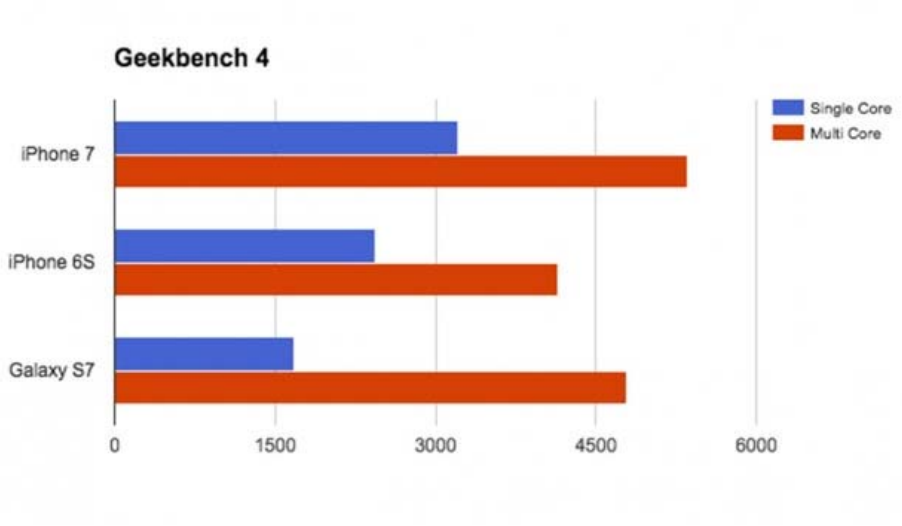
Tabulka (tabulka 1) uvádí vybrané parametry obou modelů mobilních telefonů (lepší jsou zeleně zvýrazněny). Sledované parametry jsou následující: konstrukce, displej, operační systém, procesor, paměť, fotoaparát, LTE, technologie a baterie. Je zřejmé, že dle uvedeného se jeví výkonnějším zařízením telefon Samsung Galaxy S7.

Tabulka 1: Komparace HW konkrétních modelů

Název parametru	iPhone 7	Galaxy S7
Konstrukce	**celokovové tělo, 138 x 67 x 7,1 mm, 138 g**, voděodolnost (IP67)	kovový rám + sklo, 142 x 70 x 7,9 mm, 152 g, voděodolnost (**IP68**)
Displej	4,7", **IPS** LCD, 1334 x 750 px, jemnost 326 ppi	**5,1"**, Super AMOLED, **2560 x 1440 px, jemnost 575 ppi**
Operační systém	iOS 10	Android 6.0 Marshmallow + TouchWiz UI
Procesor	4 jádrový, 2,23 GHz, Apple A10 Fusion	**8 jádrový**, 2,3 GHz, Samsung Exynos 8890
Paměť	2 GB RAM, 32/128/256 GB úložiště, bez microSD slotu	**4 GB RAM**, úložiště 32/64 GB + microSD karty
Fotoaparát	12 Mpx, **4x blesk**, OIS, f/1.8, 4K video + **přední 7 Mpx**	12 Mpx, 1x blesk, OIS, **f/1.7**, 4K video + přední 5 Mpx
LTE	800, 900, 1800, 2100, 2600 MHz	800, 900, 1800, 2100, 2600 MHz
Technologie	Bluetooth 4.2, Lightning port, NFC (Apple Pay), Wi-Fi, GPS, stereo reproduktory, čtečka otisků prstů	Bluetooth 4.2, NFC, Wi-Fi, GPS, 3,5 mm Jack, čtečka otisků prstů
Baterie	1960 mAh	**3 000 mAh, rychlonabíjení, bezdrátové nabíjení**

Zdroj: [vlastní tvorba]

Test výkonnosti dle programu Geekbench 4 společnosti Primate Labs ukazuje obrovský nárůst výkonu procesoru Apple A10 oproti modelu A9 a tím i výrazné navýšení celého výkonu telefonu. Samsung S7 zůstal až na 3. pozici. Více je uvedeno na obrázku 9.



Obrázek 9: Test výkonu napříč platformami

Zdroj:[48]

Podrobný test výkonu aplikací Geekbench 4 včetně parametrů na obrázku 10 ukazuje obrovský výkon na jádro procesoru Apple A10 Fusion oproti procesoru Samsung ARMv8. Jelikož iPhone 7 má jeden procesor se dvěma jádry, je jasné, že Samsung S7 s jedním procesorem a osmi jádry jej měl dle testu na jednotlivé jádro mnohonásobně překonat. Výsledky na multi-jádra jsou ale velmi podobné. Více podrobností je uvedeno na obrázku 10.

System Information	
	iPhone 7
Operating System	iOS 10.2.1
Model	iPhone 7
Processor	Apple A10 Fusion @ 2.34 GHz 1 processor, 2 cores
Processor ID	ARM
L1 Instruction Cache	64 KB
L1 Data Cache	64 KB
L2 Cache	3072 KB
L3 Cache	0 KB
Motherboard	D101AP
BIOS	
Memory	2000 MB

System Information	
	Samsung Galaxy S7
Operating System	Android 7.0
Model	Samsung Galaxy S7
Processor	ARMv8 @ 1.59 GHz 1 processor, 8 cores
Processor ID	ARM implementer 83 architecture 8 variant 1 part 1 revision 1
L1 Instruction Cache	0 KB
L1 Data Cache	0 KB
L2 Cache	0 KB
L3 Cache	0 KB
Motherboard	universal8890
BIOS	
Memory	3533 MB

Single-Core Performance	
Single-Core Score	**3323**
Crypto Score	**2361**
Integer Score	**3594**
Floating Point Score	**3214**
Memory Score	**3118**

Single-Core Performance	
Single-Core Score	**1905**
Crypto Score	**1399**
Integer Score	**2065**
Floating Point Score	**1506**
Memory Score	**2271**

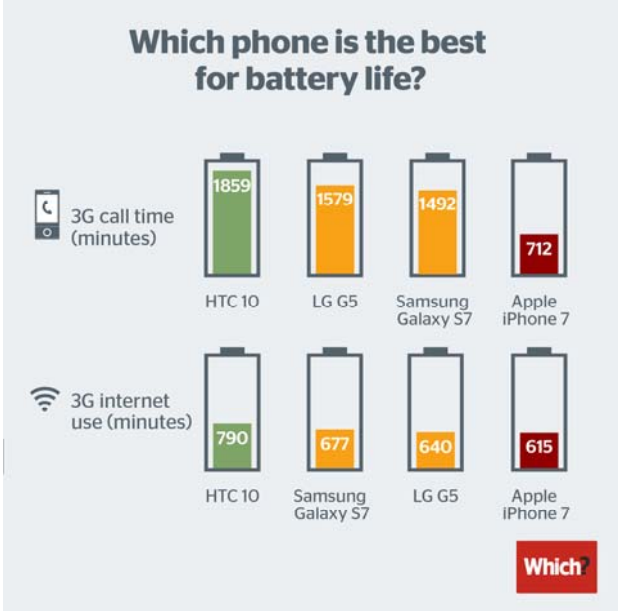
Multi-Core Performance	
Multi-Core Score	**5545**
Crypto Score	**4498**
Integer Score	**6426**
Floating Point Score	**5990**
Memory Score	**3158**

Multi-Core Performance	
Multi-Core Score	**5626**
Crypto Score	**6045**
Integer Score	**7048**
Floating Point Score	**5272**
Memory Score	**2852**

Obrázek 10: Podrobný test výkonu aplikací Geekbench 4 včetně parametrů

Zdroj:[24]

Z hlediska výdrže baterie Samsung S7 výrazně překonává Apple iPhone7. Více ukazuje následující obrázek 11, kde byly oba telefony testovány ještě s dalšími modely.



Obrázek 11: Porovnání výdrže baterií

Zdroj:[28]

Velmi užitečná funkce u telefonu iPhone je mechanický přepínač pro vypínání zvuku. Tento přepínač je patentován společností Apple a dodnes žádný výrobce mobilních telefonů podobné tlačítko na svých zařízeních nemá. Považuji jej za velké plus tohoto telefonu. Bez potřeby přihlášení se přes zabezpečení telefonu má uživatel možnost ihned jedním hmatem deaktivovat zvuk (např. na poradách či schůzkách).

3.1.4 Porovnání operačních systémů

Porovnáváme-li aktuální verzi obou telefonů, tedy iOS 10 a Android 7 Nougat, objevíme u obou společností řadu nových funkcionalit.

Notifikace

První z nových funkcionalit je v notifikační neboli oznamovací liště. Android zjednodušil notifikační lišty, které jsou teď snadněji čitelné, mají menší font a umožňují reagovat na oznámení přímo z notifikačního panelu bez potřeby otevřít aplikaci. V tomto ohledu lze říci, že Google následuje cestu, kterou vyšlapal Apple. Dokonce začal vyvíjet vlastní tlakově citlivý obraz, který se prvně objevil právě ve verzi Android 7 Nougat.

Apple ze zkušeností s notifikacemi rozšířil možnost reagovat oznámení nejen z oznamovací lišty, ale i uzamčené obrazovky telefonu. Umožnil tak aplikacím třetích stran, aby právě jejich oznamovací panely mohly být zobrazeny i na této obrazovce, a to i jejich aktivní okamžité

aktualizace. Motivoval se tak widgety (pozn.: widget je aktivní aplikace na ploše obrazovky), které na ploše používá Google již od starých verzí systému.

Digitální asistenti

Dalším rozdílným vývojem prochází i digitální asistenti. Apple se svou Siri asistentkou je výrazně dále. Uživatelé si tak mohou objednat taxi, mohou posílat zprávy kontaktům umístěným v aplikacích třetích stran (např. WhatsApp), umí online vyhledávat, je možno zeptat se na cestu, úkoly, nastavit budík, upomínky, oznámení a uskutečnit hovory tím, že řekneme Siri. Bohužel tato služba není stále v českém jazyce.

Android Nougat v poslední verzi 7.1 začíná využívat Google asistenta. Navazuje na zkušenosti Google Voice, která mimo jiné mluvila v češtině. Tato nová verze je dostupná pouze v angličtině a němčině. Zatím je dostupná pouze prostřednictvím aplikace Allo. Pro společnost Google je tato služba novou érou možností hlasového ovládání. Umí nabídnout pomoc, vysvětluje, odpovídá, učí se chování uživatele, nabízí odpovědi, ekomotivy. Umí rovněž vyhledat lety, nastavit budík, událost v kalendáři, najít výraz, kterému člověk nerozumí.

Operační systém společnosti Apple iOS 10 má více vylepšení než Google Android Nougat. Avšak ten není zase tak pozadu. Google nabídl více než 250 nových funkcí. Neustálý boj obou konkurentů ve snaze přinést na trh nové funkce a nové vychytávky do svého systému, které přiláká nové uživatele. Dá se říci, že ani jeden směr není špatný. Záleží na osobních preferencích uživatele, jakému rozhraní dá přednost.

3.1.5 Porovnání bezpečnosti

Rozdílnost hardware i operačních systémů není tak zásadní, jako rozdílný přístup k bezpečnosti mobilního telefonu. Oba typy telefonů nabízí možnost šifrování, zabezpečení zámkem, pinem, heslem či otiskem, v případě Samsungu také i znakem. Rozdílný je pohled, přístup k bezpečnosti zařízení. Telefon iPhone je automaticky šifrován a po nastavení zabezpečení je v podstatě stále neprolomitelný. U telefonu Samsung je nutná určitá znalost k zabezpečení telefonu tak, aby byl šifrován. Tato možnost se nenabízí při prvotní zapnutí telefonu a je nutno ji ručně vyvolat. Po zapnutí funkce šifrování zařízení dochází k snížení výkonu zařízení. U modelu S7 to nemusí být až tak výrazné jako u předchozích modelů, kdy po zapnutí šifrování byl pokles výkonu zařízení razantní. (mnou testováno např. u telefonu Samsung Galaxy A3(2016)). Samotné zašifrování telefonu trvá dle výrobce přibližně hodinu.

Další obrovskou výhodou telefonů iPhone firmy Apple je jejich úplné uzamčení. V případě ztráty či odcizení telefonu, může uživatel vynutit úplné uzamčení přístroje. Tato varianta je nevratná a následně ani společnost Apple nedokáže zpětně takovýto telefon oživit.

3.2 Závěr hodnocení komparovaných modelů

Vývojáři obou OS stále pilně pracují na zdokonalení vlastní bezpečnosti, jelikož jsou si vědomi vysokých nároků uživatelů na bezpečnost zařízení a jejich dat.

Ze základního porovnání hardware telefonů je zřejmé, že každý systém má jiné nároky. Obecně je známo, že systém Android potřebuje k práci více operační paměti. Další parametry výrobců jsou si velmi blízké, protože výrobci vzájemně kopírují technologie, které se osvědčily. Společnost Samsung navíc také dlouhodobě spolupracovala se společností Apple v oblasti výroby komponent telefonů iPhone.

Z hlediska operačních systémů, software, aplikací, je zde také řada zásadních rozdílů. Společnost Samsung oproti společnosti Apple operační systém svých telefonů nevyvíjí, ale pouze upravuje. Aplikace jsou také mnohem lépe testovány a certifikovány v obchodě App Store společnosti Apple.

Funkce usnadnění jsou v podstatě u obou výrobců podobné, je zřejmé, že se výrobci navzájem inspirují, doplňují a kopírují. Snad jen lidé používající tyto funkce by mohli posoudit oba výrobce a vyhodnotit ten lepší.

Z hlediska bezpečnosti je zřejmá stálá převaha telefonů Apple. Svou vysokou certifikací na bezpečnost splňují veškeré požadavky, a proto jsou stále tak oblíbené pro práci v bezpečnostních složkách, státních institucích či firmách. Důvěra ve značku Apple stále trvá, a dokud se neobjeví první prolomení systému či odemčení zařízení ze strany výrobce, budou stále více prodávány tyto telefony.

Naše mobilní zařízení jsou plna důvěrných dat, a proto je jejich bezpečnost velmi důležitá. Obsahují kontakty, dokumenty, emaily, fotografie, databáze hesel a jiných důvěrných údajů. Většina uživatelů zabezpečí svůj telefon tak, jak mu je nabídnuto při prvním spuštění telefonu. Část z nich dokonce přeskočí bezpečnostní prvky, a tak nemají telefon ani dostatečně zabezpečený.

Doporučení pro uživatele bez ohledu na to, zda se jedná o soukromé osoby nebo společnosti jsou:

- Je vhodné používat zámek telefonu, a to ať pinem, vzorem, heslem nebo moderním otiskem, dostačujícím jistě není přejetí displeje telefonu. Ubráníme se tak plně nebo alespoň částečně neoprávněnému vniknutí do našich zařízení a k našim datům. V případě zadávání hesel je nutno dbát zvýšené opatrnosti na bezpečné zadávání hesla, aby nás někdo nesledoval. V případě zadávání znaku je dobré si vypnout stopu znaku, tedy se nám nebude zobrazovat při zadávání. Dobré je i následně displej očistit, stopa po znaku bývá viditelná v podobě mastnoty na displeji. Znak může být považován za základní ochranu mobilních telefonů, často jej však lze prolomit při opakovaném zadávání již po několika pokusech. Proto je lepší využít bezpečného hesla a případné kombinace s otiskem prstu.
- Vždy je nutné instalovat pouze takové aplikace, které jsou stažené z oficiálního obchodu výrobce, tedy Apple App Store či Google Play.
- Je dobré číst vše, s čím je nutno souhlasit, smluvní podmínky výrobce či přístup aplikací do zařízení. Vždy se jedná o naši bezpečnost. Většina uživatelů smluvní podmínky pro jejich délku nikdy nepřečetla.
- Je-li to možné, je vhodné využít dvoufázových ověření. Znamená to pro nás další klikání či cvakání na obrazovce, zamezíme tak ale neoprávněnému vstupu cizí osoby.
- Zálohujte svá zařízení tak často, jak jen to bude možné.
- Je nutné být vždy pozorný a ostražitý, protože míra bezpečnosti mobilního zařízení je vždy závislá na míře chování jednotlivce. Nejslabším článkem bezpečnosti mobilních zařízení je a vždy bude uživatel.

ZÁVĚR

Cílem mé práce bylo popsání současného stavu bezpečnosti mobilních zařízení, mobilních operačních systémů a jejich bezpečnostního software, bezpečnosti mobilních aplikací, komunikačních přenosů, bezpečnosti soukromých a firemních mobilních zařízení a také provést komparaci konkrétních mobilních telefonů.

V první části jsem popsal problematiku bezpečnosti, projekt OWASP Mobile Security a také analýzu SWOT.

V druhé části jsem se podrobně zabýval problematikou bezpečnosti OS iOS a Android, jejich architektury, bezpečnostními prvky (zabezpečení aplikací i zařízení samotného). Také jsem provedl analýzu SWOT silných a slabých stránek, rizik a hrozeb bezpečnosti OS.

Ve třetí části jsem provedl komparaci konkrétních modelů telefonů s operačním systémem iOS i Android. Specifikoval jsem jejich hardware, software, funkce usnadnění i jejich bezpečnost. Následuje porovnání výkonu hardware, zásadních výhod a rozdílů daných operačních systémů, také rozdílu jejich bezpečnosti a hodnocení komparovaných modelů.

V závěru jsem doplnil svá doporučení, týkající se především bezpečnosti mobilních zařízení. Z důvodu rozsáhlosti této práce jsem přesunul do příloh kapitoly A-Vývoj mobilních telefonů a B-Vývoj operačních systémů. Doplňují informace ohledně vývoje bezpečnosti od počátků až po současnost.

POUŽITÁ LITERATURA

[1] 2016 NowSecure Mobile Security Report | NowSecure. The Mobile App Security Company | NowSecure [online]. [cit. 2017-04-14]. Dostupné z: https://www.nowsecure.com/ebooks/2016-nowsecure-mobile-security-report/

[2] Advantages And Disadvantages Of Apple iOS. *Thetechhacker - Simplify your tech life* [online]. Copyright © 2017 Vithala Media Network [cit. 19.04.2017]. Dostupné z: http://thetechhacker.com/2015/01/08/advantages-disadvantages-apple-ios/

[3] Advantages And Disadvantages Of Google Android. *Thetechhacker - Simplify your tech life* [online]. Copyright © 2017 Vithala Media Network [cit. 19.04.2017]. Dostupné z: http://thetechhacker.com/2015/01/03/advantages-disadvantages-android/

[4] ALLEN, Grant. *Android 4: průvodce programováním mobilních aplikací*. 1. vyd. Brno: Computer Press, 2013, 656 s. ISBN 978-80-251-3782-6.

[5] Android/WP7/iOS strengths and weaknesses. *Android Forum for Mobile Phones, Tablets, Watches & Android App Development - XDA Forums* [online]. Copyright © xda [cit. 19.04.2017]. Dostupné z: https://forum.xda-developers.com/showthread.php?t=1019752

[6] ANDROULIDAKIS, Iosif I. Mobile phone security and forensics: a practical approach. New York: Springer, c2012, xi, 105 p. SpringerBriefs in electrical and computer engineering. ISBN 1461416493.

[7] *Apple* [online]. Copyright © [cit. 19.04.2017]. Dostupné z: https://www.apple.com/business/docs/iOS_Security_Guide.pdf

[8] Apple iPhone 7 - Full phone specifications. *GSMArena.com - GSM phone reviews, news, opinions, votes, manuals and more...* [online]. Copyright © 2000 [cit. 19.04.2017]. Dostupné z: http://www.gsmarena.com/apple_iphone_7-8064.php

[9] Apple iPhone price, specifications, features, comparison. Tech News, Latest Technology News, New Best Tech Gadgets Reviews, Mobile, Tablet, Laptop, Gaming, Video Game, Tech Photos, Technology Videos Daily [online]. Copyright © Copyright Red Pixels Ventures Limited 2017. All rights reserved. [cit. 19.04.2017]. Dostupné z: http://gadgets.ndtv.com/apple-iphone-761

[10] Attacking the chain of trust. [online]. Copyright © [cit. 19.04.2017]. Dostupné z: https://image.slidesharecdn.com/jailbreakingios-110117101009-phpapp02/95/jailbreaking-ios-41-728.jpg?cb=1295259315

[11] Bezpečnost mobilních aplikací. *Aec.cz* [online]. 2015 [cit. 2016-05-26]. Dostupné z: https://www.aec.cz/cz/ztisku/lukas-blaha-bezpecnost-mobilnich-aplikaci-dsm-2015.pdf

[12] Bezpečnost. Ministerstvo vnitra České republiky: Pojmy a bezpečnost [online]. 2016 [cit. 2016-05-24]. Dostupné z: http://www.mvcr.cz/clanek/pojmy-bezpecnost

[13] BITTO, Ondřej. *Šifrování a biometrika aneb tajemné bity a dotyky*. Vyd. 1. Kralice na Hané: Computer Media, 2005, 168 s. ISBN 80-86686-48-5.

[14] *CUBRID - Open Source Database Management System Optimized for Web* [online]. Dostupné z: http://www.cubrid.org:8080/files/attach/images/220547/480/224/typical-schematic-of-android_structure.png

[15] Customer Letter - Apple. *Apple* [online]. Copyright © 2017 Apple Inc. All rights reserved. [cit. 27.04.2017]. Dostupné z: https://www.apple.com/customer-letter/

[16] Dashboards - Platform Versions - Developer.android.com [online]. [cit. 19.04.2017]. Dostupné z: https://developer.android.com/about/dashboards/index.html#Platform

[17] Galaxy S7 and Galaxy S7 edge | Samsung US. [online]. Copyright © 1995 [cit. 24.02.2017]. Dostupné z: http://www.samsung.com/us/explore/galaxy-s7-features-and-specs/#specs

[18] Galerie - Žebříčku 50 nejinovativnějších firem roku dominuje Apple. Zaslouženě? – MobilMania.cz. *MobilMania.cz – O mobilech víme vše* [online]. [cit. 19.04.2017]. Dostupné z: http://www.mobilmania.cz/Client.Gallery/show.aspx?id_file=847801546&article=1337635

[19] GRASSEOVÁ, Monika, Radek DUBEC a David ŘEHÁK. Analýza podniku v rukou manažera: 33 nejpoužívanějších metod strategického řízení. 2. vyd. Brno: BizBooks, 2012. ISBN 978-80-265-0032-2.

[20] Historie Androidu v kostce: aneb od verze 1.0 až po Android M. *Svět Androida* [online]. Praha: Karel Kilián, 2015 [cit. 2016-05-26]. Dostupné z: https://www.svetandroida.cz/historie-androidu-201506

[21] HUB, Miloslav. *Bezpečnost a ochrana informací v prostředí internetu*. Pardubice: Univerzita Pardubice, 2013. ISBN 978-80-7395-701-8.

[22] iOS security. White Paper. [online]. 2016-05-01 [cit. 2017-02-11]. Soubor ve formátu PDF. Dostupné z: https://www.apple.com/business/docs/iOS_Security_Guide.pdf

[23] *IOS Security: iOS 9.3 or later* [online]. Apple Inc., 2016 [cit. 2016-05-26]. Dostupné z: https://www.apple.com/business/docs/iOS_Security_Guide.pdf

[24] iPhone 7 vs Galaxy S7: Which is best [online]. Copyright © 2004 [cit. 19.04.2017]. Dostupné z: https://browser.primatelabs.com/v4/cpu/1855497

[25] iPhone 7 – Technické specifikace – Apple (CZ). *Apple* [online]. Copyright © [cit. 24.02.2017]. Dostupné z: http://www.apple.com/cz/iphone-7/specs/

[26] IT bezpečnost: Bezpečnost mobilních zařízení s iOS. *SystemOnLine* [online]. CCB spol. s r.o., ©2001-2016 [cit. 2016-05-24]. Dostupné z: http://www.systemonline.cz/it-security/bezpecnost-mobilnich-zarizeni-s-ios.htm

[27] Kompletní historie iOS: od prvního iPhonu až po iOS 9. *Letem světem Applem* [online]. Praha: David Grebeň, 2016 [cit. 2016-05-26]. Dostupné z: https://www.letemsvetemapplem.eu/2016/03/06/kompletni-historie-ios/

[28] *Letem světem Applem - Magazín o společnosti Apple a produktech Apple* [online]. [cit. 19.04.2017] Dostupné z: https://www.letemsvetemapplem.eu/2016/09/30/iphone-7-vydrz-baterie/smartphone-battery-life

[29] MAISNER, Martin. *Základy softwarového práva*. Vyd. 1. Praha: Wolters Kluwer Česká republika, 2011, xv, 339 s. Právní monografie (Wolters Kluwer ČR). ISBN 978-80-7357-638-7.

[30] MLÝNEK, Jaroslav. *Zabezpečení obchodních informací*. Brno: Computer Press, 2007. ISBN 9788025115114.

[31] Mobile OS market share 2016 | Statista. • *Statista - The Statistics Portal for Market Data, Market Research and Market Studies* [online]. Dostupné z: https://www.statista.com/statistics/266136/global-market-share-held-by-smartphone-operating-systems/

[32] Mobile platforms security models. *Standford University* [online]. Standford University, 450 Serra Mall, Stanford, CA 94305, USA: John Mitchell, 2015 [cit. 2016-05-26]. Dostupné z: https://crypto.stanford.edu/cs155/lectures/17-mobile-platforms.pdf

[33] Mobile Top 10 2016 - Top 10 - OWASP. [online]. [cit. 2017-04-14]. Dostupné z: https://www.owasp.org/index.php/Mobile_Top_10_2016-Top_10

[34] Mobilní OS pro experty: Vzestup a strmý pád Windows Mobile. *Mobil.idnes.cz* [online]. Praha: iDNES.cz, 2010 [cit. 2016-05-26]. Dostupné z: http://mobil.idnes.cz/mobilni-os-pro-experty-vzestup-a-strmy-pad-windows-mobile-pnm-/telefony.aspx?c=A100811_180849_chytre-telefony_ham

[35] Motorola DynaTAC 8000x - All-TIME 100 Gadgets - TIME. [online]. Copyright © 2016 Time Inc. All rights reserved. [cit. 19.04.2017]. Dostupné z: http://content.time.com/time/specials/packages/article/0,28804,2023689_2023708_2023656,00.html

[36] Nokia 5110 pictures, official photos. *GSMArena.com - GSM phone reviews, news, opinions, votes, manuals and more...* [online]. Copyright © 2000 [cit. 19.04.2017]. Dostupné z: http://www.gsmarena.com/nokia_5110-pictures-7.php

[37] *O'Reilly logo* [online]. [cit. 19.04.2017]. Dostupné z: https://www.safaribooksonline.com/library/view/mobile-application-penetration/9781785883378/graphics/B05055_02_28.jpg

[38] První foto: Špičkové smartphony Qtek 8300 a 8310. [online]. [cit. 19.04.2017]. Dostupné z: http://mobil.idnes.cz/prvni-foto-spickove-smartphony-qtek-8300-a-8310-fks-/mob_tech.aspx?c=A050815_220844_mob_aktuality_dno

[39] PUŽMANOVÁ, Rita. *Bezpečnost bezdrátové komunikace: jak zabezpečit Wi-Fi, bluetooth, GPRS či 3G*.Vyd. 1. Brno: Computer Press,2005,179 s. ISBN 80-251-0791-4.

[40] Revealed: Only 1.2 million Windows Phones sold in Q2 2016 - MSPoweruser. *MSPoweruser - All of Microsoft, all of the time* [online]. Copyright © 2017 MSPoweruser [cit. 19.04.2017]. Dostupné z: https://mspoweruser.com/revealed-1-2-million-windows-phones-sold-q2-2016/

[41] Samsung Galaxy S7 - Full phone specifications. GSMArena.com - GSM phone reviews, news, opinions, votes, manuals and more... [online]. Copyright © 2000 [cit. 19.04.2017]. Dostupné z: http://www.gsmarena.com/samsung_galaxy_s7-7821.php

[42] Samsung Knox™ | Mobile Security From Samsung Business. [online]. Copyright © 2015 Samsung Electronics America, Inc. [cit. 24.02.2017]. Dostupné z: http://www.samsung.com/us/business/security/knox/

[43] Samsung My Knox – Aplikace pro Android ve službě Google Play. [online]. Copyright © 2017 Google [cit. 19.04.2017]. Dostupné z: https://play.google.com/store/apps/details?id=com.sec.enterprise.knox.express&hl=cs

[44] SCHNEIER, Bruce. *Applied cryptography: protocols, algorithms, and source code in C*. 2nd ed. New York: Wiley, c1996. ISBN 0471128457.

[45] Smartphones sales by operating system worldwide 2009-2016 | Statistic. • *Statista - The Statistics Portal for Market Data, Market Research and Market Studies* [online]. [cit. 19.04.2017]. Dostupné z: https://www.statista.com/statistics/266219/global-smartphone-sales-since-1st-quarter-2009-by-operating-system/

[46] SWOT analysis of Android - Android SWOT Analysis. *Marketing blog for students and professionals* [online]. [cit. 19.04.2017]. Dostupné z: http://www.marketing91.com/android-swot-analysis/

[47] SWOT analýza - ManagementMania.com. [online]. Copyright © 2011 [cit. 19.04.2017]. Dostupné z: https://managementmania.com/cs/swot-analyza

[48] the iPhone 7 Pictures. *Trusted Reviews - The Latest Technology News and Reviews* [online]. Copyright © Time Inc. [cit. 19.04.2017]. Dostupné z: http://www.trustedreviews.com/iphone-7-photos

[49] VÁVRŮ, Jiří. *IPhone: vývoj aplikací*. 1. vyd. Praha: Grada, 2012, 179 s. Průvodce (Grada). ISBN 978-80-247-4457-5.

[50] VÁVRŮ, Jiří. *JQuery Mobile*. 1. vyd. Brno: Computer Press, 2013, 247 s. ISBN 978-80-251-3811-3.

[51] Z pravěku do přítomnosti: historie systému Windows Mobile. *Mobil.idnes.cz* [online]. Praha: idnes.cz, 2007 [cit. 2016-05-26]. Dostupné z: http://mobil.idnes.cz/z-praveku-do-pritomnosti-historie-systemu-windows-mobile-pn9-/mob_tech.aspx?c=A071126_121747_tech-a-trendy_ram

SEZNAM PŘÍLOH

PŘÍLOHA A - VÝVOJ MOBILNÍCH TELEFONŮ

Roku 1983 vyvinul americký konstruktér Martin Cooper první mobilní telefon Motorola DynaTAC 8000X (obrázek I). Přístroj vážil přibližně 2 kg a byl dlouhý 25 cm. Paměť na 25 čísel a doba dobití baterie byla 10 hodin, nabízel možnost až 30 minu hovoru a jeho cena byla v přepočtu přibližně 90.000,- Kč. Lidově se mi říkalo „cihla“, vypadal jako vysílačka s dlouhou anténou. Tento trend antén byl následně zachován až do roku 2002, kdy byl vyroben první telefon s vnitřní anténou.

Obrázek I: Motorola DynaTAX 8000X

Zdroj:[38]

Roku 1998 se na trhu objevil jeden z nejpopulárnějších telefonů, a to model telefon Nokia 5110 (obrázek II). Ten byl odlehčenou verzí manažerského model Nokia 6110. Umožňoval množství výměnných předních krytů a měl vestavěné hry.

Obrázek II: Nokia 5110

Zdroj:[36]

V roce 2005 se na trhu objevil první chytrý telefon vůbec. Jeho označení bylo QTEC 8300 (obrázek III). Tento model měl již operační systém Windows Mobile 5.0, TFT displej s rozlišením 240x320 pixelů, 65 000 barev, Wi-Fi, BT, funkci záznamníku a také fotoaparát s rozlišením 1,3Mpix. Výdrž přibližně 5 hodin hovoru s dobitím za přibližně 3 hodiny. Obsahoval již také slot mini SD pro rozšíření paměti o paměťové karty.

Obrázek III: QTEC model 8300 (vlevo) a 8310.

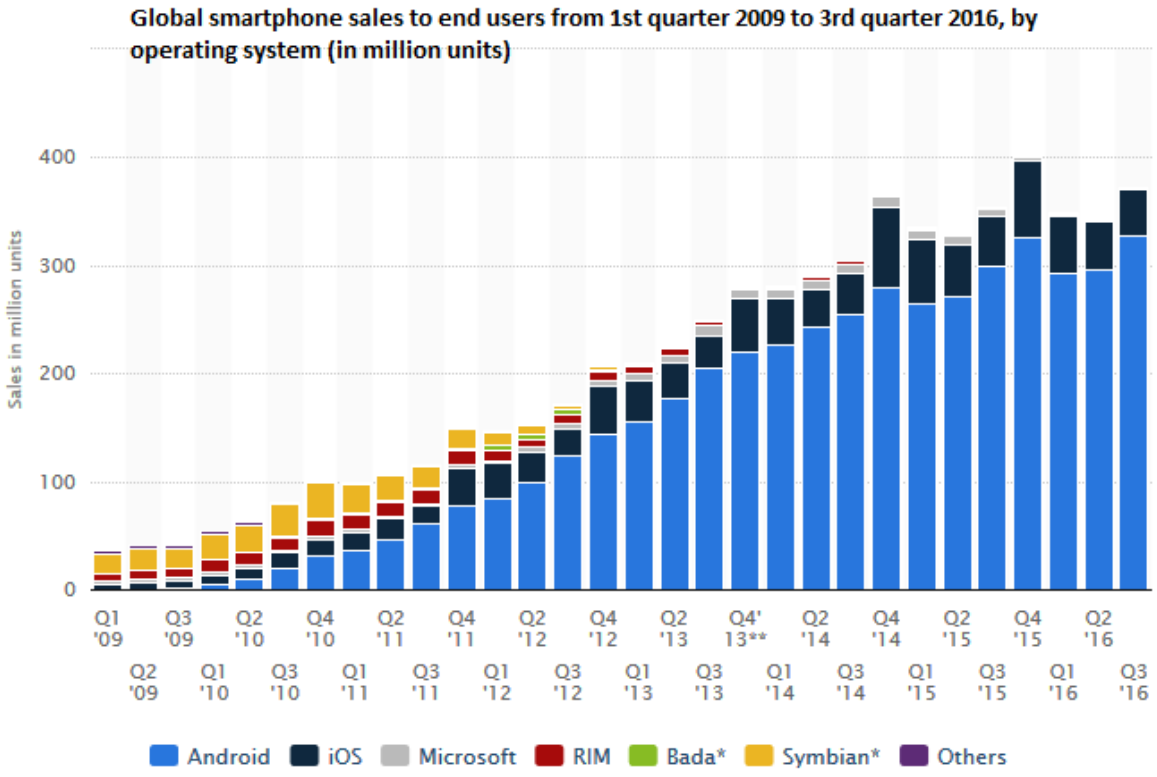
Zdroj:[38]

Roku 2007 přišel průlom mezi chytrými telefony. Na trhu se objevil dosud neznámý výrobce mobilních telefonů, a to společnost Apple, se svým mobilním telefonem iPhone (obrázek IV). Jeho prodej byl zahájen 29. června 2007. Byl však podmíněn závazkem k výhradnímu operátorovi v USA, společnosti AT&T Mobility. Podobným způsobem se prodával i dále ve světě. U nás jej bylo možno z počátku zakoupit jen z dovozu ze západní Evropy, neblokovaný na operátora. Tento telefon disponoval oproti dosavadním telefonům displejem o velikosti 3,5 palce s rozlišením 480x320 pixelů. Měl 2Mpix fotoaparát a vlastní 4, 8 nebo 16GB vnitřní uložiště.

Obrázek IV: Apple iPhone

Zdroj:[9]

Vývoj a prodej tohoto telefonu měl zásadní vliv na budoucí využití mobilních telefonů a tabletů. Všichni hlavní výrobci mobilních telefonů se začali směřovat na výrobu chytrých telefonů. Tomu napomohl také převážně vývoj operačního systému Android roku 2008. Jediná společnost, která na danou situaci na trhu reagovala po svém, byla společnost Nokia. Ta nadále věřila ve svůj vlastní systém Symbian, který nadále vyvíjela až do roku 2011, kdy byl ukončen. Vývoj prodeje telefonů dle operačních systémů je znázorněn na obrázku V.



Obrázek V: Celosvětový prodej chytrých telefonů 1/2009 až 3/2016.

Zdroj:[45]

Společnost Microsoft vyvíjela svůj vlastní operační systém, avšak až do roku 2015, kdy začala prodávat vlastní telefony Lumia, nevyrobila žádné zařízení, které by se hojně prodávalo. Zrovna tak ani společnost Google nevyvíjela, respektive neprodávala žádný telefon, který by hrál výhradní postavení na trhu své doby. Ano lze oponovat telefony Nexus, ale ty byly vyvíjeny jinými společnosti jako HTC, LG, Samsung a ASUS. Obě společnosti se zaměřili na vývoj a následný prodej vlastního operační systému pro jednotlivé výrobce hardware. Oba tyto systémy jsou v podstatě nezávislé na hardware. Oproti tomu operační systém iOS společnosti Apple byl vždy vyvíjen a testován pro každý model upravován samostatně.

PŘÍLOHA B - VÝVOJ MOBILNÍCH OPERAČNÍCH SYSTÉMŮ

V této části se zaměřím na tři nejpoužívanější mobilní operační systémy, které v současné době nejvíce ovlivňují trh. Jsou jimi Apple iOS, Google Android a Microsoft Windows Mobile.

I. iOS

Operační systém společnosti Apple byl a je vždy něčím speciální. Tento systém není možné provozovat na telefonech alternativních výrobců, ale pouze na telefonech společnosti Apple. Ty do jisté míry umožňují přechod na verze vyšší až po limity hardware, kdy výrobce již nadále tento telefon vyřazuje z telefonů podporovaných danou aktualizací. Výhodou takto sofistikovaného software pevně svázaného s úzkým počtem telefonů konkrétního jednoho výrobce je jednoznačně kompatibilita operačního systému, software s telefonem, hardware.

iPhone OS1

Roku 2007 byl představen iPhone OS operační systém společnosti Apple společně s prvním telefonem iPhone. Obsahoval jen 16 předinstalovaných aplikací, neexistoval žádný obchod a nebylo možné další aplikace stahovat. Výchozí aplikace, které tento telefon obsahoval byly: Mail, iPod, Kalendář, Fotky, Hodinky, SMS, Safari, Poznámky, Youtube, Kalkulačka, Mapy, Nastavení, Fotoaparát, Počasí, Akce a Telefon. [27]

iPhone OS2

Druhá generace tohoto systému přibyla představena o rok později, v roce 2008. Zároveň s touto novou verzí byl představen i nový telefon iPhone 3G. Přibyla možnost stahování aplikací díky novému obchodu App Store a díky tomu i množství aplikací vývojářů třetích stran. Novinkou této verze byly Push notifikace a také aplikace App Store. [27]

iPhone OS3

Roku 2009 byla vydána třetí řada operačního systému iPhone OS s označením 3.0. S touto verzi byl také vydán nový telefon iPhone 3GS. Přidal telefonu funkce kopírovat, vyjmout, vložit. Vylepšena byla přesnost GPS modulu a přibyla aplikace Kompas. Další z nových funkcí bylo hledání telefonu (Find my iPhone) s danou aplikací. Prvně zde přibyla funkce ovládání hlasem, vyhledávání obsahu, také funkce push notifications (pro zobrazení upozornění pro aplikace třetích stran), funkce natáčení videa, podpora MMS zpráv, aplikace Záznamník a možnost změny pozadí plochy.[27]

iPhone OS4

O rok později byla vydána čtvrtá řada operačního systému. Přibyl nově vydaný telefon iPhone 4. Přinesl společně s novým systémem také nové funkce jako multitasking (možnost přepínat mezi otevřenými aplikacemi bez nutnosti jejich ukončení), aplikaci FaceTime a její službu, která umožnila uživatelům telefonů iPhone komunikovat přes videohovory. Podporován byl také nový displej s vyšším rozlišením označovaný jako Retina. Z nových aplikací v této verzi OS byla aplikace iBooks, která sloužila pro čtení elektronických knih. V této době byl změněn název operačního systému iPhone OS na iOS.[27]

Apple iOS5

Tento systém vydaný roku 2011 přinesl více než 200 nových funkcí. Jednou z přelomových novinek byla aplikace iMessage. Ta umožňovala posílat zprávy mezi uživateli těchto telefonů bez potřeby operátora. Další přelomovou novinkou této verze systému byla inteligentní hlasová asistentka Siri. S touto verzi jako vždy přichází i nový telefon, iPhone 4S. Společně s touto verzi OS přichází také nový virtuální disk pro data uživatelů označovaný jako iCloud.[27]

Apple iOS6

Tento systém z roku 2012 zásadně inovoval vlastnosti týkající se velikosti telefonu. Z původních 3,5 palců byla úhlopříčka změněna u nového modelu telefonu iPhone 5 na 4 palce. Tento systém byl prvním v řadě, který tak podporoval dvě velikosti obrazu najednou. Bylo nutné upravit kompatibilitu všech aplikací tak, aby se správně zobrazovali na celé obrazovce. iPhone 5 byl také prvním z řady telefonů, který přinesl oproti předchozím modelům také nový konektor označovaný jako Lightning. Byl oboustranný a umožňoval uživatelům rychle, jednoduše a přesně zapojovat datový kabel či jiné příslušenství. Z aplikací byla zásadní změnou výměna aplikace mapy společnosti Google za vlastní mapy Apple. Integrována byla přímo do systému aplikace Facebook, sdílení fotografií na sociálních sítích. Přibila také nová aplikace Passbook, která slouží na centrální umístění platidel, jako jsou lístky, letenky, vstupenky a další.[27]

Apple iOS7

Sedmá řada z roku 2013 přinesla změnu grafického prostředí systému. S touto řadou přibyly prvně telefony dva. Nový telefon iPhone 5S, který se oproti předchozím verzím nabízel v barvě černé, a bíle a nově zlaté a také ochuzená verze s plastovým pouzdrem iPhone 5C. Od této doby do dneška již Apple vydával s novou verzí operačního systému telefony dva. Přelomovou novinkou u modelu iPhone 5S bylo TouchID, tlačítko fungující zároveň jako čtečka otisku prstu. Nově tak již od této verze dále bylo možno telefon odemykat otiskem prstu. [27]

Apple iOS8

S osmou řadou operačního systému iOS v roce 2014 přibyly prvně telefony dva. iPhone 6 a iPhone 6 s přízviskem Plus. První měl úhlopříčku 4,7 palců a verze Plus 5,5 palců.

Apple iOS9

Devátá řada je opět jakousi mezi řadou se kterou byly vydány dva hardwarově zrychlené telefony iPhone 6S a 6S Plus. Ty mají novou funkci, 3D Touch. Ta rozpoznává sílu přítlaku displeje, a tak lze na rozdílnou sílu programovat jiné funkce. V roce 2015 s touto verzí systému získává prioritu stabilita systému, což u některých předchozích verzí byl značný problém, a tak výrobce neustále vydával záplaty a záplaty záplat, aktualizaci za aktualizací. S verzí devět se tak nově objevuje také dvoufázové ověření účtu Apple ID. Funguje tak, že v případě potřeby přístupu k Apple ID účtu je vyžadován ověřovací kód. Ten se zobrazí sám v případě zapnuté funkce hledání telefonu nebo pomocí krátké textové zprávy na všech zaregistrovaných důvěryhodných zařízeních. [27]

Apple iOS10

Aktuálně vydaná verze 10 přinesla další dva nové telefony. iPhone 7 a 7 Plus. Byla zde výrazně rozšířena podpora funkce 3D Touch a nativními aplikacemi výrobce. Novinkou překvapivou této verze systému je nezašifrováni jádra systému. Mluvčí společnosti Apple tvrdí že mezi paměť kernelu neobsahuje žádné uživatelské údaje, a díky jeho rozšifrování jsou tak schopni optimalizovat výkon operačního systému bez ohrožení zabezpečení. Přitom všechny předchozí verze měla jádra systému zašifrovaná. Díky tomu se otevřelo mnoho diskuzí, zda nebude porušena bezpečnost či zajištění dat uživatele. Je zde také možná souvislost v důsledku souboje s FBI ve věci odemknutí iPhone střelce ze San Bernardina, kdy Apple odmítl odemknout své zařízení s dopisem vysvětlující jejich rozhodnutí všem uživatelům, proč se tak rozhodli.[27][22]

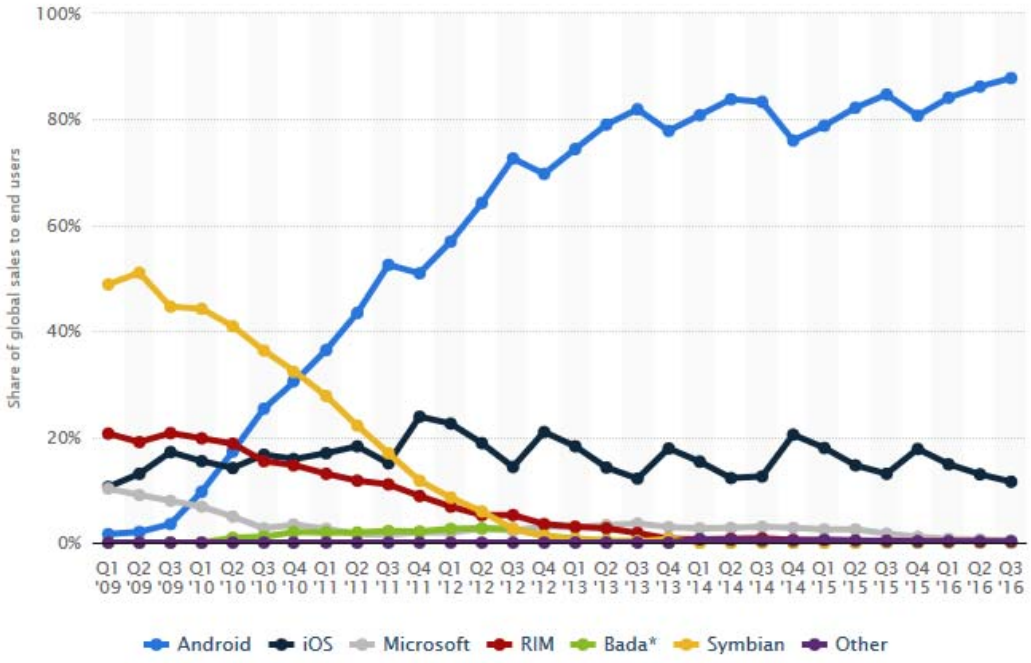
II. Android

Roku 2005 společnost Google odkoupila nepříliš známou společnost Android Inc. a udělala z ní svou dceřinou společnost. O dva roky později společnost Google získala několik patentů v oblasti mobilních technologií. V roce 2009 se tak na trhu objevila první verze Android 1.0. Aktuální dostupná verze, vydaná 22.srpna 2016 je Android 7.0 (Nougat).

Operační systém Android je od prvopočátku založen Linuxovém jádře. Tyto první verze operačního systému společnosti Google s označením Android byly průkopnické. Otevřely zcela

nový trh prodeje mobilních telefonů všech společností zabývajících se jejich výrobou. Byl totiž prvním otevřeným operačním systémem, který přinesl průlomové prostředí, přívětivé uživatelům. Pro výrobce byla prioritní právě ta možnost použít hotový funkční operační systém, který mají zdarma. To bylo jistě také jedním z důvodů, proč se takto dobře tento systém rozšířil a dnes má na trhu většinovou převahu. Na trh vstoupil roku 2008 a již v roce 2010 převzal vedoucí pozici podílu na trhu dle operačního systému, kdy roku 2013 překonal absolutní podíl 80 %.[20]

Vývoj na trhu dle operačního systému zobrazuje obrázek VI, na kterém je názorně vidět růst operačního systému Android, poměrně stabilní podíl na trhu systému iOS a upadající ostatní systémy.



Obrázek VI: Podíl na trhu dle operačního systému

Zdroj:[40]

Android beta, Android 1

Po krátkém testování beta verzí se koncem roku 2008 na americkém trhu objevil telefon HTC Dream/G1. Tento telefon byl prvním telefonem s tímto operačním systémem verze 1.0. Operační systém Android již od první verze nabízel Android Market, vlastní obchod aplikací, podporu notifikací, synchronizaci se službou Gmail, Widgety (označení miniaplikace) aktivní na domovské obrazovce, seskupování do složek, hlasové vytáčení, vlastní prohlížeč webových stránek, aplikaci pro SMS a MMS, přehrávač portálu Youtube, podporu Wi-Fi a BT,

kalkulačku, budík, možnost ukládání příloh ze zpráv, zobrazení, skrytí číselníku. Verze 1.5 Cupcake založena na jádře 2.6.27 obsahovala další nové funkce. Rychlejší spouštění a práci fotoaparátu, rychlejší určování pozice GPS (Global Positioning System – vysílané radiové signály, které umožňují uživatelům určovat svou polohu a čas.), klávesnici na displeji. Verze 1.6 Donut přinesla možnost okamžitého vyhledávání a vyhledávání hlasem, integrovaný fotoaparát s kamerou (možnost přepínat mezi režimem focení a kamerou), podporu CDMA, funkci převodu textu na řeč ve více jazycích než v předchozích verzích ale hlavně schopnost fungovat na různých rozlišeních obrazovky.[20]

Android 2

Verze Éclair s Linuxovým jádrem 2.6.29 vyšla roku 2009. Nabízela synchronizaci emailů (s nativní podporou MS Exchange), kontaktů z více účtů, BT v2.1, webový prohlížeč s podporou HTML5 novější verzi Google Map, novou odemykací obrazovku. Verzí 2.2 Froyo byla celkově vylepšena rychlost telefonu i práce s pamětí, možnost spouštění Wi-Fi přístupového bodu pro sdílení internetu telefonu, přesun aplikací do rozšířené paměti, paměťové karty SD, lokalizace do mnoha jazyků včetně češtiny. Verze 2.3 Gingerbread přinesla další zjednodušení a zrychlení telefonů, přidána byla nová klávesnice pro rychlejší zadávání textu, podpora NFC a internetové volání (SIP, VOIP), nativní podpora dalších senzorů, jako jsou gyroskop, barometr a další.[20]

Android 3

Android 3.0 Honeycomb, který byl původně speciálně vyvinut pro tablety a zařízení s větší úhlopříčkou displeje, dal trend další budoucnosti, rostoucích rozměrů mobilních telefonů a počátek prodeje tabletů. V této verzi byl vylepšen multitasking, sdílení internetu přes BT. Tato verze však byla rychle přeskočena, tak se v podstatě ani neobjevila na mobilních telefonech a výrobci nabízeli aktualizace z verze 2 rovnou na verzi 4.[20]

Android 4

Roku 2011 vydává Google další verzi již známého operačního systému Android 4.0 Ice Cream Sandwich. Ta byla správnou cestou jednotného operačního systému pro všechna zařízení. Grafické prostředí bylo značně přepracováno a došlo k mnoha vylepšením. Objevuje se zde kontrola užívání dat, integrace pořízení snímku obrazovky, rozpoznání tváře, lepší práce s hlasovým zadáváním (převod mluvené řeči v reálném čase), hardwarová akcelerace grafiky uživatelského rozhraní, podpora FullHD rozlišení (1980x1020 bodů na obrazovku), Android VPN Framework. Verzí 4.1 Jelly Bean přichází USB audio, vylepšená podpora usnadnění, práce s grafikou. Verzí 4.4 KitKat přibyla podpora nositelných zařízení Android Wear, podpora

bezdrátového tisku, optimalizace výkonu na starších zařízeních, Nativní API pro infračervený vysílač. [4][20]

Android 5

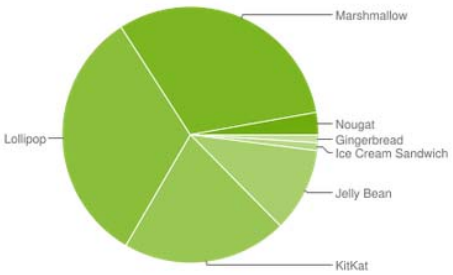
Android 5.0 Lollipop je založen na Linuxovém jádru 3.4.0. Přibyla podpora 64 bitových procesorů, funkce chytrého zamykání zařízení. Přináší také možnost více uživatelů na jednom mobilním zařízení, podpora více SIM karet najednou, HD kvalita zvuku.

Android 6 a 7

Přidávají podporu 4K rozlišení (3840x2160 bodů), nativní podpora snímače otisku prstů, podpora konektoru USB 3.1 Type C a jistě další mnohé změny a úpravy již oblíbeného operačního systému. Od verze 6 (Marshmallow) dochází ke změně v oblasti řízení oprávnění pro aplikace systému Android. Aplikace tak získají pouze taková práva, která jsou nezbytně nutná k jejímu spuštění, může sice následně během běhu vyžadovat oprávnění další, avšak ty již může uživatel odmítnout. Je možné tak zamezit přístupu k mikrofonu, fotoaparátu, souborů nebo i telefonnímu seznamu. Nově také přidávají podporu pro virtuální realitu. Poslední aktuálně dostupnou verzí Android je 7.0 Nougat. Anglický propagační list k této verzi píše – „Security is at the heart of all we do“ - lze česky přeložit jako „Bezpečnost je v srdci všeho, co děláme“. Tím lze poukázat na směr vývoje systému Android, který se stále více snaží zvyšovat bezpečnost systému, který je dominantním OS na trhu.[20]

Na následující stránce na obrázku VII je distribuce jednotlivých verzí OS Android do mobilních zařízení k březnu 2017. Verze s méně než 0,1 % nejsou zobrazovány.

Version	Codename	API	Distribution
2.3.3 - 2.3.7	Gingerbread	10	1.0%
4.0.3 - 4.0.4	Ice Cream Sandwich	15	1.0%
4.1.x	Jelly Bean	16	3.7%
4.2.x		17	5.4%
4.3		18	1.5%
4.4	KitKat	19	20.8%
5.0	Lollipop	21	9.4%
5.1		22	23.1%
6.0	Marshmallow	23	31.3%
7.0	Nougat	24	2.4%
7.1		25	0.4%



Obrázek VII: Distribuce jednotlivých verzí OS Android – stav k 03/2017

Zdroj:[16]

III. Microsoft Mobile

Společnost Microsoft vyvíjela svůj vlastní operační systém od verzí Pocket PC 2000, Windows Mobile 2002, Windows Mobile 5.0 až do verze 6.5.5, kdy vývoj ukončily. Následoval přechod na nový systém Windows Phone 7, 8, 8.1. V roce 2015 tento systém opět nahradila nová verze Windows 10 s přízviskem Mobile.[51][34]

Pocket PC 2000

Tento operační systém s velmi jednoduchým grafickým rozhraním, podporoval rozlišení 240x320 bodů. Tento systém podporoval vyměnitelné karty, umožňoval přenos souborů pomocí infračerveného záření (IR) a podporoval architektury procesorů SuperH SH-3, MIPS a ARM. Byl založen na Windows CE 3.0 jádru. Dodáván byl s rozsáhlou sadou základních aplikací vyvinutých pomocí Windows API vlastnostmi i vzhledem se podobali aplikacím desktopové verze operačního systému.

Pocket PC 2002

Tato verze byla vydána v říjnu roku 2001. Tento systém s kódovým označením „Merlin“ byl taktéž znám pod názvem Windows Mobile 2002. Stejně jako předchozí verze je provozován na jádru Windows CE 3.0. Tato verze se objevila na prvních chytrých zařízeních s podporou GSM telefonního modulu, což právě verze předchozí nepodporovala. Rozlišení 240x320 bodů bylo stále rozlišením maximálním. Vzhled této verze se podobal desktopové verzi Windows XP.

Windows Mobile 2003

Roku 2003 byla uvolněna nová verze Windows Mobile 2003. Byla založená na jádru Windows CE 4.2 a vyšla rovnou ve čtyřech edicích. Pocket PC Premium Edition, Pocket PC Professional Edition, Pocket PC Smartphone (zařízení s telefonním modulem bez dotykové obrazovky) a Pocket PC Phone Edition (v zařízeních s telefonním modulem s dotykovou obrazovkou).

Windows Mobile 2003 SE

V roce 2004 byla vydána ještě další verze s označením SE označující druhé vydání (Second Edition). Umožňovala již možnost otočení displeje na šířku i zpět na výšku. Tato verze podporovala rozlišení displeje VGA, tzn. 640x480 bodů a také podporu čtvercového rozlišení 240x240 a 480x480) pro výrobce s podporou hardwarové klávesnice. Také se zde objevuje chráněný přístup k Wi-Fi označovaný jako Wi-Fi Protected Access, tedy bezpečnějšího připojení k Wi-Fi nežli v té době již prolomené WEP zabezpečení.[51]

Windows Mobile 5.0

Verze s kódovým označením „Magneto“ byla představena v roce 2005. Jak je částečně i v jeho názvu vidět, poháněla ji Windows CE 5.0 a používá .NET Compact Framework 1.0 SP2

U této verze byla pozměněna práce s pamětí, data jsou ukládána do FlashROM paměti, paměť RAM je určena již pouze pro běh aplikací. Přidána byla centrální správa GPS pro navigační programy a také podpora USB 2.0

Windows Mobile 6

Roku 2007 byla vydána verze s kódovým označením „Crossbow“. Vydány byly opět tři verze operačního systému, Standard pro chytré telefony, Professional pro PDA s integrovaným telefonním modulem a Classic pro zařízení bez telefonního modulu. Byla zde přidána podpora 800x480 (WVGA), nově také podpora editace dokumentů Office na chytrých telefonech, automatické aktualizace systému, podpora VOIP (Voice Over IP – podpora přenosu hlasu přes internet, využívá se pro telefonování prostřednictvím internetu). Objevuje se také šifrování dat na paměťové kartě, podpora AJAX, JavaScript, XML DOM.

Windows Mobile 6.1

Vydána roku 2008. Tato verze byla již určena pouze pro zařízení s dotykovým displejem. Bylo upraveno celkové ovládání systému pro usnadnění práce na mobilním telefonu s tímto operačním systémem.

Windows Mobile 6.5

Roku 2009 byla vydána opět další verze Windows Mobile s označením 6.5. Opět systém přinesl nový vzhled přizpůsobený pro lepší ovládání prsty. Objevuje se zde první obchod aplikací Marketplace. Byly vydány ještě další podverze tohoto vydání systému, avšak žádné převratné novinky už nepřinesly.

Windows Phone 7

V druhé polovině roku 2010 vyšla nová převratná verze operačního systému Microsoft pro mobilní telefony. Přineslo grafické prostředí Metro, které umožňovalo více dotykové ovládání, integraci sociálních sítí (Facebook, Twitter, Windows Live Messenger a další), propojení s herní konzolí XBOX, ovládání hlasem, integrace cloudových uložišť, podnikových účtů (Exchange, Sharepoint, Lync, Office 365). Verze 7.5 Mango, Refresh, Tango z roku 2011 až 2012 přidaly podporu LTE sítí, podporu více operační paměti až do 256 MB RAM, podporu

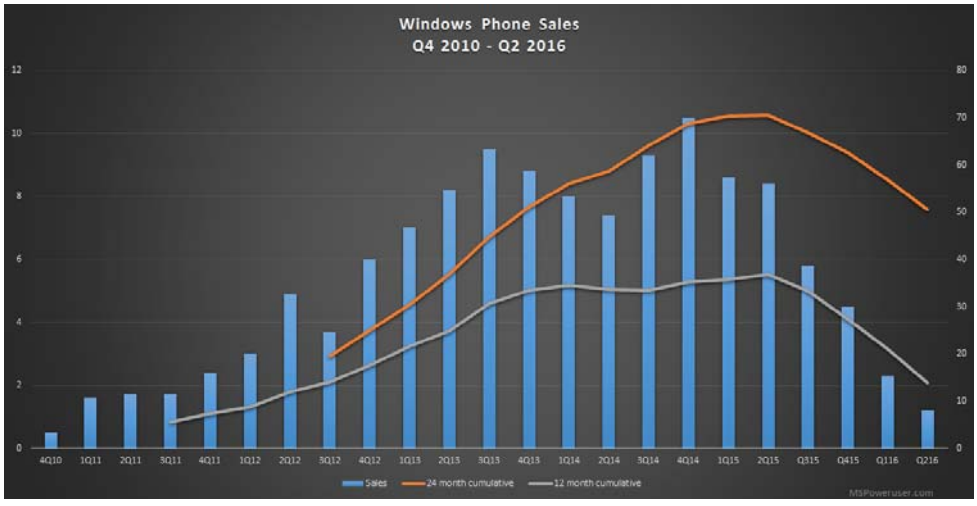
dalších regionů. Verze 7.8 přinesla následně i předělané, vylepšené rozhraní Metro (Modern UI)

Windows Phone 8

Osmá verze mobilního operačního systému Windows byla opět průlomová. Staré jádro založené na Windows CE bylo nahrazeno jádrem NT. Přerušilo tak ale zpětnou kompatibilitu s Windows Phone 7. V průběhu mnoha verzi byla přidána podpora FullHD rozlišení 1980x1020 bodů, moderních čtyřjádrových procesorů Qualcomm, nová hlasová asistentka Cortana, notifikační centrum, podpora DualSim (dvě sim v jednom telefonu), OTA aktualizace (Over The Air – aktualizace vzduchem, online), u verze 8.1. posledního vydání i podpora 4K rozlišení.

Windows 10 Mobile

Roku 2015 následovala nová, aktuální verze mobilního operačního systému, u kterého došlo k průlomovému odstranění slova „phone“ a návrat k původnímu „mobile“. Mobilní zařízení především značky Microsoft s tímto operačním se prodávají do dnes. Svá chytrá zařízení s tímto operačním systémem nabízejí i ostatní výrobci mobilních telefonů, avšak prodeje telefonů s tímto operačním systémem v poslední době velmi pokulhávají, což je vidět i na následujícím obrázku č.8. Společnosti Microsoft to jistě dělá nelehkou hlavu, objevují se na internetu zprávy o tom, že společnost Microsoft zvažuje ukončení výroby telefonů Lumia a také co bude nadále vůbec s divizí mobilních telefonů (viz obrázek VIII). Proto jsem se ve své práci zabýval již jen operačním systémem iOS a Android.[34]



Obrázek VIII: Prodej mobilních zařízení Windows Phone

Zdroj:[31]