



UNIVERZITET SINGIDUNUM

FAKULTET ZA INFORMATIKU I RAČUNARSTVO

Zaštita podataka na mobilnim uređajima sa studijom slučaja: Android OS

- Diplomski rad -

Mentor:

Doc. Dr Saša Adamović

Student:

Vladimir Ćirović

Br. indeksa: 2009/201785

Beograd, 2015.



FAKULTET ZA INFORMATIKU I RAČUNARSTVO

UNIVERZITET SINGIDUNUM

FAKULTET ZA INFORMATIKU I RAČUNARSTVO

Beograd, Danijelova 32

Kandidat: Vladimir Ćirović

Broj indeksa: 2009/201785

Smer: Informatika i računarstvo

Tema: Zaštita podataka na mobilnim uređajima sa studijom slučaja: Android OS

Datum odobrenja rada:

Beograd, ____ . ____ . ____ .

MENTOR

Doc. dr Saša Adamović

DEKAN

Prof. dr Miroslav Lutovac

Zaštita podataka na mobilnim uređajima sa studijom slučaja: Android OS

Sažetak:U ovom radu bavićemo se analizom bezbednosti BYOD (*Bring Your Own Device*) koncepta mobilnih uređaja krozMDM (*Mobile Device Management*) sistem, kao i pregledom najčešćih slučajeva sigurnosnih pretnji i napada. Takođe, predstavimo arhitekturu i ranjivost *Android* platforme, zatim implementirana, kao i neka *third party* sigurnosna rešenja. Pored toga predložićemo neka rešenja za povećanje bezbednosti kako samo uređaja tako i podataka koji se nalaze na njemu, kao i predloge za budući rad.

Poslednjih nekoliko godina, mobilni uređaji preplavili su privatno i poslovno okruženje koristeći se na dnevnoj bazi, između ostalog, za skladištenje bitnih podataka na samom uređaju. Uređaji kao što su mobilni telefoni, tableti, laptopovi i drugi predstavljaju nove sigurnosne pretnje, pogotovu u slučaju posedovanja osetljivih informacija unutar kompanija vodeći se BYOD konceptom. Kako bi uspostavili kontrolu nad ovim uređajima i podacima koji se nalaze na njima, bitna je implementacija sigurnosnih rešenja kao što je MDM odnosno softvera koji omogućava daljinski pristup, putem interneta, mobilnim uređajima. Danas je ovaj sistem implementiran gotovo na svim popularnim platformama kao što su *Android*, *iOS*, *Windows Phone* itd.

Međutim kao i svaki sistem, i ovaj ima svoje nedostatke i propuste, na koje ćemo, u ovom radu, skrenuti pažnju i pokušati da ih obrazložimo. Predstavimo aktuelni pregled pretnji, kao i predloge kako zaštititi mobilne uređaje za BYOD. Rezultati istraživanja pokazuju da je upravo*Android* najranjivija platforma.

Ključne reči:Android OS, BYOD, MDM

Sadržaj

Spisak slika.....	- 3 -
Spisak tabela.....	- 3 -
1 Uvod.....	- 4 -
1.1 Predmet istraživanja	- 5 -
1.2 Metodi istraživačkog rada	- 5 -
2 Pregled pretnji u oblasti istraživanja.....	- 6 -
2.1 Opšti problemi unutar BYOD	- 6 -
2.2 Malware.....	- 7 -
2.3 Curenje podataka i krađa	- 8 -
2.4 Socijalni inženjering	- 8 -
2.5 Phishing	- 9 -
2.6 Ranjivost softvera	- 9 -
3 Pregled Android platforme	- 11 -
3.1 Arhitektura Android platforme.....	- 11 -
3.2 Ranjivost Android platforme	- 13 -
3.3 Podrška Android platforme	- 15 -
3.4 Android Device Manager.....	- 17 -
3.5 Dodatna rešenja.....	- 20 -
3.5.1 Google Apps.....	- 20 -
3.5.2 Exchange ActiveSync	- 20 -
3.5.3 HTCpro MDM.....	- 20 -
3.5.4 Samsung SAFE.....	- 20 -
3.5.5 Samsung KNOX.....	- 20 -
4 Obezbeđivanje mobilnih uređaja.....	- 21 -
4.1 Zaključavanje ekrana.....	- 21 -

4.2	Daljinsko zaključavanje i brisanje	- 24 -
4.3	Šifrovanje.....	- 24 -
4.4	Kontrola aplikacija.....	- 25 -
4.5	Životni ciklus uređaja	- 25 -
4.5.1	Inicijacija	- 26 -
4.5.2	Razvoj	- 27 -
4.5.3	Implementacija	- 27 -
4.5.4	Upravljanje i održavanje.....	- 27 -
4.5.5	Uklanjanje.....	- 28 -
4.6	Sumiranje.....	- 28 -
4.7	Predlozi i saveti u praksi	- 29 -
4.7.1	Zaštita od fizičkog oštećenja.....	- 29 -
4.7.2	Zaštita od krađe uređaja	- 30 -
4.7.3	Zaštita informacija.....	- 30 -
5	Zaključak	- 32 -
5.1	Sumarni ciljevi rada.....	- 32 -
5.2	Predlog za budući rad – Operater mobilne mreže MNO	- 33 -
6	Literatura	- 35 -

Spisak slika

Slika 2.1 – Ilustracija BYOD koncepta [32]	- 6 -
Slika 2.2 – APT životni ciklus [27].....	- 7 -
Slika 3.1 – Ilustracija Android logoa.....	- 11 -
Slika 3.2 – Arhitektura Android operativnog sistema [9].....	- 13 -
Slika 3.3 – Omogućavanje daljinskih dozvola – LG L9.....	- 18 -
Slika 3.4 – Android Device Manager korisnički interfejs – LG L9	- 18 -
Slika 3.5 – Opcija zvonjenja telefona – LG L9	- 19 -
Slika 3.6 – Opcija menjanja šifre zaključavanja ekrana – Google Chrome	- 19 -
Slika 3.7 – Opcija fabričkog resetovanja – Google Chrome	- 19 -
Slika 4.1 – Ilustracija obezbeđivanja mobilnih uređaja [33]	- 21 -
Slika 4.2 – Podešavanje zaključavanja ekrana – LG L9.....	- 22 -
Slika 4.3 – Podešavanje PIN-a – LG L9	- 23 -
Slika 4.4 – Neuspelo otključavanje ekrana – LG L9.....	- 23 -
Slika 4.5 – Životni ciklus uređaja.....	- 26 -
Slika 5.1 – Tipovi MDM provajdera.....	- 33 -

Spisak tabela

Tabela 3.1 – Android nivoi zaštite	- 12 -
Tabela 3.2 – Android matrica funkcionalnosti	- 16 -

1 Uvod

Upotreba mobilnih uređaja se dramatično povećala u protekloj deceniji, pogotovu u poslovnom kao i u privatnom sektoru, gde većina građana zavisí od upotrebe pametnih telefona u svakodnevnom životu. Danas kompanije traže veću fleksibilnost od svojih zaposlenih koja podrazumeva mogućnost pristupa elektronskoj pošti, kalendaru i drugim podacima unutar kompanije na daljinu, odnosno putem Interneta. Tržište je postavilo novi trend gde zaposleni radije koriste svoje privatne umesto službenih uređaja zarad poslovnih aktivnosti i ovaj fenomen se podrazumeva pod terminom *Bring Your Own Device* (BYOD) u prevodu: donesi svoj uređaj.

BYOD se odnosi na koncept gde je zaposlenima dozvoljeno da koriste svoje privatne uređaje (mobilni telefoni, tableti, laptopovi, netbukovi) u poslovne svrhe radi pristupa internih resursa kompanije, što nudi veću slobodu i fleksibilnost za zaposlene, a pritom smanjuje troškove kompanije po pitanju održavanja i podrške. Pošto su zaposleni zaduženi za odgovornost sopstvenih uređaja, to ostavlja prostora kompanijama da se, prvenstveno, fokusiraju na sigurnost svojih podataka, što se pokazalo kao ne tako lak zadatak. Iako BYOD koncept donosi mnoge beneficije, takođe predstavlja nove i značajne rizike kao i sigurnosne izazove.

Uobičajeno je da poslodavac obezbeđuje uređaje svojim zaposlenima koji su u vlasništvu kompanije i stoga nisu u vlasništvu zaposlenih. Tada kompanija stiče kontrolu nad uređajima i sadržaju koji se nalazi na njima. Preduzeća su imala ogroman uticaj nad ovim uređajima, pogotovu u implementaciji različitih DM (*Device Management*) rešenja koja su se odnosila na postavku odredbi, kontrolu pristupa, kontrolu aplikacija itd. Međutim, pošto nije moguće kontrolisati privatne uređaje na isti način, BYOD dolazi sa nekoliko bezbednosnih problema koje bi trebalo rešiti.

- Kako dozvoliti nepouzdate uređaje (uređaji koji nisu pod kontrolom organizacije) u okviru infrastrukture organizacije?
- Kako osigurati poverljivost i verodostojnost internih resursa?
- Kada se nepouzdati uređaji mogu smatrati pouzdanim? Koje uslove bi trebalo ispuniti?

Rastuća zabrinutost zbog rizika i izazova implementacije BYOD-a, dovela je do razvitka novog sigurnosnog rešenja koje se zove *Mobile Device Management* (MDM). MDM rešenje postaje vrlo popularno unutar BYOD implementacije, nudeći servise kao što su zaštita, praćenje, upravljanje kao i podršku za mobilne uređaje različitih firmi i modela. Primarni cilj MDM-a je sprovođenje bezbednosti u implementaciji BYOD-a kao i da pojednostavljuje bezbednost fokusiranjem na operacije kao što su detekcija *malware*-a, zaključavanje *PIN/Password*-a, restrikcija sumnjivih aplikacija, zaključavanje na daljinu, potpuno ili selektivno brisanje podataka. Glavne komponente MDM rešenja su klijent i server. Klijent komponenta je instalirana kao aplikacija na mobilnom uređaju kojim želimo da upravljamo, dok je server zadužen za sprovođenje instrukcija i monitoringa uređaja. Nakon registracije klijenta na dodeljeni server, klijent će slati status svog uređaja, sa druge strane kada server od klijenta zahteva neku operaciju, poslaće *push message* poruku

uređaju sa instrukcijama koje će biti izvršene. Slanje instrukcija na daljinu predstavlja temelj MDM bezbednosti u cilju očuvanja integriteta mobilnog uređaja.

1.1 Predmet istraživanja

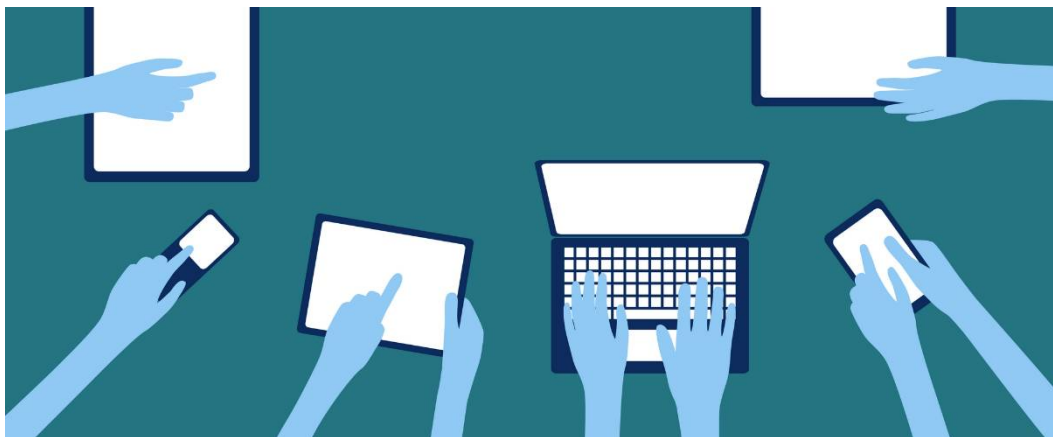
Cilj ovog rada biće istraživanje mogućnosti i ograničenja BYOD rešenja uopšte, kao i podrška za Android platformu. Cilj je da se utvrdi nivo podrške koji se odnosi na MDM funkcionalnost i može se koristiti za poboljšanje rešenja za BYOD. Problem leži u činjenici da su različite platforme nezavisne i ne dele zajedničke standarde ili javne okvire kako bi se osigurao MDM. U cilju pružanja sveobuhvatne politike za BYOD koristeći MDM funkcionalnost na različitim platformama, mora postojati zajednički nivo zaštite koja se može primeniti na svakom uređaju nezavisno od platforme.

Količina napada na mobilne uređaje se povećava, stoga je relevantno da se razmotri nivo pretnje na svakoj platformi kako bi odredili mere za zaštitu protiv njih. Istraživaćemo glavne pretnje kao i neophodna rešenja kako bi se smanjio nivo rizika i cilj će nam biti da se istraže mogućnosti i ograničenja BYOD na Android platformi. Takođe, utvrdićemo nivo podrške koji se odnosi na funkcionalnost MDM u cilju poboljšanja BYOD koncepta. Ovim istraživanjem, pokušaćemo da utvrdimo mogućnosti i ograničenja, bilo zbog nedostatka podrške u OS-u (*Operating System*) ili ograničenja zadata od strane OEM-a (*Original Equipment Manufacturer*). Konačno predstavimo predlog za budući rad gde bi MNO (*Mobile Network Operator*) obezbedio BYOD uslugu, kao i korišćenje SIM kartice za BYOD rešenje, čime bi ostavili prostora za dalje istraživanje mogućih prednosti u ovom scenariju.

1.2 Metodi istraživačkog rada

Istraživanje ovog rada utemeljeno je na osnovu domaće i strane literature, pre svega dostupne na internetu. Većina materijala koja se tiče, pre svega, Android platforme, dobavljen je od strane odgovarajućeg proizvođača kako bi se opisala funkcionalnost i sigurnosna arhitektura platforme. Informacije o individualnim nedostacima i propustima su okupljeni sa raznih izvora i publikacija i bezbednosnih istraživanja nekoliko firmi koje se bave bezbednošću mobilnih uređaja. Svaki scenario pretnji se određuje na osnovu izveštaja objavljenih od strane bezbednosnih firmi kako bi se opisao trenutni opseg pretnji i bezbednosnih nedostataka koji su se dešavali u prošlosti. Primeri koji opisuju ove proboje bezbednosti su pomenuti kako bi čitaocu pružili uvid u širu perspektivu o mogućim posledicama koje mogu imati veliki uticaj na kompanije i organizacije.

2 Pregled pretnji u oblasti istraživanja



Slika 2.1 – Ilustracija BYOD koncepta [32]

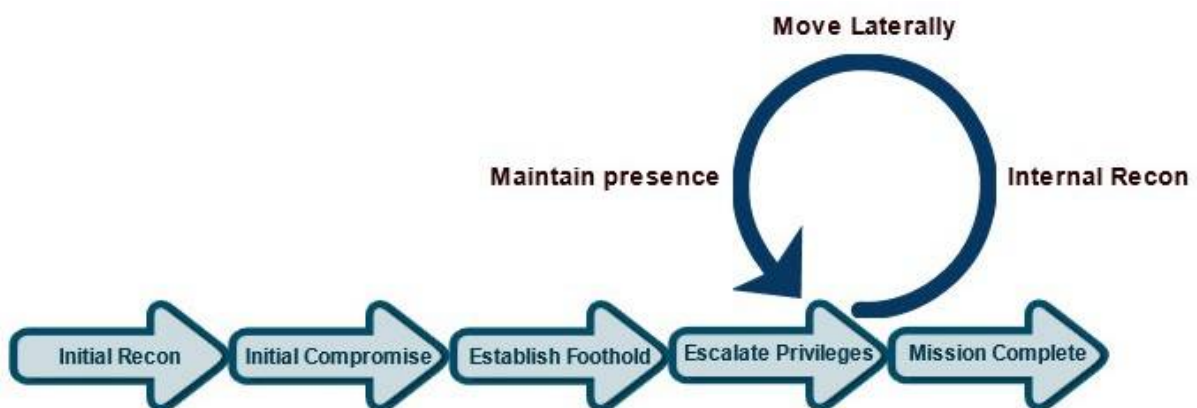
U oba slučaja, profitabilne ili neprofitabilne organizacije, predstavljaju potencijalne mete u rastućem opsegu sajber pretnji, tržište izveštava o eskalaciji pretnji kao što su *malware*, *Advanced Persistent Threat* (APT), *Distributed Denial of Service* (DDoS) i mnogim drugim vrstama napada koji su usmereni protiv preduzeća[1, 2]. Spisak napadača može imati opseg od takozvanih *scriptkiddies*, tinejdžera koji koriste već postojeće zlonamerne softvere u cilju vandalizacije tuđih računarskih sistema radi sopstvene zabave, do ciljanih i *stealth*, odnosno nevidljivih napada, napravljenih, ili naručenih od strane konkurentnih kompanija, aktivističkih grupa ili čak od strane savezne vlade. Primarni cilj ovih napada jeste ranjivost personalnih računara, međutim povećanom upotrebom pametnih telefona i tableta, tržište postaje svedok sve većih napada na mobilne uređaje.

2.1 Opšti problemi unutar BYOD

Stroga kontrola pristupa primenjuje se na uređajima koji su u vlasništvu kompanija u cilju sprečavanja neovlašćenog pristupa i obično se upravlja putem MDM softvera koji može biti obezbeđen i od strane *third party* proizvođača. Međutim kod privatnih uređaja ne postoji garancija da će bilo koja od ovih beneficija sigurnosnog softvera zaštititi uređaj i podatke na njemu. Elektronska pošta, prilozi koji idu uz elektronsku poštu ili neki drugi podaci unutar kompanije, ranjivi su i mogu se proslediti kroz zlonamerne softvere ili konektovanjem uređaja na nepouz dane laptopove. Kompanije takođe nemaju mogućnost da upravljaju uređajima koji su izgubljeni ili ukradeni, s toga uređaj, koji nije više u posedstvu svog namenjenog korisnika, može staviti intelektualnu svojinu kompanije u opasnost. Ukoliko uređaj nije zaštićen PIN-om (*Personal Identification Number*) ili lozinkom (*Password*), tada napadač može dobiti direktan pristup uređaju i njegovom sadržaju. Međutim uređaji koji su zaštićeni lozinkom i dalje mogu biti podložni krađi podataka ukoliko su konektovani na Internet ili povezani npr. na laptop. Privatni uređaj treba smatrati nepouzdanim u poslovne svrhe sve dok se ne sprovede odgovarajući pregled bezbednosti koji bi potvrdio da je uređaj pouzdan, npr. instalacijom klijent aplikacije koja potvrđuje da uređaj ispunjava sve uslove pravila kompanije.

2.2 Malware

Malware predstavlja generalnu klasifikaciju zlonamernih, odnosno malicioznih softvera (*Malicious software*) kao što su virusi, *rootkit*-ovi, Trojanci itd. čija je osnovna namena uništenje ili krađa podataka. Definicija *malware*-a menjala se tokom poslednjih godina i može se podeliti u dve kategorije: tradicionalni ili moderni *malware*. Tradicionalni *malware* se odnosi na klasičnu formu *malware*-a čiji je cilj infekcija i širenje kroz što veći broj uređaja, pritom nanoseći što veću štetu sistemu, bez nekog posebnog razloga ili motiva iza napada. Moderni *malware* je sofisticiraniji i strateški isplaniran. APT (*Advanced Persistent Threat*) je primer modernog *malware*-a koji postaje sve češći primer rizika. APT je dobro isplanirani sajber napad koji ima određenu metu i sprovodi se iz više etapa kako bi postigao određeni cilj, pritom je nevidljiv kako bi izbegao detekciju. Ovo predstavlja osnovnu razliku između tradicionalnog i modernog *malware*-a, a to je da je moderni *malware* ciljan i nevidljiv. Specifičan odabir mete, uzimajući u obzir da ima određenu vrednost za napadača, i izbegavanje detekcije je od suštinskog značaja kako bi se sproveo prolongirani napad koji može trajati duži vremenski period i dokle god prolazi nedetektovan, više podataka će proslediti.



Slika 2.2 – APT životni ciklus [27]

Karakteristike APT životnog ciklusa mogu se opisati kao sekvencijalni procesi koji uključuju istraživanje, upad, sakupljanje akreditiva, ekstrakciju podataka i čišćenje [3]. Prvi korak podrazumeva istraživanje mete u cilju pronalaženja slabih, ili ulaznih, tačaka u perimetru kompanije, kao i određivanje lokacije informacije koja može biti u interesu napada. Napadač pretražuje ranjivost, a zatim je eksploatiše kako bi započeo inicijalni upad koristeći se tehnikama kao što *suphishing* ili socijalni inženjering (*Social engineering*). Nakon ulaska, *malware* cirkuliše sve dok traženi akreditivi ne budu nađeni kako bi se uspostavio pristup ciljanim podacima, koji će, eventualno, biti ekstraktovani i prosleđeni napadaču putem udaljenog servera. Nakon što je prosleđivanje podataka završeno, *malware* sprovodi čišćenje za sobom kako bi prikrio svoje tragove. Mogu biti potrebne nedelje ili čak meseci pre nego što iko otkrije da je napad uopšte bio izvršen.

Autori modernih *malware*-ova počeli su da ciljaju mobilne uređaje i *Android* je platforma po njihovom izboru. Primer APT napada na *Android* skorije se odigrao, a meta je bila tibetanska aktivistička grupa. Koristeći se kompromitovanim *e-mail* nalogom, napadač je uspeo da pošalje lančani *e-mail* koji je u svojoj sadržini imao zlonamerni *.apk* fajl (*Android application file*)[4]. Napad je detaljnije opisan u nastavku rada.

2.3 Curenje podataka i krađa

Informaciona bezbednost od suštinskog je značaja za bilo koje preduzeće koje želi da zaštiti poverljive poslovne informacije koje mogu biti u raznim formama kao što su dokumenti, prezentacije, proračuni, patent, evidencije o zaposlenima i sl. Curenje podataka i krađa u ovom kontekstu se odnosi na podatke koji su primljeni i sačuvani na prostoru za skladištenje na mobilnom uređaju i gde postoji više načina za curenje ili krađu ovih podataka od strane *third-party* aplikacije. *Malware* je jedna od njih, međutim, takođe mogu biti napadnuti fizičkim pristupom uređaju, koristeći se elektronskom poštom ili spoljnim medijumom.

Zlonamerne aplikacije eventualno mogu da prate aktivnosti korisnika iskorišćavanjem nekih karakteristika uređaja kao što je GPS (*Global Positioning System*), *screen capture* opcije, zvučnih zapisa itd. Neovlašćeno korišćene ovih informacija takođe se može smatrati kao krađa podataka ili njihovo praćenje, koje ima potencijala da se iskoristi u svrhe industrijske špijunaže. Napadač tada može da špijunira zaposlene u realnom vremenu, kao i da sluša privatne razgovore, prati lokaciju korisnika ili čak snima fotografije dokumenata koji bi se našli u blizini i tako otkrio poverljive dokumente.

Jailbreak se takođe može smatrati zlonamernim. *Jailbreak*-ovan (*root*-ovan) uređaj može biti ranjiviji nego regularan uređaj sa instaliranim zlonamernim aplikacijama, jer je osnovni softver (*bootloader*, *firmware*) *flash*-ovan i bezbednost od strane Androida može biti kompromitovana i van funkcije. Tada korisnici imaju mogućnost upravljanja *root* pristupa sistemu kao i prosleđivanja ovog pristupa ostalim aplikacijama kako bi omogućili korišćenje dozvola visokog rizika ovih aplikacija, što nije moguće sa ne *jailbreak*-ovanog uređaja. Iz tog razloga, korišćenje *jailbreak*-ovanih uređaja treba zabraniti u poslovne svrhe kako bi sprečili dalje širenje privilegija visokog rizika od strane zlonamernih aplikacija.

Snooping je još jedna mogućnost i odnosi se na praćenje saobraćaja unutar mreže kao i na monitoring podataka koji se razmenjuju, takođe može biti korišćen i za špijunažu. Cilj ovoga jeste da se prikupe korisnička imena, lozinke ili drugi tipovi podataka koji mogu biti od važnosti. Internet nije dizajniran sa implementiranim sigurnosnim sistemom, prema tome ukoliko podaci nisu pravilno šifrovani, lako mogu biti *snoop*-ovani od strane iskusnijih napadača.

2.4 Socijalni inženjering

Utehničkom smislu, socijalni inženjering se odnosi na napade gde se upotrebljavaju društvene veštine u cilju prikupljanja informacija o računarskim sistemima[5]. Osobe koje praktikuju socijalni inženjering (prevaranti, foliranti) koriste socijalnu interakciju da, ili prevare svoje žrtve kako bi dobili od njih informaciju, ili manipulacijom kojom bi stekli poverenje žrtve koja bi kasnije podelila informaciju sa njima. Obično, napadač bi koristio

lažni identitet, npr. predstavljajući se da je novi zaposleni u istoj firmi kao i žrtva. Postoje izveštaji o napadačima koji su uspjeli da dobiju informacije o kreditnim karticama, transakcijama, lozinkama, akreditivima i mnogim drugim informacijama služeći se finesama i tehnikama socijalnog inženjeringa. „*The Art of Deception*“ [6] opisuje nekoliko scenarija iz stvarnog života u kome su tehnike socijalnog inženjeringa korišćene u praksi za hakovanje računarskih sistema velikih razmera.

Ova vrsta napada, konkretno ne predstavlja pretnju samo za BYOD već generalno za sve vrste računarske i mobilne sigurnosti.

2.5 Phishing

Phishing je oblik socijalnog inženjeringa, odnosno pokušaj sticanja osetljivih informacija od korisnika uveravajući ih da je u legitimne svrhe [7]. Napad se obično sprovodi upotrebom elektronske pošte ili zlonamerne Internet stranice kao osnovnog alata. *Phishing-mail* se može prerusiti tako da izgleda kao da potiče od banke ili IT odeljenja u kome je zaposlena žrtva, i može sadržati upit u lične ili finansijske informacije, kao što su informacije o kreditnoj kartici i lozinke. Postoji napredniji oblik fišinga poznat kao *spear phishing* koji se odnosi na ciljan napad u kome je meta unapred određena, u zavisnosti od uloge ili položaja u organizaciji gde se lako može dobiti određeni nivo ili odobrenje pristupa. Izabranoj meti je možda odobren pristup informaciji koja je potrebna napadaču kako bi dobio odgovarajuće odobrenje u cilju sprovođenja većeg napada, kao što je APT napad.

2.6 Ranjivost softvera

Ranjivost softvera predstavlja konstantni sigurnosni rizik bilo koje aplikacije i vreme koje prođe između otkrića nedostatka i popravke i zakrpe, predstavlja rizik od eksploataisanja tog softvera. Internet pretraživači, koji se mogu naći na svakom PC ili mobilnom uređaju danas, su tipičan primer. Ukoliko autori *malware*-a otkriju prolaz ili manu, onda je mogu iskoristiti kako bi ubrizgali zlonamerni kod koji može uticati na milione uređaja sve dok se ta mana ne zakrpi na korisničkom sistemu. Svake godine *Open Web Application Security Project* (OWASP) objavljuje listu deset najčešćih ranjivosti softvera [8] koje se uglavnom odnose na Internet pretraživače. Nije toliko uobičajeno da korisnici Internet pretraživača osete katastrofalne posledice ovih napada, međutim svi mobilni uređaji imaju već ugrađene pretraživače koji su klasifikovani kao sistemske aplikacije, što znači da su deo operativnog sistema i imaju pristup sistemskim resursima. Takođe bi trebalo napomenuti da ranjivost Interneta nije ograničena na samoj pretraživačkoj aplikaciji i propusti koji se nalaze u *web* tehnologijama kao što su *ActiveX* i *JavaScript* su takođe na meti sa namerom izvršavanja zlonamernog koda. Upotreba QR(*QuickResponse*) kodova je jedan primer gde legitimna funkcionalnost može biti iskorišćena od strane *malware* autora i mogu se smatrati nesigurnim. QR kod je matični tip bar koda koji se može skenirati kamerom na mobilnom uređaju preko QR aplikacije. Skenirani kod može biti preveden na URL (*Uniform Resource Locator*) koji upućuje na Internet stranicu ili preuzimanje aplikacije, obično se automatski otvara od strane Internet pretraživača i može se iskoristiti za preuzimanje zlonamernih aplikacija. Napadač može napraviti QR kod koji uključuje URL koji sprovodi korisnika do zlonamernog .apk fajla, pritom maskirajući ga u legitimnom kontekstu, kao npr. lažni oglaš

na nekom popularnom sajtu. Kod je nemoguće prevesti direktno od strane korisnika koji ne može znati da li je kod legitiman ili ne, pre nego što ga skenira.

3 Pregled Android platforme



Slika 3.1 – Ilustracija Android logoa

The Android Open Source Project[9] je platforma otvorenog koda koja je prvobitno razvijena od strane *Android Inc.* kompanije, kasnije je kupuje *Google* 2005. godine koji predstavlja prvu verziju 2007. godine zajedno sa osnivanjem *Open Handset Alliance* (OHA), odnosno organizacijom koja postavlja otvorene standarde za mobilne uređaje[10].

Razvojni tim je želeo da *Android* bude otvoren i slobodan, zbog toga je najveći deo *Android* koda bio pod *Apache License* licencom, koja se odnosi na otvoreni kod, što znači da svako može da koristi *Android* preuzimanjem njegovog izvornog koda. Štaviše, proizvođači (pre svega, hardvera) mogu da dodaju sopstvene ekstenzije i podešavaju *Android* u skladu sa svojim proizvodima kako bi se oni razlikovali u odnosu na druge proizvode[11].

3.1 Arhitektura Android platforme

Android platforma bazirana je na *Linux*-u od koga je direktno nasledila neke od bezbednosnih karakteristika kao što je *sandboxing*. *Sandboxing* radi na principu da se svaka aplikacija izvršava kao odvojeni proces koristeći *UniquelIdentifier* (UID) kako bi je izolovao od ostalih aplikacija i omogućio joj pristup samo svojim resursima. Na primer, aplikacija A ne može čitati fajlove koji pripadaju aplikaciji B i obrnuto. Međutim, postoji mogućnost da više aplikacija dele isti proces (UID) ukoliko dele istog izdavača. Izdavač može odrediti u specifikaciji aplikacije (*manifest file*) koji određuje da li će deliti isti UID sa nekom drugom aplikacijom, koja je prethodno instalirana i koja potiče od istog izdavača.

Android aplikacija može koristiti nekoliko sistemskih resursa. Međutim, većina njih biće zabranjena bez odgovarajuće dozvole. Dozvole (*permissions*) su potrebne kako bi dobili pristup funkcijama operativnog sistema kao što je pristup Internetu ili funkcijama koje su nisu besplatne kao što je SMS. Dozvola za određeni resurs mora biti precizno deklarirana u manifestu aplikacije i korisnik mora prihvatiti više osetljivih dozvola tokom instalacije. Korisniku će biti ponuđena lista svih dozvola koje su deklarirane aplikacijom, kako bi imao neku vrstu uvida u ponašanje aplikacije. Postoji četiri vrste dozvola koje su razvrstane na osnovu potencijalnog uticaja koje mogu imati na sistem. Ove kategorije možemo videti na tabeli 3.1.

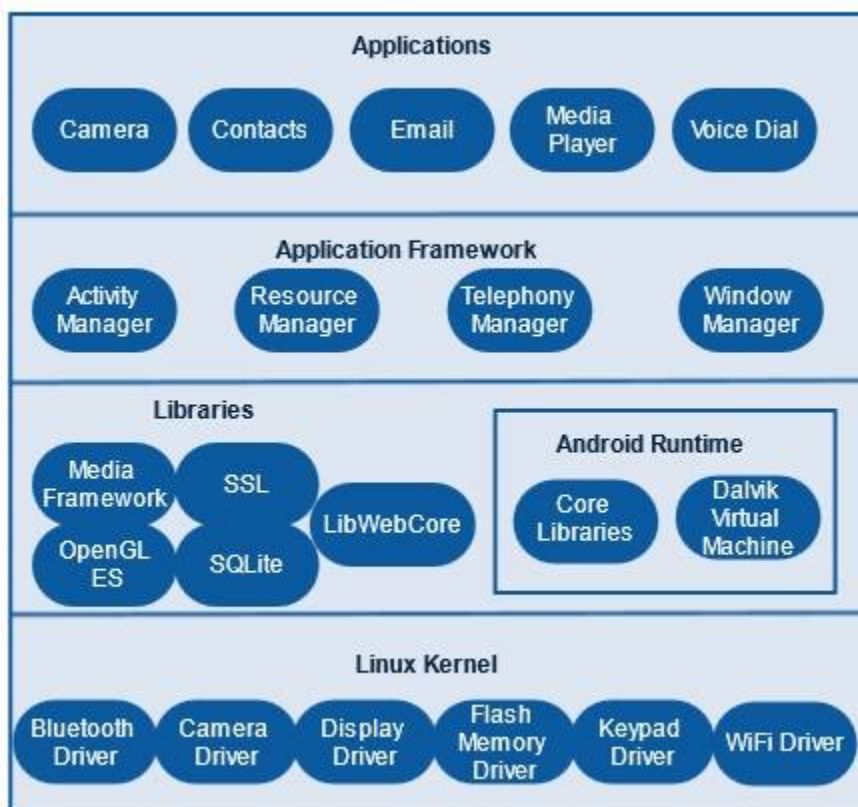
<i>Normal</i>	Dozvole niskog rizika; odobrava se automatski bez bilo kakve interakcije korisnika ili obaveštenja prilikom instalacije.
<i>Dangerous</i>	Dozvole srednjeg rizika; odobrava se od strane korisnika prilikom instalacije. U suprotnom aplikacija neće biti instalirana. Dozvole se ne mogu selektivno odobriti, stoga ili su sve dozvole odobrene ili ni jedna.
<i>Signed</i>	Dozvole visokog rizika; ove dozvole su veoma jake, ali nisu dostupne za redovne programere. Aplikacija mora imati <i>firmware</i> potpis kako bi imala ove dozvole.
<i>SystemOrSigned</i>	Isto kao i kod prethodnih dozvola, osim što se dozvole odobravaju svim aplikacijama koje su instalirane u <i>system/apps</i> direktorijumu na uređaju.

Tabela 3.1 – Android nivoi zaštite

Deklaracije dozvola omogućavaju sistemu u praćenju i ograničavanju aplikacija koje pokušavaju da komuniciraju van svog izolovanog virtuelnog okruženja kako bi se sprečio veći uticaj zlonamernih aplikacija nad sistemom.

Android projekat poseduje svoju virtuelnu mašinu (VM) pod imenom *Dalvik Virtual Machine* (DVM) koja je softver otvorenog koda, odgovoran za upravljanje aplikacijama na Androidu. Prilagođen je uređajima koji crpe snagu iz baterija i koji koriste ograničene procesorske jedinice (CPU) ili memorijske resurse. Zbog svojih niskih zahteva za resursima, DVM može efikasno raditi na više VM instanci istovremeno, što predstavlja dobar kvalitet za *sandboxing*. *Java* radi na DVM, što se razlikuje od tradicionalne *Java* virtuelne mašine (JVM) koja se inače koristi u *Java*[12]. Ova kompilacija se može posmatrati kao proces iz dva koraka; *Java* prevodilac (kompajler) stvara JVM bajt kod prevođenjem izvornog koda i skladišti ga kao klasni fajl. Zatim *Dalvik* prevodilac koristi kompajlirani klasni fajl i prevodi ga u jedan *.dex* fajl, koji će biti deo konačnog paketa aplikacija za *Android* (*.apk*).

Androidboot proces može se ukratko opisati u šest koraka [13]. Prilikom uključivanja uređaja izvršava se *Boot Read-Only Memory* (ROM) kod koji je utisnut u hardver. Time se učitava *boot loader* u RAM memoriju i nakon izvršavanja ROM-a, nastaviće sa *boot loader*-om. *Boot loader* će izdvojiti zaseban deo iz RAM memorije i učitati *glavniboot loader* u nju. Tada se parametri nižeg sloja aktiviraju u sistemu, kao što su konfiguracije sistemskih datoteka i dodatnih sredstava memorije, i ukoliko je ovaj proces uspešan, tada će nastaviti sa učitavanjem *Linux* jezgra.



Slika 3.2 – Arhitektura Android operativnog sistema [9]

Linux jezgro je odgovorno za učitavanje sistema, npr. učitavanje drajvera, kako bi sve funkcionisalo pravilno. Kada je učitavanje završeno, tada jezgro locira *init.rc* fajl u *root* fajl sistemu. Ovo je *root* čvor iz koga će svaki budući proces biti pokrenut dok će sve ovo na kraju pokrenuti proces koji se zove *Zygote* koji učitava DVM.

Sledeći i poslednji korak u procesu podizanja sistema je pokretanje i izvršavanje sistemskog servera koji će pokrenuti sve *Android* servise i upravljače. Različiti servisi se mogu videti na slici 3.1. Onog trenutka kada su svi servisi učitani pravilno, tada je proces *boot*-ovanja završen.

3.2 Ranjivost Android platforme

U septembru 2012. godine, 25 milijardi aplikacija je preuzeto sirom sveta preko *Google Play™* aplikacije od njenog lansiranja 2008. godine [14]. U poređenju na prethodnu godinu, kada je barijera od 10 milijardi aplikacija probijena u istom periodu, što ukazuje na značajan porast od 15 milijardi novih aplikacija u periodu od samo jedne godine.

Juna 2013. godine *Juniper Networks* prijavio je da su se *malware* pretnje povećale za 600% tokom proteklih par godina [15]. Izveštaj je baziran na osnovu istraživanja koje je sproveo *Juniper Networks Mobile Threat Center (MTC)* u periodu od marta 2012. do marta

2013. Ovo istraživanje pokazuje da se nivo pretnje mobilnih uređaja ubrzano povećava kako tržište raste dok se broj novih razvijenih aplikacija strahovito širi.

Google nema proces odobravanja na *Google Play™* aplikaciji, što čini da su aplikacije momentalno dostupne. Međutim, to ne predstavlja utočište za mobilni *malware*. Početkom 2012. godine *Google* predstavlja uslugu na *Google Play* koja se zove *Bouncer*[16]. *Bouncer* je automatski servis za skeniranje koji proverava potencijalno zlonamerne softvere i vrši analizu aplikacija čim su postavljene. *Bouncer* će izvršiti program u okviru *Google Cloud* infrastrukture kako bi simulirao njegovo ponašanje na virtuelnom *Android* uređaju. Cilj je bio da se doda još jedan sloj zaštite koji će se baviti povećanjem *malware*-a na *Google Play™*. Međutim, juna 2012. godine poznati istraživači *malware*-a *Charlie Miller* i *Jon Oberheide* objavljuju izveštaj u kome su bili u stanju da prodru u *Bouncer* i pronađu ograničenja koja su im dozvolila da podnesu zlonamerne aplikacije i prođu neotkriveni [17, 18]. *Bouncer* obavlja dinamičku analizu podnetih aplikacija pri čemu sam test traje samo pet minuta. Ukoliko zlonamerni sadržaj ili ponašanje ne biva pronađeno u ovom procesu, tada aplikacija prolazi test. Autori zlonamernih aplikacija su zato u stanju da izbegnu *Bouncer* ili odlaganjem izvršavanja ili preuzimanjem zlonamernog sadržaja kasnije.

Da bi se aplikacija objavila na *Google Play™* mora biti digitalno potpisana od strane autora. Međutim, ne postoje zahtevi o aktuelnim sertifikatima i samo-potpisani sertifikati se mogu koristiti. Samo-potpisani sertifikati su oni koji su potpisani od strane sopstvenog privatnog ključa što znači da programeri mogu lako da naprave lažne sertifikate kako bi potpisali njihove aplikacije bez otkrivanja bilo kakvih ličnih informacija, što omogućava prijavljivanje zlonamernih aplikacija na *Google Play™* anonimno. Zato, zbog nedostatka pregleda aplikacija, moguće je prerađivanje zlonamernih aplikacija kao postojećih, legitimnih aplikacija koristeći se sličnim opisom i grafikom na *Google Play™*. Ovo može prevariti većinu korisnika koji će preuzeti i instalirati zlonamernu aplikaciju umesto aplikacije koju su zapravo hteli da preuzmu.

26. marta 2013., sigurnosna kompanija *Kaspersky Lab* predstavila je detalje koji se tiču jednog od prvih ciljanih napada na *Android* platformu koji je nedavno otkriven [4]. Napad je sproveden samo nekoliko dana pre i bio je usmeren ka tibetanskim aktivistima uz pomoć kompromitovanog *e-mail* naloga i veruje se da je izvršen od strane Kineske vlade.

Nalog je pripadao aktivisti visokog profila i iskorišćen je od strane napadača kako bi poslao *spear-phishing* poštu, na celu listu kontakata vlasnika, koja je sadržala zlonamerni *.apk* fajl.

Većina prijemnika nisu imali nikakvih saznanja o *Android* platformi i nisu shvatili da se u fajlu nalazi aplikacija, pretpostavljajući da se u njemu nalazi dokument koji sadrži rezime sa konferencije koja je održana nedavno (kako je rečeno u *e-mail*-u), niti su sumnjali s obzirom da je *e-mail* poslat od strane aktiviste. Onog trenutka kada je aplikacija instalirana i pokrenuta od strane korisnika, koji je želeo da pročita navodni dokument, *malware* je bio u mogućnosti da ukrade kontakte, evidencije poziva, tekstualne poruke i ostale informacije. Ukradeni podaci su potom poslani na udaljeni server. *Kaspersky Labs* su imali prilike da vide slične napade na tibetanske i druge aktiviste i ranije, međutim ovo je bio prvi napad koji je ciljan na mobilne uređaje.

3. jula 2013., kompanija pod imenom *BlueBox Security*, navodi da su pronašli manu u *Android* platformi, koja dozvoljava aplikacijama da budu menjane bez uticaja na njihov digitalni potpis[19]. Kao što smo već napomenuli, postoji mogućnost da više aplikacija dele

isti UID i stoga budu u istom virtuelnom okruženju (*sandbox*). U ovom slučaju, ubrizgani kod biće dodatna aktivnost koja deklarise pristup deljenom sistemskom *sandbox*-u. Sve klase u *Android* aplikacijama prevedene su u jedan *.dex* fajl i svaka klasa ima individualni *hash* unutar *.dex* fajla koji se na kraju potpisuje istovremeno kada i fajl iz aplikacije. *.apk* fajl je sličan *.zip* ili *.jar* fajlu, što znači da se fajlovi mogu dodati ili ukloniti, ali modifikovanjem jednog fajla bi rezultovalo novoj *hash* vrednosti jer tada taj fajl i aplikacija ne mogu biti verifikovani od strane sistema. Međutim, *BlueBox* su otkrili da mogu prevariti proces verifikacije ubrizgavanjem dodatnog *.dex* fajla koji uključuje dodatnu i zlonamernu aktivnost.

Proces *hash* verifikacije je sekvencijalan i ključ ovog procesa je u uklanjanju originalnog *.dex* fajla i njegovom zamenom novom modifikovanim verzijom, a zatim ponovnim dodavanjem originalnog [20]. Verifikator će zatim izračunati *hash* novog *.dex* fajla pre originala i *hash* originala će zameniti prethodno izračunati *hash* lažnog *.dex* fajla. Zlonamerni kod je sada uspešno dodat i potpis aplikacije je netaknut.

Detalji ovog napada dugo su držani u tajnosti kako bi *Google* imao vremena da reši ovaj problem i čim je zakrpa puštena, detalji su predstavljeni na *Black Hat* konferenciji u Las Vegasu 2013. godine.

3.3 Podrška Android platforme

Google pruža administrativni API (*Application Programming Interface*) interfejs koji se može koristiti za implementaciju nekih osnovnih funkcija upravljanja [21]. Ovaj API je predstavljen u *Android* verziji 2.2 i od tada je konstantno unapređivan, iako mu je broj dostupnih mogućnosti i dalje ograničen. Sledeća MDM funkcionalnost je dostupna upotrebom *Device Administration* API:

- **Polisa lozinke**
 - Zahtev za PIN-om ili lozinkom je omogućen
 - Minimalna dužina
 - Minimalni broj cifara, simbola, velika slova
 - Rok važenja
 - Restrikcija istorije
 - Maksimalno vreme podešavanja za zaključavanje
- **Šifrovanje (omogućiti/onemogućiti)**
- **Kontrola kamere (omogućiti/onemogućiti)**

Sposobnost podešavanja napredne politike lozinke je najkorisnija mogućnosti ovog API-ja uporedo sa primenom šifrovanja. Takođe podržava mogućnost kontrole kamere koja može biti primenljiva u nekim okolnostima ali nije od velike bitnosti za BYOD. Ovo je solidan početak u jačanju bezbednosti uređaja, ali i dalje nedostaje nekoliko ključnih opcija, kao što su kontrola aplikacija ili mogućnost konfigurisanja servisa kao što su *e-mail*, VPN, *Wi-Fi* itd.

	<i>Native</i>	<i>EAS</i>	<i>Public</i>	<i>Internal</i>	<i>Motorola</i>	<i>HTC</i>	<i>Samsung</i>	<i>SystemOrSigned</i>
<i>Password Policy</i>	-	X	X	X	X	X	X	X
<i>Application Control</i>	-	-	-	-	-	-	X	X
<i>-Install</i>	-	-	-	-	-	-	X	X
<i>-Uninstall</i>	-	-	-	-	-	-	X	X
<i>-Silent install</i>	-	-	-	-	-	-	X	X
<i>-Silent update</i>	-	-	-	-	-	-	X	X
<i>-Silent uninstall</i>	-	-	-	-	-	-	X	X
<i>-Prevent uninstall</i>	-	-	-	-	-	-	X	X
<i>Disable camera</i>	-	-	X	X	X	X	X	X
<i>Disable Wi-Fi</i>	-	-	X	X	X	X	X	X
<i>Disable NFC</i>	-	-	-	-	-	-	-	X
<i>Lock device</i>	-	-	X	X	X	X	X	X
<i>Wipe device</i>	-	-	X	X	X	X	X	X
<i>Encryption</i>	-	X	X	X	X	X	X	X
<i>Configure VPN</i>	-	-	-	-	X	X	X	X
<i>Configure EAS</i>	-	X	-	X	X	X	X	X
<i>Configure Wi-Fi</i>	-	-	X	X	X	X	X	X
<i>Configure APN</i>	-	-	-	-	-	-	-	X
<i>Configure NTP</i>	-	-	-	-	-	-	-	X
<i>Endpoint control</i>	-	X	X	-	-	-	X	X
<i>Install certificate</i>	-	-	-	-	X	X	X	X
<i>Check battery</i>	-	-	X	X	X	X	X	X
<i>Power mgnt</i>	-	-	-	-	-	-	-	X

Tabela 3.2 – Android matrica funkcionalnosti

Tabela 3.2 prikazuje dostupnu podršku za MDM funkcije gde je korišćen različit API za *Android* platformu. Maternji *Androidframework* manjka podršku za upravljanje uređajem i kako bi nadoknadili, mnogi proizvođači (OEM) su razvili sopstveni API specifičan za njihove uređaje. Time pružaju podršku za naprednije MDM opcije iako su i one prilično ograničene. API koji je obezbeđen od strane kompanija kao što su *HTC* i *Samsung* je ograničen samo na partnere, a partnerstvo mora postojati pre nego što razvojni tim može koristiti njihov API i SDK (*Software Development Kit*) za MDM. *Samsung* obezbeđuje API sa najviše funkcija i ne zavisi od bilo kakvih visoko-rizičnih dozvola (*Signed/SystemOrSigned*). Međutim, ove funkcije su deo programa *Samsung For Enterprise (SAFE)* koji obezbeđuje *Samsung* i koji nije dostupan developerima ukoliko nisu posvećeni partneri *Samsung* kompanije.

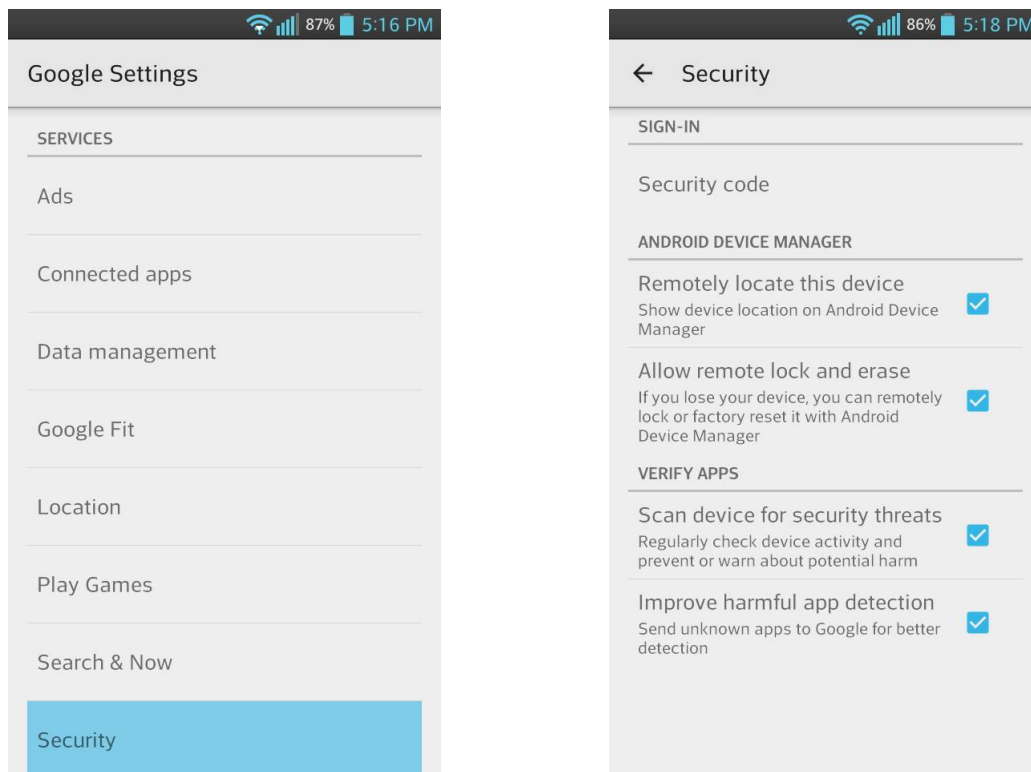
U poređenju, *HTC* i *Motorola* podržavaju slične funkcije u svom API ali se razlikuju u dostupnosti. Motorolin API je dostupan javnosti i može biti korišćen od strane developera, dok je *HTC* API ograničen samo na partnere. Pored funkcija koje obezbeđuje API administracija uređaja, oba proizvođača su u stanju da konfigurišu EAS (*Exchange ActiveSync*) i VPN (*Virtual Private Network*) podešavanja i instaliraju sertifikate tiho. Redovan *Android* API takođe podržava instalaciju sertifikata ali će zahtevati interakciju korisnika kako bi završio instalaciju. Što se tiče ovog istraživanja, ostali proizvođači kao što su *LG* i *Sony* ne pružaju dodatni MDM API i stoga nisu deo ovih rezultata.

Međutim, najmoćnije MDM funkcije mogu biti dostupne na bilo kom uređaju, bez obzira ko je proizvođač, ukoliko su *System* or *Signed* dozvole odobrene aplikaciji. Ove funkcije nisu fabrički ugrađene ali bi im ove dozvole omogućile da budu implementirane ako uzmemo u obzir da pružaju potpunu kontrolu nad sistemom.

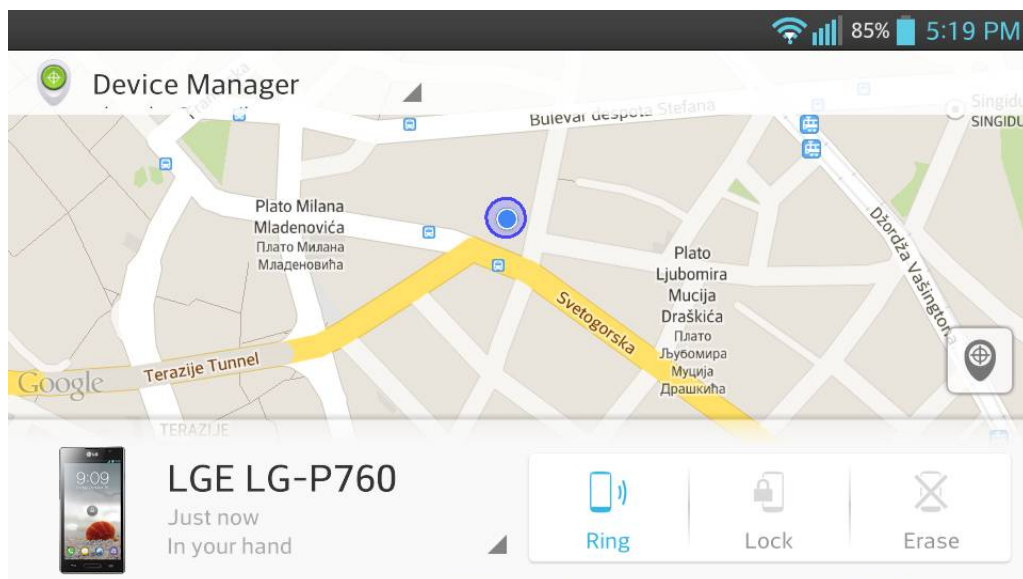
3.4 Android Device Manager

Google je razvio aplikaciju pod nazivom *Android Device Manager* koja omogućava korisnicima da prate i osiguraju svoje uređaje daljinskim putem. U zavisnosti od dozvola koje korisnik pruži ovoj aplikaciji, biće u mogućnosti da daljinskim putem prate njihove uređaje, narediti im da zvone (čak i kad su u tihom režimu rada), menjati im šifru zaključavanja ili čak kompletno obrisati sve podatke i informacije sa svojih uređaja. Novije opcije, kao što su zvonjenje ili slanje SMS poruka izgubljenom uređaju, skorije su dodate, tako da, ukoliko neko pronađe izgubljeni uređaj, korisnik može stupiti u kontakt sa tom osobom [22].

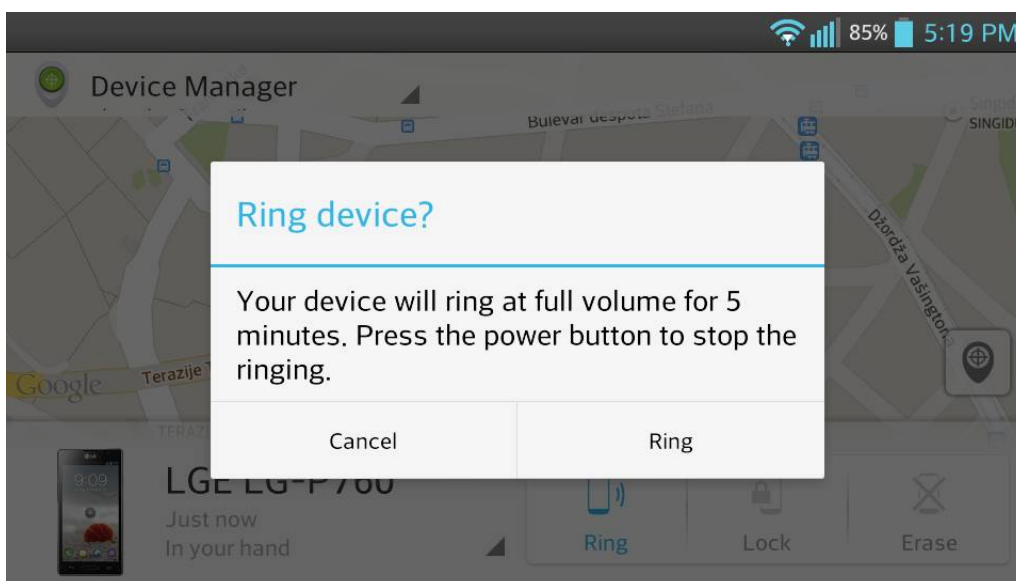
Potrebne su dve stvari pre nego što *Android Device Manager* može biti u mogućnosti da locira uređaj. Potrebno je da uređaj ima omogućenu daljinsku lokaciju (*remote location*) i potrebno je da se omogući pristup lokaciji (*location access*) uređaja što je prikazano na slici 3.2 i bez toga je nemoguće locirati izgubljeni uređaj. *Android Device Manager* takođe funkcioniše i na tabletima, ali ukoliko korisnik ima više korisničkih naloga, samo vlasnik tableta (*owner*) može pokrenuti ovu funkciju ili isključiti je po potrebi.



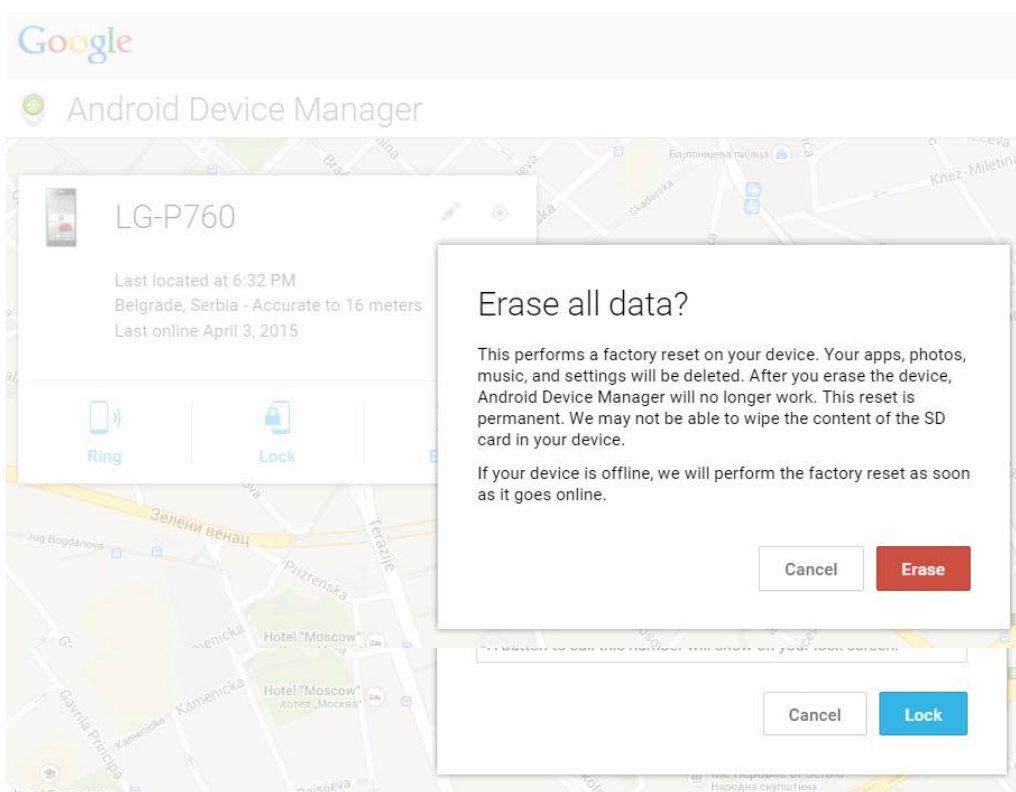
Slika 3.3 – Omogućavanje daljinskih dozvola – LG L9



Slika 3.4 – Android Device Manager korisnički interfejs – LG L9



Slika 3.5 – Opcija zvonjenja telefona – LG L9



Slika 3.6 – Opcija menjanja šifre zaključavanja ekrana – Google Chrome

Slika 3.7 – Opcija fabričkog resetovanja – Google Chrome

3.5 Dodatna rešenja

3.5.1 Google Apps

Google nudi uslugu pod nazivom *Google Apps for Business*. Bazirana je na *cloud* principu kako bi kompanije upravljale svojim podacima unutar *Google* servisa kao što su *Gmail*, *Calendar*, *Drive* itd. [23]. *Google Apps* pruža sigurnost, konstantnu podršku, jako šifrovanje i potvrdu identiteta za korisnike koji plaćaju ove usluge i jedna od najisplativijih tačaka je da kompanije zapravo poseduju svoje sopstvene podatke.

3.5.2 Exchange ActiveSync

Korporacija koja je razvila *Microsoft Exchange* rešenje je u stanju da sprovede politiku dostupnu za *Device Administration API* za *Android*. Ugrađeni *e-mail* klijent za *Android* podržava EAS i može biti upravljani od strane *Exchange* servera daljinski. Razlog je poboljšanje bezbednosti uređaja pre nego što je korisniku odobren pristup elektronskoj pošti, kalendaru ili listi kontakata.

3.5.3 HTCpro MDM

HTC svojim partnerima pruža API koji može da sprovede politiku na nivou preduzeća i bezbednost koja nadmašuje onu koja je uključena u regularnom *Android API*. Izgrađen je na ključnom *Androidframework*-u kako bi proširio svoju MDM funkcionalnost. Međutim, uzimajući u obzir da ovaj API nije dostupan javnosti, dodatne opcije nisu uključene u realizaciji prototipa. Lista MDM funkcija prikazana na tabeli 3.2 dolazi iz kompanije pod nazivom *Airwatch* (*HTCpro* partner) koja tvrdi da podržava ove funkcije sa njihovim *HTC* MDM klijentom [24].

3.5.4 Samsung SAFE

Kompanija *Samsung* nudi poslovni program pod nazivom *SAFE* (*Samsung for Enterprise*)[24]. *SAFE* je sveobuhvatno MDM rešenje za preduzeća ali nije direktno ponuđen developerima već *third-party* MDM proizvođačima. Njegov API nudi više od 300 IT politika [25], uključujući tiho instaliranje i brisanje aplikacija (*silent install*, *uninstall*), mogućnost da se onesposobi snimanje govora, snimanje ekrana (*screen capture*), GPS itd. Ove mogućnosti su redovno dostupne samo u slučaju kada je *firmware* potpis na raspolaganju da obezbedi pristup potpisu *SystemOrSigned* dozvolama.

3.5.5 Samsung KNOX

Samsung KNOX je rešenje na nivou preduzeća, koje nudi efikasan način za koegzistiranje poslovnog i ličnog sadržaja na istom uređaju [26]. *KNOX* je deo *SAFE* programa koji pruža MDM, bezbednost za aplikacije i platforme. Bezbednost platforme je poboljšana upotrebom *Secure Boot*-a koji štiti *Androidframework*, *Linux* jezgro i *boot loader*. To sprečava izvršavanje neovlašćenog OS-a ili softvera prilikom pokretanja uređaja i povezan je sa rešenjem koje se može naći na WP8 (*Windows Phone 8*) uređajima. Bezbednost aplikacija se odnosi na odvajanje ličnog i poslovnog sadržaja. Uređaj je podeljen na različite kontejnere i svaki kontejner se može smatrati zasebnim *Android* okruženjem koji ima sopstvene aplikacije, „vidžete“ (*widgets*), početni ekran itd. Ovi kontejneri su slično izolovani isto kao što su aplikacije izolovane jedna od druge koristeći *sanboxing*. *Samsung KNOX* takođe obezbeđuje podršku za šifrovanje i VPN konfigurisanje.

4 Obezbeđivanje mobilnih uređaja



Slika 4.1 – Ilustracija obezbeđivanja mobilnih uređaja [33]

Kao što smo imali prilike da vidimo u poglavlju 2, postoji nekoliko tipova napada koji ciljaju mobilne uređaje kao i više propusta i ranjivosti koje bi trebalo uzeti u obzir pre BYOD implementacije unutar poslovnog okruženja.

Zajednički princip u raspravi o bezbednosti informacija je CIA trijada [27]: poverljivost, verodostojnost i dostupnost.

- **Poverljivost** – Podaci bi trebalo da se čitaju samo od strane namenjenih i ovlašćenih korisnika.
- **Verodostojnost** – Podaci bi trebalo da se menjaju samo od strane namenjenih i ovlašćenih korisnika.
- **Dostupnost** – Ovlašćeni korisnici bi trebalo uvek da budu u mogućnosti da pristupe podacima za koje im je odobren pristup.

Cilj ovoga, jeste da samo korisnici sa odgovarajućim akreditivima bi trebalo da budu u mogućnosti da čitaju, menjaju i imaju pristup privatnim podacima u bilo kom trenutku.

Ova tri principa sumiraju uslove koje je potrebno ispuniti kako bi se obezbedio prihvatljiv nivo sigurnosti. U ovom poglavlju biće predstavljena najkritičnija rešenja u cilju obezbeđivanja mobilnih uređaja. Svako rešenje potiče od jednog ili više od gore navedenih principa i imaju za cilj da pruže uvid o tome kakvu zaštitu mogu da pruže od napada opisanim u poglavlju 2.

4.1 Zaključavanje ekrana

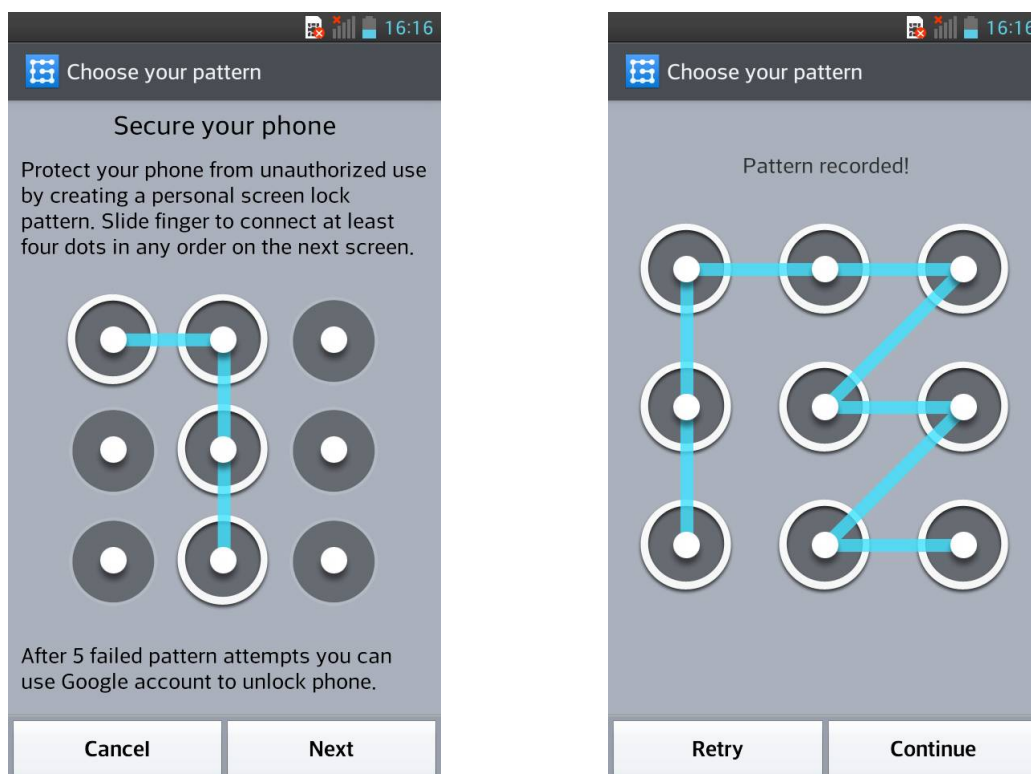
Mogućnost podešavanja zaključavanja ekrana korišćenjem PIN-a ili lozinke su česte funkcije na mobilnim uređajima za povećanje bezbednosti i privatnosti korisnika. Pruža jednostavan mehanizam autentifikacije kako bi se sprečio direktan pristup sadržajima

uređaja od strane napadača. Obično, više vrsta zaključavanja ekrana je dostupno na različitim platformama i uključuju opcije kao što su obrasci ili jednostavno biometrije. Međutim, PIN ili lozinke su najčešće alternative u smislu definisanja izvodljivih polisa.

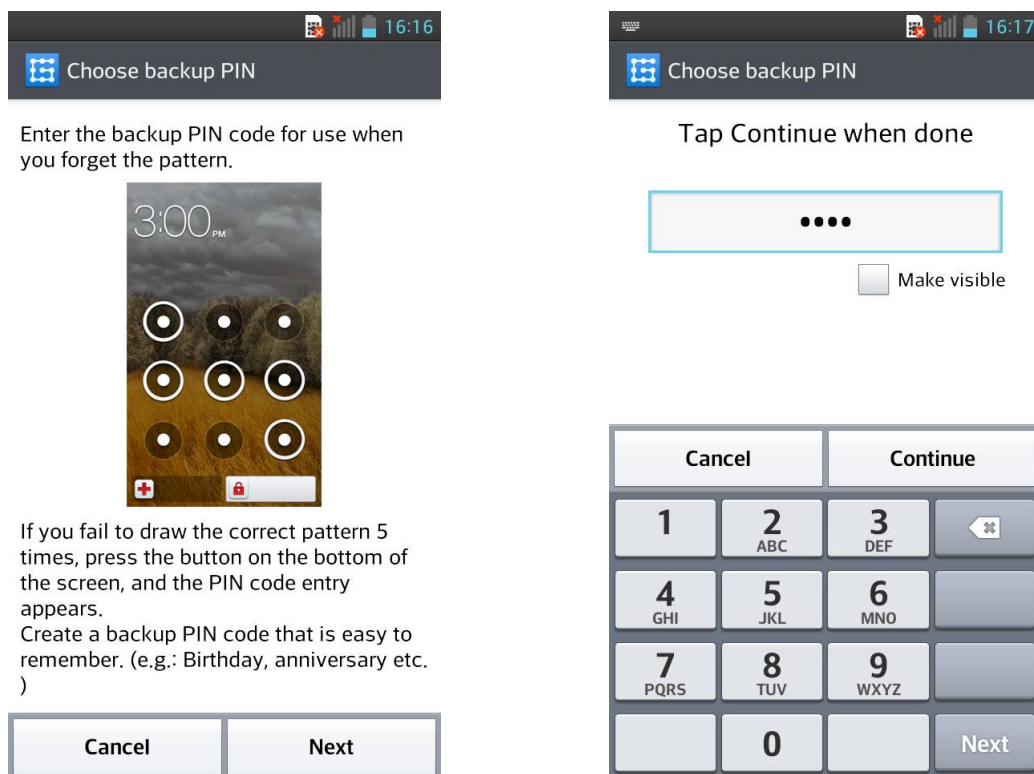
Polisa zaključavanja ekrana obezbeđuje minimalan nivo entropije PIN-a ili lozinke. Entropija je mera jačine lozinke i njenog otpora protiv *brute-force* napada. Stoga, polisa zaključavanja ekrana ne bi trebalo da bude previše jednostavna ili predvidljiva. Pravilna polisa zaključavanja ekrana na mobilnim uređajima bi trebalo da uključuje sledeće:

- **Uslov za zaključavanje ekrana** – Korisnici su dužni da imaju PIN ili lozinku omogućenu na uređaju.
- **Jaka entropija** – Određuje minimalnu dužinu, broj slova, cifara, simbola itd.
- **Neuspeli pokušaji**– U slučaju previše neuspešnih pokušaja autentifikacije, odnosno „logovanja“ uređaju, uređaj se briše.
- **Vreme zaključavanja ekrana** – Vreme neaktivnosti pre nego što se zaključavanje ekrana aktivira.

Ovo će sprečiti neovlašćene korisnike da dobiju direktan pristup aplikacijama i fajlovima, i zabraniti *brute-force* i napade rečnikom.



Slika 4.2 – Podešavanje zaključavanja ekrana – LG L9



Slika 4.3 – Podešavanje PIN-a – LG L9



Slika 4.4 – Neuspelo otključavanje ekrana – LG L9

4.2 Daljinsko zaključavanje i brisanje

Često upotrebljavani uređaji u vlasništvu kompanija, najverovatnije će imati neku vrstu osetljivih podataka koji ne moraju biti u vidu dokumenata ili datoteka, već u vidu akreditiva za elektronsku poštu ili VPN servisa. U oba slučaja, intelektualna svojina kompanija je u opasnosti ukoliko se desi da je uređaj izgubljen ili ukraden. Efikasan način zaštite poverljivosti i integriteta podataka je polisa daljinskoj zaključavanja i brisanja. Ovo omogućava administratoru da daljinskim putem aktivira zaključavanje ekrana ili pokrene brisanje uređaja čime se briše sav sadržaj na uređaju. Funkcija daljinskog zaključavanja će zabraniti direktan pristup uređaju dok će daljinsko brisanje osigurati da podaci kompanije nisu više u opasnosti. Uzimajući u obzir da polisa lozinke obično uključuje vreme zaključavanja ekrana (obično podešeno na nekoliko minuta) i da bi bilo potrebno neko vreme pre nego što se daljinsko zaključavanje izvrši, tada je opcija daljinskog zaključavanja suvišna za implementaciju. Ipak, može biti vrlo korisno promeniti trenutnu lozinku koristeći jaču entropiju, čineći je težom za obavljanje *brute-force* napada. Međutim, trebalo bi napomenuti da su podaci i dalje dostupni na uređaju koji je zaključan, time i dalje pod rizikom. Stoga, daljinsko brisanje je bezbednija opcija.

4.3 Šifrovanje

Šifrovanje podataka je klasična tehnika zaštite digitalnih informacija i koristi se da se osigura poverljivost podataka. „*Mobile Device Security*“ (MDS), pre svega, uključuje dve vrste šifrovanja: šifrovanje uređaja i šifrovanje mreže.

Šifrovanje uređaja se odnosi na šifrovanje podataka u prostoru za skladištenje. Kao što je napomenuto u prethodnom odeljku, čak i ako je aktivirano zaključavanje ekrana na uređaju, i dalje je podložan direktnim napadima. Ovo su napadi koji su direktno usmereni protiv hardvera uređaja u cilju izdvajanja podataka, bilo direktno od RAM memorije ili sa prostora za skladištenje. Šifrovanje uređaja se koristi za zaštitu običnog teksta i sprečava ekstrakciju ovih podataka u slučaju *offline* napada. Ovim se obezbeđuje poverljivost mobilnih uređaja, ali ne i zaštita od direktne krađe poverljivih podataka. Međutim, ukoliko je napadač u mogućnosti da dešifruje podatke, tada postaje beskorisno, ali u zavisnosti od šeme šifrovanja, ili će odložiti ili sprečiti nameru napadača da preuzme konkretne podatke.

Šifrovanje mreže se tiče podataka na mrežnom sloju i pruža zaštitu u tranzitu preko neproverenih mreža (Internet). „*Hypertext Transfer Protocol Secure*“ (HTTPS) i „*Virtual Private Network*“ (VPN) su primeri protokola i servisa koji se mogu koristiti za sprovođenje ove vrste nivoa bezbednosti i da bi se izbeglo prisluškivanje kao i curenje podataka. HTTPS je osigurana verzija HTTP-a (*Hypertext Transfer Protocol*) [28] koji koristi kriptografske funkcije za šifrovanje hедера i *payload*-a HTTP paketa. Takođe se široko koristi za autentifikaciju na strani servera kako bi dokazali identitet servera (ili *web* sajta) predstavljanjem važećeg sertifikata klijentu (korisniku). Tada klijent može da potvrdi svoje akreditive kroz svoj CA (*Certificate Authority*). Konačno proces pregovaranja se izvršava kako bi generisao ključeve potrebne za šifrovanje saobraćaja. Ovaj proces je na „jedan-na-jedan“ osnovi, što znači da se pregovori obavljaju između svakog servera sa kojim korisnik želi da uspostavi vezu. Druga alternativa za sigurnu mrežnu komunikaciju je korišćenje VPN konekcije. VPN funkcioniše na nižem sloju internet protokola u odnosu na HTTPS i boravi na mrežnom sloju (u odnosu na HTTP koji je na sloju aplikacije) što pruža mogućnost zaštite celog IP (*Internet Protocol*)

paketa a ne samo *payload*-a. VPN simulira virtuelni mrežni interfejs koji omogućava korisnicima daljinski pristup resursima i servisima interne mreže. Virtuelni interfejs enkapsulira IP paket unutar drugog IP paketa koji se koristi kao skladište između dve krajnje tačke na nepouzdanjoj mreži, poznat kao VPN tunel. Enkapsulirani paket se na kraju izvlači na VPN *gateway* (npr. kompanijin *firewall*) i tada može omogućiti korišćenje više usluga preko istih mreža bez ikakvih dodatnih ključnih pregovora ili provere identiteta. Ni HTTPS ni VPN ne mogu da obezbede zaštitu podataka koji su već uskladišteni na uređaju, ali će obezbediti siguran kanal koji se može koristiti za prenos podataka.

4.4 Kontrola aplikacija

Karakteristike opisane u odeljcima 4.1, 4.2 i 4.3 su primeri mehanizama zaštite koji se koriste protiv spoljnih pretnji, međutim ne štite od unutrašnjih pretnji kao što su maliciozne aplikacije koje bi mogle biti instalirane iz nehata od strane korisnika i koje eventualno mogu da krađu podatke koristeći se legitimnim metodama. Takve aplikacije mogu biti instalirane bez znanja korisnika koristeći *phishing* elektronskom poštom, socijalnim inženjeringom ili maskirajući se kao legitimna aplikacija. Tržište nudi širok spektar uređaja različitih proizvođača i sa nekoliko operativnih sistema koje možete izabrati. Prilikom dizajniranja rešenja za BYOD, svaki brend i OS treba uzeti u obzir zajedno sa njihovim različitim sposobnostima. Opštu politiku za kontrolu aplikacija je, stoga, teško sprovesti, jer se podrška razlikuje na različitim platformama. Većina proizvođača operativnih sistema ne dozvoljavaju distribuciju aplikacija od treće strane (*third party*) već isključivo od njihovih zvaničnih prodavnica. Većina ovih proizvođača sprovode proces razmatranja koji uključuje test i pregled koda kako bi se izbeglo objavljivanje zlonamernog sadržaja. Proces se razlikuje između različitih proizvođača koji imaju različite principe u distribuciji aplikacija.

Nakon primene revizije i pregleda aplikacija, određuju se takozvane bele ili crne liste. Crna lista podrazumeva listu zabranjenih, dok se bela lista odnosi na listu odobrenih aplikacija. Crnom listom smanjujemo rizik instalacije poznatih malicioznih ili neodgovarajućih aplikacija, dok bela lista nije pogodna za globalnu kontrolu aplikacija niti BYOD zbog velikog obima dostupnih aplikacija za svaku platformu. Uzimajući u obzir da se nove aplikacije konstantno objavljuju, rezultat bi bio u velikom broju sati održavanja i posla od strane administratora.

Ali isto tako, ipak bi trebalo uzeti u obzir da je korisnik i dalje vlasnik svog uređaja i potrebno mu je dozvoliti korišćenje aplikacija po njegovom izboru. Preduzeća bi trebalo da zabrane isključivo uređaje sa poznatim malicioznim aplikacijama instaliranim prilikom prijavljivanja, kao i da pomognu u održavanju i zaštiti uređaja od zlonamernih aplikacija. Stoga, crna lista je bolji izbor, takođe može biti upotpunjena listom potrebnih aplikacija, aplikacija koje preduzeće može da zahteva od korisnika da instalira, npr. VPN klijent.

4.5 Životni ciklus uređaja

Kako bi se osigurala zaštita intelektualne svojine, važno je uzeti u obzir čitav životni ciklus mobilnog uređaja. Većina BYOD i MDM rešenja prvenstveno se fokusiraju na bezbednost inicijalne prijave i aktivnog perioda. Međutim, takođe je bitno uzeti u obzir šta se dešava prilikom uklanjanja uređaja. Uređaj koji se uklanja iz upotrebe firme ili koji se menja drugim uređajem, uglavnom će sadržati bitan sadržaj i o tome treba obratiti pažnju.

Otuda polisa uklanjanja uređaja i njegovog sadržaja je potrebna kako bi se zaštitio integritet podataka.

Nacionalni institut za standarde i tehnologiju NIST (*National Institute of Standards and Technology*) je nedavno objavio opštu dokumentaciju koja sadrži predloge ili smernice, u vezi sa time kako bi trebalo rukovati mobilnim uređajima u okviru velikih IT infrastruktura, kako bi se obezbedio prihvatljiv nivo sigurnosti [29]. Fokus je na rizike koje treba uzeti u obzir prilikom razvijanja odgovarajućih rešenja za upravljanje uređaja i kako održati visok nivo sigurnosti tokom njihovog čitavog životnog ciklusa, od inicijalnog pristupa uređaju do njegovog uklanjanja.

NIST definiše sledeće korake za obezbeđivanje životnog ciklusa mobilnog uređaja:

1. **Inicijacija**
2. **Razvoj**
3. **Implementacija**
4. **Upravljanje i održavanje**
5. **Uklanjanje**



Slika 4.5 – Životni ciklus uređaja

4.5.1 Inicijacija

Prvi korak bi bio identifikacija zahteva i neophodnih funkcija za raspoređivanje mobilnih uređaja unutar organizacije. Lista pripremnih akcija uključuje:

- **Nivo pristupa**
 - Koji resursi bi trebalo da budu dostupni?
 - Koliko je odstupanje između kompanijinih i privatnih (BYOD) uređaja?
- **Polisa**
 - Šta bi trebalo da bude uključeno u ovu polisu?
 - Može li se polisa primeniti na svim uređajima?
 - Da li je u skladu sa drugim polisama kompanije?
 - Koji uređaji bi trebalo da budu dozvoljeni i podržani?

Princip najmanje privilegije bi trebalo uzeti u obzir i organizacije ne bi trebalo da omoguće više pristupa nego što je potrebno za mobilne uređaje. Korisnici koji poseduju visok nivo pristupa bi trebalo, bez obzira, da imaju ograničen pristup resursima prilikom korišćenja mobilnog uređaja, kako bi se smanjili gubici prilikom potencijalnog proboja. Cilj ovog koraka inicijacije je dobijanje opšte bezbednosne polise o tome kako upravljati

mobilnim uređajima. O različitim ograničenjima uređaja je takođe diskutovano. Vrlo je bitno imati znanje o dostupnoj podršci kako bi utvrdili da li je određena vrsta uređaja u stanju da ispuni sve zahteve, ili postoje bolje alternative.

4.5.2 Razvoj

Sledeći korak obuhvata razvoj dizajna. Postoje mnogi faktori koje bi trebalo uzeti u obzir, uključujući različite MDM tehnologije, klijent i server softvere itd. Takođe je relevantno razmotriti neke aspekte sigurnosti kao što su tipovi autentifikacije, algoritmi za šifrovanje, zaštitu integriteta i konfigurisanje zahteva. Planovi za šifrovanje bi trebalo da budu dokazano sigurni i sertifikovani od strane ovlašćenog lica. Takođe je važno koristiti sigurne algoritme kao što su AES (*Advanced Encryption Standard*) ili RSA koji su se pokazali kao sigurni, pogotovu jer se stalno testiraju kako bi se pronašle potencijalne slabosti.

4.5.3 Implementacija

Onog trenutka kada je rešenje dizajnirano, tada bi trebalo da bude implementirano i valjano testirano pre nego što uđe u proizvodnju. Svaki uređaj odobren u odeljku 4.5.1 bi trebalo propisno testirati kako bi se utvrdilo da li ispunjavaju sledeće uslove:

- **Povezivanje** – Korisnik bi trebalo da bude u stanju da uspostavi održivu vezu kako bi pristupio resursima kompanije. Korisnici bi, takođe, trebalo da budu u mogućnosti da pristupe svim resursima za koje su dobili dozvolu i sve van ovog okvira bi trebalo da bude nedostupno.
- **Zaštita** – Obezbediti zaštitu podataka na uređaju u skladu sa specifikacijama dizajna.
- **Autentifikacija** – Mora da radi ispravno i ne može se zaobići.
- **Upravljanje** – Uređajem se može upravljati efikasno i na siguran način.
- **Prijavljivanje** – Ovo rešenje bi trebalo da prijavi sve događaje kako je određeno polisom kompanije i u skladu sa specifikacijama postavljenim u koraku inicijacije.
- **Performanse** – Sve komponente u datom rešenju bi trebalo pravilno da se izvršavaju tokom normalne i maksimalne upotrebe. Čak i srednje uređaja ili opremu bi trebalo proveravati kako bi se izbegao neočekivani prekid, npr. unutar *firewall*-a ili rutera.
- **Sigurnost implementacije** – Bezbednost stvarne realizacije bi trebalo pažljivo pregledati i propisno testirati kako bi se izbeglo iskorišćavanje ranjivosti. *Jailbreak*-ovane uređaje ne bi trebalo dozvoliti i implementacija bi trebalo da otkrije ove uređaje u inicijalnom stanju, ukoliko je moguće.
- **Osnovna podešavanja** – Standardne postavke bi trebalo da ispunjavaju minimalne zahteve sigurnosti za rešenje i uređaje ne bi trebalo vraćati na podešavanja koja se mogu smatrati kao nesigurna.

4.5.4 Upravljanje i održavanje

Ova faza obuhvata uslove za procenu i ažuriranje onog trenutka kada rešenje stupi na snagu. Dostupnost najnovijih „apdejtova“ i „zakrpa“ bi trebalo redovno proveravati i primeniti na svaku komponentu u rešenju. Sposobnost rekonfigurisanja uređaja i menjanje korisničkog pristupa mora biti funkcionalna u slučaju da je korisnička polisa promenjena ili u

slučaju dodavanja dodatnih bezbednosnih funkcija. Sistem bi trebalo pratiti u cilju otkrivanja i snimanja anomalija kao što su narušavanje polisa ili zlonamerna ponašanja.

Od ključne je važnosti sinhronizacija satova na svim komponentama kako bi se izbegla neusklađenost između različitih sistema. Stoga, trebalo bi sve komponente sinhronizovati sa zajedničkim vremenskim izvorom, npr. na NTP (*Network Time Protocol*) server.

Minimiziranje ljudske greške je takođe deo ovog koraka, a postiže se edukacijom zaposlenih definisanim polisama i podizanjem svesti o aktuelnim pretnjama kao što su sumnjive elektronske pošte u kojoj se traže lozinke ili informacije o kreditnim karticama.

4.5.5 Uklanjanje

Poslednji korak ovog procesa je da se osigura bezbedan sadržaj prilikom uklanjanja uređaja. Niti jedan podatak ne bi trebalo da bude u opasnosti od kompromitovanja nakon odbacivanja uređaja kako bi se osigurao integritet poverljivih informacija kompanije.

U nekim slučajevima, ovaj zadatak će tražiti drastičnije mere od vraćanja fabričkih podešavanja na uređaju. Uklonjiva memorijska kartica i dalje može biti prisutna u uređaju i ne mora biti pogođena brisanjem uređaja. Podaci preduzeća, takođe mogu biti ostavljeni na internoj memoriji i organizacije koje zahtevaju sveobuhvatniju bezbednosnu politiku (npr. vlada), mogu zahtevati polisu koja podrazumeva potpuno uništenje uređaja u cilju održavanja poverljivosti i integriteta intelektualne svojine.

4.6 Sumiranje

Da rezimiramo, sledeće preporuke bi trebalo uzeti u obzir pre razvoja i primene BYOD rešenja:

- **Zahtevi zaključavanja ekrana**

Zaključavanje ekrana pruža jednostavnu zaštitu koja će sprečiti napade koji zahtevaju direktan pristup uređaju i biće prva prepreka za napadača na ukradenom ili izgubljenom uređaju.

- **Funkcionalnost daljinskog brisanja**

Podrška za daljinsko brisanje pruža mogućnost brisanja podataka uređaja koji su izgubljeni ili ukradeni. Mogućnost daljinskog zaključavanja, takođe se može koristiti, ali se može smatrati suvišnim ukoliko je primenjeno zaključavanje ekrana sa podešenim maksimalnim vremenom u stanju mirovanja (*maximum idle time*).

- **Šifrovanje uređaja i mreže**

Šifrovanje je efikasan način u cilju smanjivanja posledica curenja podataka, *offline* napada i *snoopin*-ga. Ukoliko se podaci izvuku iz šifrovanog skladišta, tada će ti podaci biti bezvredni ukoliko se ne dešifruju. Dokle god su šifarski ključevi sigurni i njihova dužina bitova dovoljna, dešifrovanje će biti veoma težak zadatak. Međutim, u dobroj praksi je da se ne veruje u potpunosti šifrovanju, već dodatno imati na raspolaganju mogućnost daljinskog brisanja.

- **Kontrola aplikacija**

Kontrola aplikacija može se koristiti da praćenje instalacija ili prisustva bilo kakvih poznatih malicioznih aplikacija pa stoga može smanjiti rizik od upotrebe ugroženih uređaja, ili otkrivanja potencijalnih pretnji u realnom vremenu.

- **Životni ciklus uređaja i uklanjanje njegovog sadržaja**

Bilo bi mudro razmotriti sve aspekte životnog ciklusa uređaja prilikom definisanja politike ili razvoja aplikacija klijenata za BYOD. Ukoliko procenimo ceo životni ciklus, tada će biti lakše pronaći moguće ranjivosti i time ograničiti prostor za napad.

4.7 Predlozi i saveti u praksi

Korisnici *Android* platforme, za razliku od korisnika *iOS* ili *Windows Phone*, zbog otvorenosti sistema, moraju biti nešto oprezniji prilikom preuzimanja aplikacija za svoje uređaje. Otvoreni sistem poput Androida ima svoje prednosti i mane. S jedne strane, iskusni korisnici mogu ga prilagoditi svojim potrebama, ali sa druge strane, korisnici moraju biti oprezniji i svesniji bezbednosnih pretnji [30].

Mobilni telefon je već odavno postao neophodan za održavanje kontakta sa drugim osobama i ne služi samo kao telefon. Noviji modeli imaju odlične kamere, muzičke plejere, diktafone, mogućnost surfovanja internetom, slanja elektronske pošte itd. stoga svaki korisnik sa svojim telefonom nosi i deo svoje privatnosti i trebalo bi ga zaštititi od radoznalih i pogotovu zlonamernih osoba.

Svakako telefon treba štititi i od fizičkog oštećenja i od krađe, ali je isto tako važno zaštititi informacije koje se čuvaju u memoriji: SMS, MMS. *E-mail*, mrežne usluge za prenos podataka, kontakte, fotografije, video snimke itd. Čak i kada korisnik samo prima i prihvata pozive i SMS poruke, i tada bi trebalo telefon zaštititi [30].

4.7.1 Zaštita od fizičkog oštećenja

Kao jedna od mera zaštite potrebno je uređaj (pogotovu telefon i tablet) nositi u specijalnoj torbici, futrolji ili silikonskoj navlaci predviđenoj za tu svrhu. Na ovaj način uređaj se čuva od manjih oštećenja, npr. ogrebotina, guljenja. Na našem tržištu se može naći veliki broj modela za različite brendove, od kvalitetnijih do jednostavnijih ali i jeftinijih, drugim rečima za svačiji džep.

U nekim slučajevima potrebno je zaštititi uređaj i od nas samih. Mnogim korisnicima, zbog male nepažnje, dešava se da telefon padne na tvrđu podlogu, ili upadne u vodu prilikom čega se može trajno oštetiti. Ovo se posebno odnosi na slučajeve kada se telefon, na kome je uključena vibracija, ostavi na ivici stola, ili bilo koje glatke površine, jer ukoliko duže zvoni uz vibraciju, lako može „odšetati“ sa stola i pasti na pod.

Koliko god korisnici uređaja voleli svoje najmlađe, nikako im ne bi trebalo davati svoj mobilni telefon, tablet, netbuk ili drugi mobilni uređaj. Deca vrlo lako, a nenamerno, mogu oštetiti uređaj ili, u najgoroj situaciji, obrisati vrlo bitne informacije koje korisnici čuvaju na mobilnom telefonu.

4.7.2 Zaštita od krađe uređaja

Prva mera, ili savet, bilo bi zapisivanje IMEI broja. Ovaj broj se obično nalazi odmah ispod baterije, u nekom slučaju i na poleđini uređaja, odnosno na poklopcu, a ima ga i u garantnim papirima, kupoprodajnim ugovorima itd. Postoji više načina kako možemo saznati IMEI broj na vlastitom uređaju, a jedan od njih je ukucavanje koda *#06# prilikom čega se ispisuje IMEI na telefonu. Prilikom prijave krađe policiji ili mobilnom operateru prvo što bi se tražilo je upravo ovaj broj na osnovu koga mobilni operater može da blokira korisnikov telefon tako da niko ne bude u mogućnosti da ga upotrebljava sve dok se telefon ne pronađe. U tom slučaju ovaj broj će biti potreban i za otključavanje telefona.

Kao jednu od glavnih preventiva, korisnik nikada ne bi trebalo da čuva lozinke i PIN u telefonu, već je potrebno da se potruži da ih zapamti, ili sačuva zapisane negde van uređaja. Stalno kucanje raznih lozinki, PIN koda i sličnog, prosečnom korisniku može biti ponekad naporno. Nije u svakom slučaju neophodno koristiti apsolutno svaku zaštitu i na prosečnim korisnicima je da procene koja zaštita im je potrebna kako bi se dovoljno zaštitili.

4.7.3 Zaštita informacija

Posle svake upotrebe mobilnog uređaja, bilo bi poželjno ručno zaključavanje displeja. Svaki model se različito zaključava, ili u lakšem slučaju, postoji mogućnost automatske zaštite tastature na uređajima sa ekranom na dodir (mobilni telefoni, tableti). Ovo je veoma važno, jer prilikom nošenja, konkretno, telefona u džepu ili torbi, slučajnim pritiskom korisnik može pozvati poslednji pozivan broj, pogotovu ukoliko je prethodno uključio opciju brzog pozivanja (poziv pritiskom jednog odabranog tastera). Pored toga, potrebno je odrediti vreme za koje će se uređaj automatski zaključati. Ovo vreme unosi korisnik uređaja i ono može biti od nekoliko sekundi do nekoliko minuta.

Potrebno je koristiti mogućnost zaštite uređaja lozinkom. Ova opcija se nalazi u podešavanjima svakog uređaja, i platforme uopšte, i slično je kod većine uređaja. Istom lozinkom korisnik može sasvim onemogućiti neželjeno korišćenje uređaja, dok u nekim slučajevima, lozinkom se mogu štititi samo memorija, multimedija itd.

Potrebno je omogućiti uslugu zahteva za PIN šifrom (lični identifikacioni kod). Ukoliko korisnik ostavi isključen uređaj, svaki put posle uključivanja, uređaj će tražiti da korisnik ukuca PIN kod. Ukoliko se PIN više puta za redom pogrešno upiše, kartica se blokira. U tom slučaju, kako bi odblokirali karticu, potrebno je uneti PUK šifra (lični deblokirajući kod). Ukoliko se više puta unese i pogrešan PUK kod, kartica će biti bespovratno blokirana.

Ukoliko korisnik koristi govornu poštu, takođe bi bilo poželjno omogućavanje lozinke. Ovim će korisnik sprečiti da njegova pošta bude preslušana od strane neautorizovanog lica.

Bluetooth i Wi-Fi konekciju, poželjno je isključivati nakon korišćenja, kada više nemamo potrebu za povezivanjem uređaja na mrežu ili uparivanjem sa drugim uređajem. Na ovo bi trebalo obratiti pažnju, pogotovu ako koristimo uređaj za Internet kupovinu ili *online banking*. Moguće su zloupotrebe, a istovremeno se smanjuje potrošnja baterije prenosnog uređaja.

Korisnik bi trebalo da kopira sadržaj mobilnog uređaja kao što je imenik, multimedija, dokumenti, bitne poruke ili elektronska pošta i trebalo bi voditi evidenciju ažuriranja ovog postupka, sa vremena na vreme u zavisnosti od toga koliko često pravi izmene, brisanje ili unos novih podataka.

Prilikom instaliranja raznih aplikacija, potrebno je voditi računa o tome da su od pouzdanih i proverenih izvora zbog opasnosti od virusa, trojanaca itd. Napisano je pravilo da većina aplikacija koje su lepo upakovane, blistave, sa primamljivim grafičkim interfejsom a pritom besplatne, previše dobre da bi bile istinite i uglavnom će sa sobom povući neku vrstu *malware*-a.

5 Zaključak

Ovim radom smo obuhvatili više aspekata MDS i MDM koji se odnose na BYOD. Primetili smo evoluciju pretnji za mobilne uređaje koje postaju sve upornije i naprednije. Ove pretnje su, prethodno, bile fokusirane na personalne računare, međutim sada takođe ciljaju i mobilne uređaje. Ovaj trend je u porastu, naročito zbog dramatičnog porasta upotrebe mobilnih uređaja, kako u poslovne, tako i u privatne svrhe. Mapiranjem pretnji koje smo otkrili, stekli smo razumevanje rizika koje one stvaraju i uvid o tome koje zahteve bi trebalo staviti na potencijalna rešenja. Za BYOD rešenje, utvrđeno je da su potrebne određene polise, uglavnom povezane upotrebom PIN-a ili lozinke i šifrovanjem uređaja, kao i da se može poboljšati korišćenjem klijentskih aplikacija, pogotovu kada pričamo o Android platformi. Međutim, isto tako je neophodno obezbediti mogućnost daljinskog brisanja u cilju zaštite poverljivosti podataka kompanija prilikom gubljenja ili krađe uređaja. Takođe, kontrola aplikacija je strogo preporučljiva, ali može imati osetljivi ishod zbog mogućeg kršenja privatnosti korisnika.

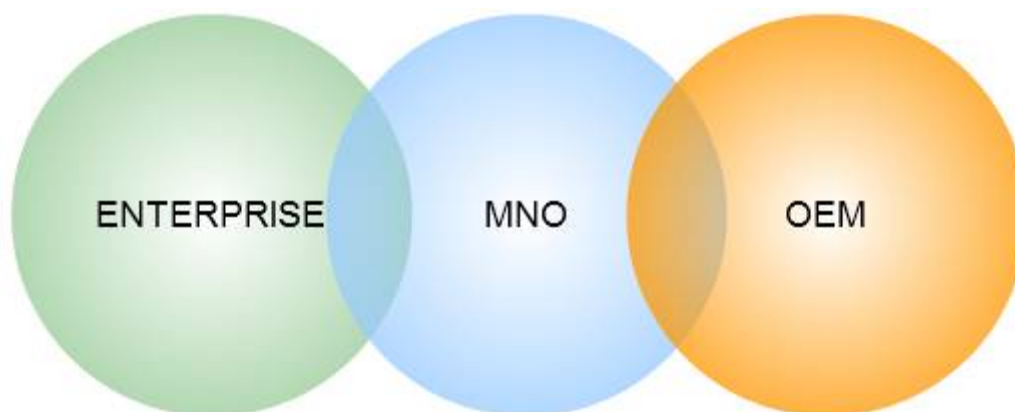
5.1 Sumarni ciljevi rada

Uprkos kontroverzi, ovi predlozi će formirati adekvatnu zaštitu privatnih uređaja i obezbediti pristojan nivo sigurnosti za ograničenu upotrebu u poslovnom okruženju. Proširiće bezbednosne funkcije kako bi se osigurala poverljivost i verodostojnost podataka kako u prostoru za skladištenje tako i u tranzitu, omogućiti daljinsko upravljanje (npr. daljinsko brisanje) i zabraniti direktan pristup od strane neovlašćenih korisnika i zaštititi od malicioznih aplikacija. Pokazali smo da je Android najugroženija platforma od strane zlonamernih aplikacija. Glavni razlog je uglavnom zbog otvorenosti platforme, npr. korisnici imaju mogućnost korišćenja alternativnih kanala distribucije aplikacija. Što se tiče *iOS* i *Windows Phone* platformi, kod ovih uređaja je jedino moguće korišćenje aplikacija koje koriste zvaničnu prijavu prodavnice ili kroz posebne programe preduzeća. Podrška za MDM razlikuje se u zavisnosti od proizvođača. *iOS* i *Windows Phone* uređaji su pokazali da imaju slične kvalifikacije kada su u pitanju bazične funkcije. Dele istu filozofiju restrikcija u interakciji sa sistemskim resursima i mogućnost interakcije developera, sa ovim servisima, je ograničena.

Priroda Androida, u smislu otvorenog koda, se pokazala fleksibilnijom u odnosu na konkurente. *Android* je korišćen od strane višestrukih OEM-a (*Original Equipment Manufacturer*), odnosno proizvođača, od kojih svaki ima svoj spisak funkcionalnosti koje mogu da se realizuju koristeći svoj API. Ustanovili smo da su ugrađene MDM funkcije na Androidu ograničene. API od strane administratora uređaja, dostupni u Android okruženju, pružaju pregršt mogućnosti, uglavnom onih koji su neophodni za osnovni nivo bezbednosti. Kako bi obezbedili šire mogućnosti klijentskim aplikacijama, potrebno je imati ili pristup dozvolama visokog nivoa ili pristup za API od strane proizvođača. *Jailbreak*-ovanje je još jedna mogućnost, ali je utvrđeno da predstavlja bezbednosni rizik koji može dovesti do eskalacije privilegija.

5.2 Predlog za budući rad – Operater mobilne mreže MNO

Dalji rad na temu bio bi scenario gde MNO (*Mobile Network Operator*) obezbeđuje BYOD kao uslugu i da se istraže sve moguće prednosti prilikom omogućavanja operatoru da pruži usluge umesto MDM dobavljača. Slika 5.1 pokazuje Venov dijagram koji opisuje različite vrste MDM rešenja. Ovi krugovi predstavljaju skupove funkcionalnosti koje se odnose na ono što određeni dobavljač može da ponudi svojim klijentima. Na primer, operateri mobilne mreže su u stanju da odrede podešavanja za APN (*Access Point Name*), koja su potrebna za pristup mreži. OEM ima najveći uticaj na njihove uređaje i tradicionalni MDM dobavljači mogu razviti aplikacije koje mogu da upravljaju njima koristeći se alatima koje pružaju proizvođači. Ovo često zahteva neku vrstu partnerstva između proizvođača i dobavljača u cilju dobijanja pristupa aplikacija dobavljaču funkcionalnosti višeg rizika. Međutim šta je sa MNO?



Slika 5.1 – Tipovi MDM provajdera

Poznato je da MNO sarađuju sa više proizvođača kako bi spojili OEM proizvode (pametne telefone itd.) zajedno sa mobilnim pretplatnicima, a takođe je uobičajeno za aplikacije koje se dobavljaju od strane operatora, da se unapred instaliraju na određenim uređajima. Postoji mogućnost za mobilne operatere da kombinuju njihov pristup OEM-u i MDM funkcijama od strane preduzeća kako bi ponudili klijentu aplikacije koje obuhvataju dodatne funkcije. Kao što je prikazano u poglavlju 3, aplikacija može dobiti pristup naprednijim funkcijama ukoliko ima pravo da koristi više dozvola visokog rizika (*signature* ili *systemOrSigned*). Postoji mogućnost mobilnog operatera za dobijanjem ovog nivoa pristupa ukoliko je dostupno partnerstvo sa jednim ili više OEM-a. Takvo partnerstvo može omogućiti MNO da razviju i obezbede svoju BYOD klijent aplikaciju koja može biti, ili unapred instalirana, ili se može preuzeti sa *Google Play* marketa od strane krajnjih korisnika. U ovom scenariju, MNO će dostaviti potrebnu opremu za prijavu uređaja, GCM, klijentskog softvera i ostalih usluga koje mogu biti potrebne preduzeću. Time bi se eliminisali troškovi za podršku i održavanje, koji su inače potrebni za kućnu upotrebu. Ova usluga bi lako mogla da se doda na korisnikov već postojeći mobilni paket preko datog portala. Time klijenti neće biti u obavezi da se vežu za samostalan MDM od strane dobavljača, pošto bi već bio obuhvaćen u paket od strane MNO.

Dodatni pristup zaštiti mobilnih uređaja bi bio da se istraže mogućnosti SIM kartice za BYOD rešenje, kako se može koristiti za bezbedno skladištenje informacija vezanih za MDM i njeno korišćenje sa BYOD. SIM kartica generalno veoma sigurna i pristup njenom sadržaju je vrlo ograničen, što je čini pogodnim kandidatom za čuvanje osetljivih podataka. Ukoliko se tasteri i podešavanja mogu čuvati na SIM kartici umesto na uređaju, tada se može pristupiti lokalno i izbeći obiman proces prijavljivanja putem Interneta.

6 Literatura

- [1] „Faced with escalating mobile malware, NIST publishes mobile security guidelines,” InfoSecurity-Magazine, [Na mreži]. Available: <http://www.infosecurity-magazine.com/news/faced-with-escalating-mobile-malware-nist/>.
- [2] „Threat Report 2013,” SOPHOS Ltd., [Na mreži]. Available: <http://www.sophos.com/en-us/medialibrary/PDFs/other/sophossecuritythreatreport2013.pdf>.
- [3] „Advanced Persistent Threats: Higher Education Security,” Dell SecureWorks, [Na mreži]. Available: http://www.secureworks.com/resources/articles/featured_articles/20120709-hcr/.
- [4] K. Baumgartner, C. Ruiu / D. Maslennikov, „Android Trojan Found in Targeted Attack,” SECURELIST, [Na mreži]. Available: <http://securelist.com/blog/incidents/35552/android-trojan-found-in-targeted-attack-58/>.
- [5] M. McDowell, „Avoiding Social Engineering and Phishing Attacks,” US CERT, [Na mreži]. Available: <https://www.us-cert.gov/ncas/tips/ST04-014>.
- [6] K. D. Mitnick / W. L. Simon, *The Art of Deception: Controlling the Human*, Wiley Publishing Inc., 2002.
- [7] „Phishing Fraud: How to Avoid,” U.S. Securities and Exchange Commission, [Na mreži]. Available: <http://www.sec.gov/investor/pubs/phishing.htm>.
- [8] „OWASP Top 10 Project,” Open Web Application Security Project (OWASP), [Na mreži]. Available: https://www.owasp.org/index.php/Category:OWASP_Top_Ten_Project.
- [9] „Android Security Overview,” Google Inc, [Na mreži]. Available: <http://source.android.com/devices/tech/security/index.html>.
- [10] „Industry Leaders Announce Open Platform for Mobile Devices,” O. H. Alliance, [Na mreži]. Available: http://www.openhandsetalliance.com/press_110507.html.
- [11] Wei-Meng-Lee, „Osnove Android programiranja,” u *Android 4 Razvoj aplikacija*, Wiley Publishing Inc., 2012.
- [12] W. Enck, D. Ocateau, P. McDaniel / S. Chaudhuri, „A Study of Android Application Security,” [Na mreži]. Available: <http://www.enck.org/pubs/enck-sec11.pdf>.
- [13] „Android boot process from power on,” Xdin Android team, [Na mreži]. Available: <http://www.androidenea.com/2009/06/android-boot-process-from-power-on.html>.
- [14] „Google Play hits 25 billion downloads,” Google Inc., [Na mreži]. Available: <http://officialandroid.blogspot.se/2012/09/google-play-hits-25-billion-downloads.html>.
- [15] „Juniper Networks Finds Mobile Threats Continue Rampant Growth as Attackers

- Become More Entrepreneurial," Juniper Networks Inc., [Na mreži]. Available: <http://investor.juniper.net/investor-relations/press-releases/press-release-details/2013/Juniper-Networks-Finds-Mobile-Threats-Continue-Rampant-Growth-as-Attackers-Become-More-Entrepreneurial/default.aspx>.
- [16] H. Lockheimer, „Android and Security," [Na mreži]. Available: <http://googlemobile.blogspot.se/2012/02/android-and-security.html>.
- [17] J. Oberheide, „Dissecting the Android Bouncer," [Na mreži]. Available: <https://jon.oberheide.org/blog/2012/06/21/dissecting-the-android-bouncer/>.
- [18] O. Hou, „A Look at Google Bouncer," Trend Labs, [Na mreži]. Available: <http://blog.trendmicro.com/trendlabs-security-intelligence/a-look-at-google-boun>.
- [19] J. Forristal, „Uncovering Android Master Key That Makes 99% of Devices Vulnerable," BlueBox Security, [Na mreži]. Available: <https://bluebox.com/technical/uncovering-android-master-key-that-makes-99-of-devices-vulnerable/>.
- [20] J. Forristal, „Android: One Root to Own Them All," [Na mreži]. Available: https://bluebox.com/wp-content/uploads/2013/08/Forristal_Blackhat-US2013__final.pdf.
- [21] „Device Administration," Google Inc., [Na mreži]. Available: <http://developer.android.com/guide/topics/admin/device-admin.html>.
- [22] „Android Device Manager," Android Central, [Na mreži]. Available: <http://www.androidcentral.com/app/android-device-manager>.
- [23] „Google Apps for Business," Google Inc., [Na mreži]. Available: <https://www.google.se/intx/en/work/apps/business/>.
- [24] „HTC Device Management," Airwatch, [Na mreži]. Available: <http://www.air-watch.com/solutions/android/htc/>.
- [25] „Samsung SAFE," Samsung, [Na mreži]. Available: <http://www.samsung.com/us/business/samsung-for-enterprise/>.
- [26] L. Samsung Electronics Co., „White Paper : An Overview of Samsung KNOX," [Na mreži]. Available: http://www.samsung.com/global/business/business-images/resource/white-paper/2013/06/Samsung_KNOX_whitepaper_June-0.pdf.
- [27] W. Stallings / L. Brown, Computer Security: Principles and Practice, Pearson Education Inc, 2008.
- [28] R. Fielding, „Hypertext Transfer Protocol – HTTP/1.1. RFC 2616," June 1999. [Na mreži]. Available: <http://www.ietf.org/rfc/rfc2616.txt>.
- [29] N. I. o. S. a. Technology, „Guidelines for Managing and Securing Mobile Devices in the Enterprise," [Na mreži]. Available: http://csrc.nist.gov/publications/drafts/800-124r1/draft_sp800-124-rev1.pdf.
- [30] G. Hogben / M. Dekker, „Smartphones: Information security risks, opportunities and recommendations for users," [Na mreži]. Available:

<https://www.enisa.europa.eu/activities/identity-and-trust/risks-and-data-breaches/smartphones-information-security-risks-opportunities-and-recommendations-for-users>.

[31] „APT1: Exposing One of China’s Cyber Espionage Units,” Mandiant Corporation, [Na mreži]. Available: <http://intelreport.mandiant.com/>.

[32] „BYOD Security Concerns,” [Na mreži]. Available: <http://www.carat.uk.com/byod-vs-cyod-whats-better-business/>.

[33] „How to Write a Secure BYOD Policy,” [Na mreži]. Available: <http://www.trackvia.com/blog/technology/how-to-write-a-secure-byod-policy>.