Povečanje varnosti mobilne aplikacije v javnem potniškem prometu

Marko Avberšek [1], Katja Podrzavnik [1], Amor Chowdhury [1,2]

[1] Margento R&D d.o.o., Turnerjeva ulica 17, 2000 Maribor, Slovenija
[2] Univerza v Mariboru, Fakulteta za elektrotehniko, računalništvo in informatiko, Smetanova 17, 2000 Maribor
E-pošta: marko.avbersek@margento.com

Safety increase of the mobile application for the public passenger transport

Security is one of the most important topics in today's development of mobile applications that manage sensitive personal data and financial instruments. Application security must be multi-layered if it is to be successful. When designing the security of the entire system, the mobile application is one of the most vulnerable elements, therefore a high-quality integrated security concept is required from the application's design itself on the phone, to the transfer of data between the application and the backend system, and also the data communication to the terminal equipment in case the applications support it.

1 Uvod

Varnost je ena najpomembnejših tem v današnjem razvoju mobilnih aplikacij, ki upravljajo z občutljivimi osebnimi podatki ter finančnimi instrumenti. Varnost aplikacij mora biti večplastna, če želimo da je uspešna. Pri načrtovanju varnosti celotnega sistema je mobilna aplikacija eden bolj ranljivih elementov, zato je potrebna kvalitetna zasnova celovite varnosti od same zasnove aplikacije na telefonu, do prenosa podatkov med aplikacijo in zalednim sistemom in tudi pošiljanje podatkov do terminalske opreme v primeru, da aplikacije to podpirajo.

Poleg ustaljenega medija uporabnikov, brezstične kartice, se je s konstantnim razvojem aplikacij za mobilne naprave, ki so uporabnikom v pomoč na vsakem koraku, pridružila tudi mobilna aplikacija Urbana za mobilne naprave z iOS in Android operacijskim sistemom. Mobilna aplikacija, ki je po svoji osnovni namenskosti identična brezstični kartici ponuja uporabnikom še vrsto različnih, dodatnih servisov, kot npr. pregled nad voznimi redi, načrtovanje poti, vpogled v sheme prevoznikov, polnjenje mobilne kartice - aplikacije z dobroimetjem, plačevanje parkirnine na javnih parkiriščih, pregled izposoje koles, zasedenosti parkirnih mest v garažnih hišah itd [5].

Sistem Enotne Mestne kartice (EMK) Urbana omogoča izvajanje elektronskih transakcij, kot je plačevanje produktov z elektronsko denarnico ali shranjevanje podatkov o kupljenih produktih in ustrezno preverjanje uporabe teh produktov - validiranje. Celoten sistem EMK je zasnovan na podlagi naslednjih zahtev: centraliziran nadzor nad delovanjem sistema, centraliziran nadzor nad izvedenimi transakcijami, varen prenos podatkov (enkripcija), avtomatsko ugotavljanje nepravilnosti v delovanju sistema ali zlorab, delovanje v različnih načinih prenosa podatkov, kot sta brezžični način prenosa preko sistema GPRS, ali žični IP način ter robustno mobilno delovanje v okoljih z nestabilnimi podatkovnimi povezavami (npr. GPRS).

Namen članka je predstavitev vpeljave mobilne aplikacije v obstoječ ekosistem s poudarkom na ohranjanju integritete sistema in sistemske varnosti. Za boljše razumevanje rešitve in lažji pregled je v drugem poglavju podana predstavitev sistema EMK Urbana in specifičnega transakcijskega delovanja.

V tretjem poglavju sta na kratko predstavljeni rešitvi mobilnih aplikacij Urbana za operacijska sistema iOS in Android. Jedro članka predstavlja četrto poglavje, kjer so podrobneje prikazani ukrepi in mehanizmi za zaščito mobilne aplikacije Urbana ter varnostni vidiki razvoja mobilnih aplikacij in metode za preprečevanje zlorab v transakcijskih sistemih. Zaključna razmišljanja in ugotovitve so strnjena v zaključku.

2 EMK sistem Urbana

Celotni sistem EMK je zasnovan tako, da se EMK transakcije izvajajo sproti na terminalih – generirajo se z brez-kontaktnimi karticami ali z mobilnimi telefoni. Terminali določen čas hranijo podatke o vseh opravljenih transakcijah, nato te podatke v paketu pošljejo na centralni oz. zaledni del sistema EMK, kjer se izvede procesiranje transakcij.

V sistemu EMK obstaja več tipov terminalov [2] in prav tako obstaja več tipov EMK transakcij, kot na primer: nakup vozovnice, polnjenje denarnice, odvzem zneska, aktivacija vozovnice, validacija vozovnice, plačilo parkirišča, mobilno polnjenje denarnice, mobilna vozovnica ipd. Najbolj splošno pa lahko razdelimo transakcije v dva tipa: online in offline transakcije [2, 4].

Online transakcije so tiste, kjer se preverjanje izvaja na strani procesnega centra sproti oz. sočasno z izvajanjem transakcije, praviloma gre tu za transakcije, izvedene z mobilnim telefonom. Offline transakcije pa so transakcije, kjer v trenutku, ko se transakcija zgodi, ni direktne povezave s procesnim centrom in se kompletno preverjanje, ki je predpogoj za uspešno izvedbo transakcije, zgodi na relaciji kartica – terminal. Šele naknadno, ko je transakcija že izvedena, se podatki o

transakciji pošljejo v procesni center, za dokončno procesiranje.
Zaradi offline načina delovanja lahko prihajajo transakcije, ki so bile izvedene s posamezno kartico na center v nepravem vrstnem redu glede na čas izvedbe. Časovni potek izvedbe EMK transakcij in vrstni red prihoda EMK transakcij v bazo nista sinhrona. Zakasnitev, s katero transakcije prihajajo v center je v veliki večini primerov minimalna in znaša maksimalno nekaj sekund do minute [4]. Lahko pa se v določenih primerih zgodi, da transakcije zamujajo bistveno več, lahko tudi nekaj ur ali celo nekaj dni. Takšne ekstremne zakasnitve so redke, vendar se dogajajo. Najpogostejši razlogi za njihov nastanek so okvara terminala (lahko tudi samo na GPRS ali antenskem sklopu), neaktiven terminal (npr. avtobus na servisu) ali poškodbe napeljave ali GPRS antene v avtobusu (ko je onemogočena komunikacija s centrom).
Pri izvajanju EMK transakcije na terminalu lahko pride do prekinitve komunikacije med kartico in terminalom. V tem primeru terminal opozori uporabnika naj ponovno prisloni kartico. Če uporabnik upošteva navodila in kartico ponovno prisloni k terminalu, terminal preveri in dokonča nepreverjeno transakcijo, kar pomeni, da se na kartico zapišejo vsi potrebni podatki. Ker je zaključevanje nepreverjenih transakcij vezano na prejem naslednje transakcije narejene s to kartico, se lahko pri zaključevanju teh transakcij pojavljajo časovni zamiki. Sistem EMK Urbana je komercialen sistem, pri čemer ima podatkovno finančni del seveda veliko težo. Znotraj sistema se finančne poravnave izvajajo za različna obdobja in različne produkte, ki so odvisna od dogovorov med ponudniki storitev in partnerji, ki v poslovnem procesu sodelujejo. Dolžina obdobja je za različne partnerje različna, od enega dneva pa tudi do nekaj mesecev, z nekaj vmesnimi stopnjami (en teden, 10 dni, dva tedna, 15 dni, en mesec, …). Tudi pri produktih se lahko pojavljajo relativno kompleksne delitve, tako npr. poravnava se opravi na osnovi realizacije celotne linije, oz. samo dela linije ali zgolj opravljenih prevozov z določenim tipom vozovnice med različnimi deležniki v procesu. V sled kompleksnosti poravnalnih postopkov je predpogoj za njihovo kvalitetno izvedbo, točnost, zanesljivost in kredibilnost zajetih transakcij v EMK sistemu.

2.1 Skladnost z GDPR

Skrb za varstvo osebnih podatkov je ena ključnih postavk sistema EMK Urbana. Že od vsega začetka je sistem koncipiran tako, da zajema minimalno potrebno količino osebnih podatkov ter hkrati izpolnjuje maksimalne standarde zaščite slednjih.
Razširitev sistema EMK Urbana z vpeljavo novega medija – mobilna aplikacija v polni meri upošteva in izvršuje pravila o varstvu osebnih podatkov pri njihovi obdelavi in pravila o prostem pretoku osebnih podatkov v EU. Pod obdelavo uvršča vsa dejanja v zvezi z osebnimi podatki, torej zbiranje, hranjenje, urejanje, spreminjanje, razkritje, izbris, uničenje, prenos osebnih podatkov itd. Med osebne podatke pa po uredbi spadajo vsi podatki, ki se nanašajo na določljivega posameznika. Sistem EMK Urbana zagotavlja psevdonimizacijo, kar pomeni da je obdelava osebnih podatkov na način, da podatkov, ki so rezultat takšne obdelave, brez dodatnih informacij ni več možno pripisati posamezniku. Dodatne informacije se hranijo ločeno, s tehničnimi in organizacijskimi ukrepi pa se omejuje dostop do njih. Poleg pvsedonimizacije je zagotovljena tudi popolna anonimizacija osebnih podatkov, pomeni, da so vpeljani postopki pretvorbe osebnih podatkov v ” anonimizirane podatke“, ki se jih kljub dodatnim informacijam ne da pripisati posamezniku.

3 Mobilna aplikacija Urbana

Uvedba mobilne aplikacije v sistem EMK Urbana je zahtevala določene nadgradnje oz. prilagoditve zalednega sistema. Razlog temu je preprosto dejstvo, da vpeljava novega medija ni mogoča zgolj z zalednimi orodji, ki omogočajo manipulacijo z brezstičnimi karticami ampak je slednje bilo potrebno prilagoditi specifikam medija oz. mobilne aplikacije. Poleg naštetega, pa so pri nadgradnji bile upoštevane tudi prednosti interakcije med uporabnikom in aplikacijo, ki jih omogoča mobilna aplikacija za razliko od brezstične kartice. V prvi fazi je sistem EMK Urbana bil prilagojen za potrebe mobilne aplikacije na operacijskem sistemu Android, kasneje pa je bil posodobljen še za potrebe operacijskega sistema iOS, kjer je od nedavnega Urbana tudi na voljo.
Pri načrtovanju aplikacije so bile upoštevane tehnične specifike obeh operacijskih sistemov, varnostne zahteve sistema EMK, dane omejitve (dostop do NFC HCE je pri iOS še zmerom onemogočen), skladnost delovanja z zakonskimi predpisi in seveda uporabniška prijaznost oz. enostavnost uporabe [1]. Obe aplikaciji podpirata naslednje funkcionalnosti: popolnoma nadomeščata Urbana kartico in omogočata koriščenje dobroimetja in uporabo vozovnic v sistemu Urbana, prikazujeta stanje denarnice in aktivne produkte, vozovnice (skupaj s časom veljave) ter zgodovino uporabe. Prav tako prikazujeta informacije sistema Urbana (linije, postaje, bicikelj, parkomati, Urbanomati, zemljevidi, sheme), polnjenje dobroimetja, vozni redi in drugo.
Mobilni aplikaciji sta bili razviti z uradnima razvojnima orodjema, Android studio za okolje Android in Xcode za okolje iOS.

3.1 Pregled računa

Na osrednjem zaslonu mobilne aplikacije so zbrani najbolj relevantni podatki in bližnjice za uporabnika. Zaslon se vedno odpre pri zagonu aplikacije, seveda če je uporabnik že šel skozi namestitveni postopek in sta naprava in aplikacija vpisani v sistem.

V pregledu računa lahko uporabniki pregledujejo stanje dobroimetja ter ostale identifikacijske podatke aplikacije. Polnjenje računa aplikacije in nakup produktov je možno kot za običajne brezstične kartice oz. je omogočeno na daljavo ob uporabi določenih plačilnih shem (VALÚ-Moneta) do najvišjega zneska 50 €. Za vsak ID kartice se vodi zgodovina podatkov identično kot za izdane fizične brezstične kartice, vseh nakupov ter polnitev računa.
Aplikaciji ponujata prijazno ergonomsko oblikovano uporabniška izkušnjo interakcije sodobnega uporabnika s sistemom EMK Urbana in je na voljo v slovenskem ter angleškem jeziku, kar lahko uporabniki spreminjajo v nastavitvah.

Slika 1: Glavna stran

3.2 Urbana E-parking

Poleg popolne funkcionalne substitucije brezstične kartice je obeh aplikacijah dodana funkcionalnost E-parking, ki uporabniku omogoča, da plača parkirnino na daljavo preko mobilne aplikacije. Za parkiranje mora uporabnik nastaviti tri parametre: registrsko tablico, območje in čas trajanja parkirnine. Uporabnikom je omogočeno urejanje seznama registrskih tablic za vozila. Registrske številke lahko dodajajo, urejajo, brišejo ali spreminjajo pozicijo v seznamu.
Nadgrajena mobilna aplikacija prikazuje aktivno parkirnino, ki je vidna v seznamu aktivnih produktov mobilne kartice ter na domačem zaslonu. Dodan je tudi opomnik, ki omogoča prijazno manipulacijo podaljšanja parkirnine na daljavo.

3.3 Interakcija z zalednim sistemom

Obnašanje katerega koli vira, mobilne aplikacije ali spletne strani, temelji na interakciji med odjemnikom (mobilna aplikacija, terminalska aplikacija) in strežnikom. Vse datoteke spletnega projekta gostujejo na oddaljenem strežniku, ki se nahaja v ustrezno varovanem strežniškem okolju. Vse, kar se nahaja in deluje na strežniku - koda, skripte, SQL in druge datoteke – sodi v zaledni del.

Uporabniški vmesnik aplikacije (ang. front-end). je statičen in se polni s podatki, ko uporabnik uporablja mobilno aplikacijo in si želi ogledati določene podatke, v tem primeru aplikacija pošlje strežniku določeno zahtevo, slednji pa vrne pripravljene vsebine, ki jih aplikacija prikaže deloma ali v celoti.

Slika 2: E-parking

Komunikacija med mobilno aplikacijo in zalednim sistemom uporablja JSON notacijo in je kriptirana. Ta zapakira objekte v zaporedje zlogov, ki jih razumeta tako aplikacija, kakor tudi zaledni sistem. Za povezavo med zalednim sistemom in aplikacijo se uporablja asimetrična kriptografija za generiranje sejnega ključa, ki se uporablja v nadaljnji komunikaciji z simetrično kriptografijo. Pri simetrični kriptografiji gre za to, da se tako za šifriranje, kot dešifriranje uporablja enak ključ.
Dodatna zaščita sistema je v blokadi virtualnih kartic torej mobilnih aplikacij, ki so lahko v sistemu bodisi avtomatske ali pa ročne s strani administratorjev sistema.
Avtomatska blokada se vrši na podlagi avtomatske detekcije anomalij transakcij. Detekcija deluje tako, da se ob vsaki transakciji preveri čas zadnje uspešne transakcije, ki je shranjen poleg stanja dobroimetja v aplikaciji. V primeru, da se zgodi hipotetična zloraba s podvajanjem denarnice, je čas v dveh ločenih transakcijah enak, in takšna virtualna kartica-aplikacija je označena za sumljivo.
Prav tako pa se permanentno beležijo polnitve in poraba dobroimetja izdanih virtualnih kartic - mobilnih aplikacij. V določenem časovnem terminu se mora stanje polnitev in porabe ujemati, drugače se aplikacija označi za sumljivo in po pregledu administratorja se lahko takšna aplikacija doda na črno listo ter se s tem onemogoči nadaljnja uporaba. Črna lista identifikatorjev aplikacij se distribuira in kontinuirano obnavlja znotraj celotne terminalske infrastrukture EMK sistema Urbana, ki takšno aplikacijo ob prvi naslednji uporabi blokirajo in preprečijo uporabo v brezpovezavnem načinu.

3.4 NFC interakcija

V mobilni napravi je NFC modul razdeljen na različne komponente. Antena je vgrajena v ohišje naprave ali njeno baterijo (proizvajalec Samsung). NFC krmilnik je običajno ločen mikročip, ki skrbi za komunikacijo in je

vgrajen na logično vezje naprave. Varna shramba je lahko vgrajena v krmilnik, ali je ločena (SIM - Subscriber Identity Module, identifikacijski modul naročnika; MicroSD - Micro Secure Digital) [7]. Ker imajo mobilne naprave svoje napajanje, je lahko tudi aktivna NFC naprava. Tako lahko beremo značke, komuniciramo z drugo mobilno napravo (P2P) ali emuliramo NFC kartico. Najpreprostejši način NFC komunikacije je branje in pisanje NFC značk. Tak način komunikacije podpira večina NFC telefonov in je dobro standardiziran [3]. NFC značke lahko vsebujejo različne količine informacij in drugih funkcionalnosti. Prednosti uporabe NFC značk tehnologije je enostavna izvedba, hkrati pa je podpora delovanja mogoča skoraj v vseh mobilnih napravah različnih proizvajalcev. Transakcije, ki potekajo preko NFC tehnologije so počasnejše in manj zanesljive. Komunikacija ni identična komunikaciji terminal – brezstična kartica, zato je za implementacijo dotične komunikacije potrebna tudi posebna prilagoditev terminalov, da se omogoči delovanje. Podpora v nekaterih napravah pa je lahko celo problematična, saj se vsi proizvajalci ne držijo standardov. Kljub univerzalnosti rešitve glede na nabor mobilnih naprav se je rešitev izkazala kot neustrezna in je namesto nje uporabljena rešitev HCE (Hosted Card Emulation). Emulacija NFC kartice bolj znana kot HCE omogoča izvajanje transakcij, kot bi imeli dejansko brezkontaktno kartico. Slaba stran je omejitev dostopa do NFC HCE za iOS, zaradi česar je interakcija zadnjega koraka izvedena preko zvokovnega kanala mobilne naprave.

4 Varnost aplikacije »Urbana«

Današnje mobilne naprave so pravi računalniki v malem, saj imajo zmogljivo strojno opremo in hkrati kompleksne operacijske sisteme. V njih ni težko najti raznih pomanjkljivosti, ki jih je mogoče izkoristiti za poseg v varnost podatkov na napravi. Zato je pomembno, da se ob razvoju mobilnih aplikacij razvijalci zavedajo teh pomanjkljivosti (da jih je možno čim bolj obvladovati) [6]. V razvijanju programske opreme želimo z obfuskacijo namerno ustvariti izvorno ali strojno kodo, ki jo ljudje težko razumemo. Z izvedbo obfuskacije lahko na izvorni kodi preprečimo kopiranje kode v primeru obratnega inženiringa. Obfuskacija se uporablja za prekritje namena in delovanja aplikacije ter skrivanje logike. Glavna prednost obfuskacije je zaščita poslovnih skrivnosti, ki jih vsebuje programska oprema, saj je obratni inženiring v tem primeru težko izvedljiv. Hkrati se zaščiti mehanizem licenciranja in prepreči neavtoriziran dostop.

Podatki na napravi, ki so pomembni za transakcije, so shranjeni v t.i. varni shrambi. To je datoteka v mapi same aplikacije, ki je šifrirana s pomočjo ključev varne shrambe. Ti ključi so različni za vsako napravo in se generirajo s pomočjo id-ja naprave tako, da te datoteke ni mogoče enostavno kopirati na novo napravo. [3, 4]

Dodatna zaščita pred zlorabami je zapis časa zadnje spremembe varne shrambe, ki je zapisana, tako v varni shrambi, kot tudi v dodatni datoteki izven mape aplikacije. V primeru, da aplikacija zazna zlorabo, se varna shramba ponastavi in uporabnik ne more več uporabljati aplikacije za NFC transakcije.

Prenos podatkov med napravami je vedno varnostno občutljiv, saj ni popolnega nadzora nad potjo, kjer se podatki prenašajo. Najbolj učinkovita rešitev zaščite prenosa podatkov je šifriranje, ki je lahko asimetrično ali simetrično. Za zaščito NFC komunikacije se uporablja simetrično šifriranje, kjer ima vsaka naprava svoj unikatni ključ, ki se pridobi z glavnega ključa in identifikatorjem naprave, v procesu diverzifikacije na zalednem sistemu. Ta ključ se nadalje v postopku registracije naprave prenese iz zalednega sistema in je shranjen v varni shrambi naprave. Shranjen ključ je uporabljen v postopku ustvarjanja varne seje na začetku vsake transakcije. [4]

5 Sklep

Vse večja priljubljenost in razširjenost mobilnih aplikacij prinaša razvijalcem aplikacij tudi dodatne zahteve po zagotavljanju varnosti v aplikacijah in zalednih sistemih, ki jih aplikacije uporabljajo. Ker so moderni mobilni operacijski sistemi zelo razširjeni in odprti za razvijalce, aplikacije operirajo s sredstvi iz realnega sveta, so se pojavili tudi zlonamerni »igralci«, ki poskušajo zlorabiti sisteme.

Brezhibno varnost s programsko opremo v odprtih sistemih kot sta Android in delno tudi iOS je nemogoče zagotoviti. Zato je potrebno omogočiti dodatne varnostne mehanizme kot so strojni varnostni elementi in preverjanja v zalednih sistemih, ki otežijo in detektirajo zlorabe mobilnih aplikacij. Mehanizmi morajo biti tako avtomatski kot ročni, da se lahko zaznajo tudi morebitne nove ranljivosti s pomočjo statistične obdelave transakcijskih podatkov.

Literatura

[1] Breznik A., Avberšek M., Podbreznik P., Chowdhury A., Razvoj izboljšane uporabniške izkušnje in dodatnih funkcionalnosti v aplikaciji Urbana, ERK 2016

[2] Rožič B., Svečko J., Mezgec Z. in Chowdhury A., Koncept Margento sistema brezkontaktne kartice, ERK 2009

[3] Avberšek M., Informacijske rešitve brezkontaktnega plačevanja z mobilnimi napravami, diplomsko delo UM FERI, 2016

[4] Rulić P., Kotnik B., Klampfer S., Chowdhury A., Touch-and-Go mobile payment system. Journal of transportation technologies, ISSN 2160-0481, jan. 2017

[5] Svečko J., Rožič B., Chowdhury A., Razširitev funkcionalnosti sistema Enotne Mestne Kartice ERK 2011

[6] Rumež A., Vlaovič B., Varnost mobilnih naprav z operacijskim sistemom Android, ERK 2017

[7] Lepojević B., Pavlović B., Radulović A., Implementing NFC service security – SE VS TEE VS HCE, Conference: SYMORG 2014