Kritické zraniteľnosti v systéme Mobile Parking

Ing. Pavol Lupták, CISSP, CEH, pavol.luptak@nethemba.com

Abstrakt

Cieľom článku bude popísať vážne kritické bezpečnostné chyby v systéme Mobil Parking, ktorý umožňuje hradenie poplatku za parkovanie pomocou SMS správ v Bratislave, Banskej Bystrici, Košiciach, Lučenci, Martine, Prešove, Rimavskej Sobote a Trenčíne (a zrejme aj vo Viedni). Uvedené zneužitie sa určite týka parkovania s registráciou (dostupné pod číslom +421 902 020202). V prípade systému bez registrácie (štandardné dostupný pod číslom 2200) sa zraniteľnosť prejaví len v prípade, že existuje medzinárodná predvoľba pod ktorou je tento systém dostupný.

Uvedená chyba umožňuje, aby **ktokoľvek parkoval na kredit kohokoľvek**, kto je zaregistrovaný v systéme Mobil Parking. V článku tiež demonštrujeme jednoduchý spôsob, akým je možné zo systému Mobil Parking získať zoznam všetkých mobilných čísel registrovaných klientov, ktorí uvedenú službu používajú a teda môžu byť automaticky zneužití ako „platcovia“ podvrhnutého poplatku za parkovanie.

Dôležité upozornenie

Autor článku testovanie realizoval výhradne s vlastným mobilným číslom a ŠPZ vlastného auta. Pri testovaní nedošlo k ohrozeniu a poškodeniu iných osôb, ktorí sú registrovaní v uvedenom systéme.

1 Možnosť podvrhnutia SMS žiadosti o parkovanie

Systém Mobil Parking žiadateľa a teda aj samotného platcu o parkovanie identifikuje na základe odosielateľa (Sender) v zaslanej SMS žiadosti o parkovanie. Bohužiaľ odosielateľ SMS správy je ľahko podvrhnuteľný a existuje nespočetne veľa služieb, ktoré posielanie takýchto správ umožňujú. Na otestovanie sme použili službu http://www.armsms.com/, kde pri kúpe balíčka platinum (50 podvrhnutých SMS) bola cena 1 podvrhnutej SMS správy $0.243 (= 0.17 €). V prípade, že útočník už disponuje zoznamom platných registrovaných klientov v systéme Mobil Parking (možnosť ako tento zoznam získať je popísaný v

kapitole 2) suma 0.17€ predstavuje celkovú sumu, ktorú útočník musí zaplatiť za svoje podvrhnuté parkovanie (v prípade použitia lacnejšej služby, ktorá umožňuje zasielanie SMS správ s podvrhnutým odosielateľom, táto suma môže byť samozrejme ešte nižšia).

Útočník využije uvedenú webovú službu posielania podvrhnutých SMS správ na zaslanie podvrhnutej SMS správy v nasledujúcom formáte:

Číslo odosielateľa SMS správy – útočník uvedie mobilné číslo človeka, ktorý za uvedené parkovanie reálne zaplatí. Ako ďalej demonštrujeme, zoznam všetkých mobilných čísel registrovaných klientov systému Mobil Parking dokáže triviálne zistiť.

Cieľové číslo SMS správy – útočník uvedie číslo +421902020202

Obsah správy:

čas(medzera)*útočníkovaŠPZ

čas predstavuje dobu parkovania útočníkového auta.

Po zaslaní uvedenej SMS zo strany útočníka, obeť (ktorá za parkovanie reálne zaplatí) obdrží správu, že bola vykonaná platba na útočníkom definovanú dobu a útočníkovú ŠPZ.
Je potrebné si uvedomiť, že útočníková ŠPZ nemusí predstavovať bezprostredne ŠPZ auta samotného útočníka nakoľko podľa ŠPZ by bol jednoducho vypátrateľný.

Útočník dokáže vykonať zaplatenie parkovania veľkému množstvu rôznych ŠPZ (bez vedomia vlastníkov týchto áut!) na účet ľubovoľných registrovaných klientov systému Mobil Parking (samozrejme bez súhlasu týchto klientov). **Dokáže spôsobiť úplný chaos** - pri cene jednej podvrhnutej SMS správy 0.17 € (prípadne ešte menej) dokáže za 10 € spôsobiť oprávnenú reklamáciu 60 ľudí. To je množstvo, kedy sa jeho neoprávnená reklamácia jednoducho stratí – ak sa spoločnosti Mobil Parking začnú sťažovať stovky ich klientov za to, že niekto za ich predplatený kredit niekomu zaplatil parkovanie, je prakticky nemožné (bez spolupráce s mobilnými operátorom) identifikovať, ktoré z týchto sťažností sú oprávnené (a boli spôsobené podvrhnutou SMS správou) a ktoré nie.

Okrem toho útočník **dokáže byť plne anonymný** a predplatené SMS správy si zakúpiť pomocou anonymnej meny (Bitcoin) využitím anonymného prístupu (TOR), napríklad využitím služby https://smsz.net/.

2 Získanie zoznamu mobilných čísel všetkých registrovaných klientov Mobil Parking

Aby útočník dokázal podvrhnúť zaplatenie SMS parkovania pre danú ŠPZ, potrebuje poznať mobilné číslo registrované klienta systému Mobil Parking, ktoré následne nastaví ako odosielateľa pri posielaní podvrhnutej SMS správy o parkovanie.

Zoznam klientov služby Mobil Parking vzhľadom na vážnu bezpečnostnú chybu registračného formulára https://www.m-parking.sk/login.jsp?page=register dokáže získať relatívne triviálnym spôsobom. Registračný formulár totiž pri novej registrácii overuje, či dané mobilné číslo klienta v systéme už existuje alebo nie a ak áno, tak uvedenú informáciu pri registrácii automaticky zobrazí. Toto správanie sa dá jednoducho zneužiť na enumerovanie všetkých registrovaných platných mobilných čísel uložených v databáze Mobil Parking. Systém je síce chránený CAPTCHOU (konkrétne jcaptcha), všetky vygenerované CAPTCHE sa nám ale podarilo so 100%-tnou úspešnosťou zlomiť. Využili sme platené portály http://decaptcher.com a http://www.deathbycaptcha.com. Cena za prelomenie 1000 obrázkov CAPTCHE je $1.39 (= 0.97 €), čo stačí na enumerovanie 1000 mobilných čísel (a teda odhalenie, či ide o registrovaných klientov v systéme Mobil Parking alebo nie). Je pravdepodobné, že existujú aj opensource implementácie umožňujúce uvedenú CAPTCHU prelomiť tiež plne automatizovane a úplne zadarmo (z časových dôvodov sme analýzu kvalitných opensource prostriedkov na lámanie CAPTCHE nerealizovali).
V najhoršom prípade - ak by neexistoval lacnejší (alebo úplne zadarmo) automatizovaný spôsob lámanie jcaptche, tak prehľadanie celého mobilného rozsahu cez uvedený registračný formulár (napr. 0905 XXX XXX) by útočníka vyšlo na $1390 (978 €).

Je samozrejme nutné podotknúť, že útočníkovi na zasielanie podvrhnutých parkovacích SMS správ stačí odhaliť len 1 mobilné číslo registrovaného klienta (nemusí získať všetky). V prípade, že sa mu podarí odhaliť všetkých registrovaných klientov (čo je samozrejme len otázka času a peňazí), tak **dokáže ohroziť všetkých klientov systému Mobil Parking a využívať ich kredit na zasielanie podvrhnutých parkovacích SMS správ.**

Rakúsky SMS parking portál http://www.handyparken.at trpí rovnakou zraniteľnosťou – vďaka chybne implementovanému registračnému formuláru je možné plne automatizovane identifikovať mobilné čísla všetkých ich klientov. Oproti systému Mobil Parking tento registračný formulár nevyžaduje žiadne CAPTCHA overenie, čo znamená, že získanie všetkých mobilných čísel ich klientov je úplne triviálne a otázkou pár hodín.

3 Navrhované spôsoby opravy

Je potrebne si uvedomiť, že daný systém SMS parkovania obsahuje 2 nezávislé vážne bezpečnostné problémy, ktoré je potrebné opraviť.

1. Nakoľko spoločnosť Mobil Parking identitu platiteľa poplatku za parkovanie určuje na základe odosielateľa SMS správy, je potrebné **znemožniť,** aby bolo možné SMS správu (žiadosť o parkovanie) zaslať odvšadiaľ zo sveta na medzinárodné číslo +421 902 020202, napríklad tak, že budú podporované výhradne len skrátene voľby (podobne ako je to v systéme bez registrácie). Možnosť podvrhnúť odosielateľa SMS správy bude síce ďalej existovať, ale bez existencie služby na Slovensku, ktorá by umožňovala posielať podvrhnuté SMS správy z ľubovoľného čísla na skrátené čísla to nebude možné technicky jednoducho realizovať.

2. Upraviť registračný formulár na http://m-parking.sk, tak aby nebolo možné jednoducho získavať mobilné čísla už registrovaných klientov spoločnosti Mobil Parking, čo pokladáme aj za vážny problém ohrozenia osobných údajov. Ako riešenie navrhujeme implementovať daný registračný formulár tak, aby **nikdy pri registrácii nezobrazil, či dané mobilné číslo v systéme už existuje alebo nie**. Namiesto toho môže na dané mobilné číslo zaslať unikátny SMS autentifikačný kód, ktorý používateľ musí zadať v ďalšom kroku registrácie. Ak dané mobilné číslo už v systéme existuje, tak uvedená SMS správa nebude obsahovať autentifikačný kód, ale len informáciu o tom, že dané mobilné číslo je v systéme už použité a vyzve používateľa, aby v prípade, že zabudol svoje prihlasovacie meno a heslo do systému, použil štandardný formulár „zabudnuté heslo“ na preposlanie nového hesla (e-mailom, SMS).

   V tomto prípade je nevyhnutné zabezpečiť, aby útočník pri samotnej registrácii nemohol obťažovať náhodných ľudí autentifikačnými SMS správami – toto sa dá vyriešiť tak, že si pre danú IP adresu práve registrovaného klienta bude aplikácia pamätať, koľko autentifikačných SMS už bolo pre ňu poslaných a keď prekročí istý limit za definovaný časový interval, tak ďalšie posielanie autentifikačných SMS správ bude znemožnené.