Matej Kovačič

Zaupanje digitalnim dokazom in prometnim podatkom v mobilni telefoniji

O avtorju

dr. Matej Kovačič se ukvarja z vprašanji zasebnosti in nadzora v virtualnem prostoru, proučevanjem kiberkriminala, odprto kodo in informacijsko varnostjo. Je avtor več člankov in monografij iz navedenih področij. Svoje prispevke objavlja tudi na spletni strani <http://pravokator.si>.

Povzetek

Prispevek obravnava problematiko slepega zaupanja digitalnim dokazom. Sodišča in preiskovalci namreč digitalne dokaze, zlasti računalniško ustvarjene digitalne dokaze praviloma dojemajo kot zaupanja vredne same po sebi. Vendar pa takšna predpostavka ne drži vedno. V prispevku je prikazano kako je na relativno enostaven način mogoče ponarejati digitalne dokaze na SIM kartici ter kako je mogoče z relativno poceni tehnologijo pošiljati SMS sporočila s spremenjeno identifikacijo pošiljatelja ter izvajati klicanje s spremenjeno klicno identifikacijo, pri čemer se v zbirki prometnih podatkov pri operaterju zabeležijo lažni podatki. Predstavljeni so tudi rezultati varnostne analize slovenskih GSM omrežij, ki je pokazala kako je z relativno poceni opremo mogoče nezakonito prestrezati mobilne komunikacije in kako je ob neustrezni zaščiti mobilnega omrežja mogoče ponarejati mobilno identiteto uporabnika GSM telefonije – in s tem tudi vse prometne podatke, ki jih beleži operater.

Kazalo

1. Uvod

Skupina varnostnih strokovnjakov in pravnikov iz ZDA, Sergey Bratus, Ashlyn Lembree in Anna Shubina so leta 2010 na konferenci TRUST 2010 predstavili zanimiv prispevek z naslovom *Software on the Witness Stand: What Should It Take for Us to Trust It?* (Bratus, Ashlyn in Shubina, 2010).

V prispevku so izpostavili problematičnost zaupanja digitalnim dokazom. Dejstvo je, da se na sodiščih danes že rutinsko uporabljajo prometni podatki, ki jih beležijo ponudniki dostopa do interneta ter različni strežniki in druge omrežne naprave, podatki iz mobilnih telefonov, podatki iz digitalnih nadzornih videokamer, itd. Tudi pri digitalni forenziki digitalne dokaze išče in analizira različna programska oprema, saj je podatkov pogosto preveč, da bi jih lahko ročno, brez pomoči programov pregledal posamezni preiskovalec.

Težava, ki so jo izpostavili raziskovalci v svojem članku je, da sodišča digitalne dokaze, zlasti računalniško ustvarjene digitalne dokaze praviloma dojemajo kot zaupanja vredne same po sebi (avtorji uporabljajo angleški izraz *inherently trustworthy evidence*).

To ima posledice tudi na sam sodni postopek, saj imajo na (kazenskem) sodišču obtoženci oz. obramba pravico so soočenja s tožniki in (navzkrižnega) zaslišanja prič. Pri tem se postavlja zanimivo vprašanje, kaj storiti, če je »priča« računalnik oz. programska oprema? Čeprav se vprašanje na prvi pogled morda zdi akademsko, velja opozoriti na zanimiv sodni primer v ZDA *State v. Chun* (*Supreme Court of New Jersey A-96-06, Docket No. 58,879*), kjer je v sodnem postopku pritožnica oporekala rezultatom testa alkoholiziranosti zaradi možnih napak v programski opremi elektronskega etilometra.

Pritožnica je zahtevala preveritev zanesljivosti delovanja elektronskega alkotesta *Draeger Alcotest 7110 MKIII-C* (te alkoteste uporablja tudi slovenska policija). Pridobili so izvorno kodo naprave in jo predali v analizo neodvisnemu podjetju *Base One Technologies*. Podjetje je v programski kodi naprave odkrilo 19.400 potencialnih napak, med njimi devet takšnih, ki bi lahko bistveno vplivale na rezultate meritve. Med drugim se je tudi izkazalo, da je naprava na precej nenavaden način izračunavala povprečje meritev, saj je to počela na način, da je imela ena meritev veliko večji vpliv kot ostale (Resman, 2009). Vrhovno sodišče ZDA v konkretnem primeru sicer ni razveljavilo veljavnosti meritev alkoholiziranosti, je pa od proizvajalca zahtevalo odpravo napak v programski opremi elektronskega alkotesta. Primer vsekakor lepo kaže na znano dejstvo, da sodobna informacijska tehnologija vsebuje številne napake, kljub temu pa se digitalne oziroma elektronske dokaze, ki jih te naprave ustvarjajo, le redko postavlja pod vprašaj

Na problem zaupanja digitalnim dokazom bomo opozorili tudi v tem prispevku in sicer na primerih digitalnih dokazov na SIM kartici, pošiljanju SMS sporočil s spremenjeno identifikacijo pošiljatelja, klicanju s spremenjeno klicno identifikacijo ter prevzemanju mobilne identitete drugega uporabnika v GSM omrežju mobilne telefonije.

2. Digitalni dokazi na SIM kartici mobilnega telefona

2. 1. Nekaj osnov o SIM karticah

SIM kartica je tim. pametna kartica (vsebuje mikroprocesor), ki vsebuje podatke za avtentikacijo in avtorizacijo uporabnika mobilnega telefona v mobilnem omrežju. Vsebuje različne, tudi identifikacijske podatke in programsko opremo (avtentikacijske in šifrirne algoritme). Posebej pomembna je IMSI številka, ki služi kot *identifikator naročnika* v GSM omrežju. Identifikator *telefonskega aparata* pa je IMEI številka (*International Mobile Equipment Identity*), gre za neke vrste serijsko številko mobilne naprave (telefona).

IMSI številka je zapisana na SIM kartici. Na podlagi IMSI številke se mobilni uporabnik predstavi mobilnemu omrežju, omrežje pa mu »dodeli« naročniško telefonsko številko. Zaradi možnosti prisluškovanja in sledenja uporabnikom naj bi se IMSI številka po omrežju prenašala čim redkeje.[1] Namesto nje se prenaša naključno ustvarjena TMSI številka. IMSI se prenese preko omrežja v trenutku, ko se telefon vključi ali ko je potrebno obnoviti povezavo med IMSI in TMSI (oz. ustvariti nov TMSI). TMSI številka je omejena na lokacijsko območje, kar pomeni, da je potrebno nov TMSI ustvariti vsakič, ko se mobilni uporabnik premakne v novo lokacijsko območje. Lokacijska območja tvori ena ali več baznih postaj. Vsako lokacijsko območje ima svojo lastno kodo lokacijskega območja, kodo pa v intervalih oddajajo posebne bazne postaje in sicer tim. »*base transceiver station*« ali BTS v GSM omrežjih oziroma *Node B* v UMTS omrežjih.

Naslednji pomemben podatek, ki se nahaja na SIM kartici, je avtentikacijski šifrirni ključ ali Ki. Gre za 128-bitno spremenljivko (število), ki služi za avtentikacijo SIM kartice mobilnemu omrežju. Ki je unikaten za vsako SIM kartico in določen v procesu tim. personalizacije. Shranjen je na SIM kartici in v podatkovni bazi mobilnega operaterja, v tim. *Home Location Registru* (HLR). Ki ključa ni mogoče izpisati, pač pa ima SIM kartica posebno funkcijo *RUN GSM ALGORITHM*, ki telefonu omogoča, da le-ta SIM kartici pošlje podatke, SIM kartica pa jih nato podpiše s Ki ključem.

Zaradi tega je SIM kartica ključen gradnik varnosti v GSM omrežju oziroma nujno potreben element GSM omrežja. Zaradi slabe varnostne zasnove je bilo stare SIM kartice mogoče razmeroma enostavno *klonirati* oz. prekopirati Ki šifrirni ključ, pri novejših SIM karticah pa je kloniranje bistveno težje, poleg tega postopek kloniranja lahko poškoduje oz. uniči SIM kartico.

Če torej na kratko povzamemo, SIM kartica skrbi za avtentikacijo uporabnika v omrežju, na SIM kartici je shranjen šifrirni ključ, ki omogoča šifriranje pogovorov med mobilnim aparatom in bazno postajo v GSM omrežju, poleg tega pa je na SIM kartico mogoče shranjevati tudi določene uporabniške podatke. Najpomembnejši med njimi so seznam kontaktov uporabnika (tim. telefonski imenik) in SMS sporočila. Nekateri starejši mobilni telefoni pa so na SIM kartico shranjevali tudi zadnje klicane številke. Naj dodamo, da novejši mobilni telefoni uporabniških podatkov na SIM kartico praviloma ne shranjujejo, pač pa se ti podatki shranjujejo v telefon.

2. 2. Branje uporabniških podatkov iz SIM kartice

V okviru forenzične preiskave SIM kartice iz le-te navadno želimo prebrati nekaj osnovnih

1 IMSI številko je mogoče pridobiti tudi s pomočjo telefonske številke naročnka. To je mogoče s pomočjo vpogleda v HLR register (*Home Location Register; HLR lookup*), ki je mogoč premo SS7 signalizacije. Na spletu je mogoče najti nekaj ponudnikov, ki uporabniku omogočajo, da vpiše poljubno GSM telefonsko številko, sistem pa vrne IMSI številko v določenih primerih pa tudi (grobo) lokacijo mobilnega telefona. Več o tem v nadaljevanju.

identifikacijskih podatkov SIM kartice (npr. IMSI številko in ICCID identifikacijsko številko) ter seznam kontaktov, SMS sporočila ter zadnje klicane številke.

Za branje teh podatkov iz SIM kartice potrebujemo PIN ali PUK kodo (razen, če PIN koda ni blokirana). Če PIN kode nimamo, je mogoče PUK kodo pridobiti od operaterja, v tem primeru je operaterju potrebno sporočiti ICCID serijsko številko, ki je natisnjena na SIM kartici. Poleg tega potrebujemo še ustrezno strojno (čitalec SIM kartic) in programsko opremo.

Strojna oprema za branje vsebine SIM kartic je razmeroma poceni. USB čitalec SIM kartic lahko naročimo preko spleta (cena je nekaj EUR), lahko pa si ga celo izdelamo sami. Načrti za preprost čitalec SIM kartic so dostopni na spletni strani ameriške elektroinženirke *Limor Fried*.[2]

Na tej spletni strani se nahaja tudi odprtkodna in brezplačna programska oprema za branje vsebine SIM kartic *PySIMReader*. Aplikacija omogoča ne le branje, pač pa tudi zapisovanje podatkov na SIM kartico. Uporaba aplikacije je preprosta, omogoča pa branje telefonskega imenika, SMS sporočil, branje identifikacijskih podatkov SIM kartice, seznam zadnjih klicanih številk ter spreminjanje oziroma blokado PIN kode. Aplikacija omogoča tudi prikaz izbrisanih SMS sporočil (v kolikor seveda še niso bila prepisana z drugimi podatki), pri vsakem SMS sporočilu lahko pa lahko spremenimo njegov status (*read* / *unread* / *deleted* : *prebrano* / *neprebrano* / *izbrisano*).

Naj omenimo, da omenjena aplikacija ne zna delati z vsemi SIM karticami - pri nekaterih SIM karticah določenih operaterjev je v programu prišlo do napake in branje podatkov ni bilo mogoče. Vendar je aplikacija odprtokodna in je zato njeno popravljanje oziroma dopolnjevanje z razmeroma enostavno.

2. 3. Ponarejanje digitalnih dokazov na SIM kartici

Kot omenjeno aplikacija *PySIMReader* omogoča tudi zapisovanje podatkov na SIM kartico. Postopek je povsem enostaven, mogoče pa je spreminjati vse elemente SMS sporočila: *datum*, *konktakt pošiljatelja*, *številko operaterjevega centra za posredovanje sporočil* ter *vsebino sporočila* (*Date, From, ServiceCenter, Message*) ter status SMS sporočila (*rebrano* / *neprebrano* / *izbrisano*). V navedena polja lahko vpišemo poljubne podatke, biti pa morajo v ustreznem formatu.

Če sedaj tako obdelano SIM kartico vstavimo v telefon, bodo prikazana ponarejena SMS sporočila na SIM kartici. Za potrebe prikaza smo izdelali dve izmišljeni SMS sporočili. V prvem primeru smo izdelali SMS sporočilo iz prihodnosti (iz 15. oktobra 2014), v drugem primeru pa je pošiljatelj (njegovi kontaktni podatki so ponarejeni) 12. januarja 2001 poslal »napoved« terorističnih napadov na WTC 11. septembra 2001.

2 Spletna stan je dostopna na naslovu <http://ladyada.net/make/simreader/index.html>.

Slika 1: Ponarejeno SMS sporočilo "iz preteklosti"...

Slika 2: ... in ponarejeno SMS sporočilo "iz prihodnosti".

Mimogrede, v primeru novejših telefonov je SMS sporočila iz SIM kartice mogoče tudi prenesti in shraniti na telefon. Ponarejanje digitalnih dokazov v mobilnih telefonih (zlasti tim. pametnih telefonih) je tudi mogoče, vendar je postopek nekoliko drugačen, saj je potrebno spreminjati podatke v samem telefonu, kar pa je pri novejših tim. pametnih telefonih z ustrezno programsko opremo prav tako razmeroma enostavno opravilo.

Seveda bi v primeru kazenske preiskave preiskovalci (verjetno) pregledali tudi prometne podatke pri operaterju. V primeru, da bi se lahko izkazalo, da je na SIM kartici shranjeno SMS sporočilo, prometni podatki pri operaterju pa ne bi potrjevali, da je bilo SMS sporočilo zares poslano. To bi bil za preiskovalce lahko indic, da je vsebina SIM kartice morda ponarejena. Prometni podatki se v skladu z ZeKOM (*Uradni list RS, št. 13/2007- UPB 1, 102/2007-ZDRad, 110/2009, 33/2011*) sicer hranijo 14 mesecev.

Vendar pa bi napadalec lahko vzel obstoječe SMS sporočilo in mu spremenil samo vsebino, prometne podatke (kontakt pošiljatelja in datum ter čas pošiljanja sporočila) pa bi pustil nespremenjene. V tem primeru bi prometni podatki pri operaterju potrjevali, da je bilo sporočilo res poslano, forenzična analiza SIM kartice pa bi razkrila vsebino, za katero pa s forenzičnimi postopki ne bi bilo mogoče ugotoviti ali je resnična ali morda ponarejena.

Pri tem se postavlja zanimiva analogija s pogovorom, kjer operater tudi zabeleži prometne podatke, ne pa tudi vsebine pogovora. V tem primeru je s pomočjo prometnih podatkov načeloma mogoče potrditi dejstvo obstoja komunikacije (kot bomo videli kasneje ni nujno, da to drži), vsebina pa je stvar izjav oseb, ki so bile udeležene v komunikaciji. Pri nasprotujočih si izjavah se

seveda povsem legitimno postavi vprašanje kateremu izmed udeležencev v komunikaciji verjetni in kateremu ne. V primeru SMS sporočil, katerih vsebina je shranjena, pa bi bila stopnja zaupanja v resničnost vsebine SMS komunikacije verjetno bistveno višja kot v primeru govorne komunikacije, ki se ne shranjuje.

3. Pošiljanje SMS sporočil s spremenjeno identifikacijo pošiljatelja

Podobne zagate povezane s slepim zaupanjem digitalnim in računalniško ustvarjenim podatkom izvirajo tudi iz možnosti pošiljanja ponarejenih SMS sporočil preko GSM omrežja. Pri tem imamo v mislih ponarejanje podatka o pošiljatelju.

Pošiljanje SMS sporočil iz "poljubne številke" – v resnici gre za pošiljanje SMS sporočil s spremenjeno identifikacijo pošiljatelja – je v praksi pravzaprav povsem enostavno izvedljivo, saj za to ni potrebno praktično nikakršno poznavanje tehnologije. Vse, kar mora potencialni napadalec narediti je le, da na internetu poišče ustreznega ponudnika pošiljanja SMS sporočil.

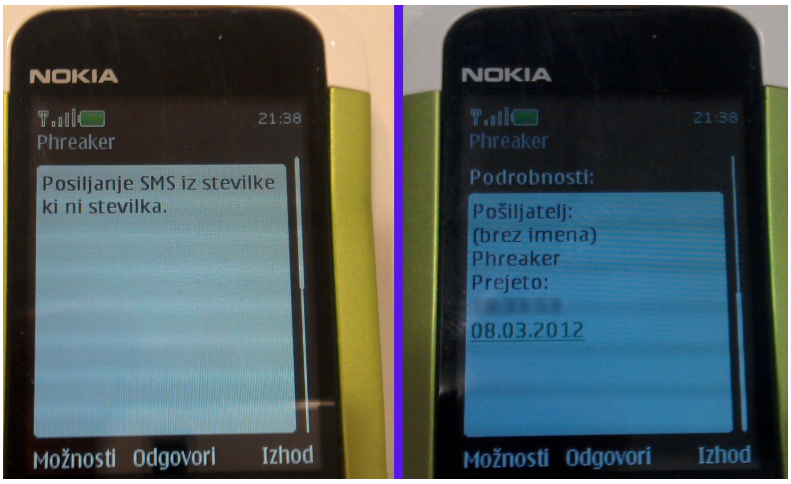
Na spletu je mogoče najti ponudnike, ki oglašujejo pošiljanje tim. ponarejenih SMS sporočil, vendar je cena pošiljanja teh sporočil lahko kar visoka – tudi nekaj EUR na poslano sporočilo. Z malo brskanja po spletu pa lahko najdemo večje ponudnike pošiljanja SMS sporočil, ki svojim strankam omogočajo avtomatizirano pošiljanje velikega števila SMS sporočil preko preprostega spletnega servisa. Te storitve praviloma uporabljajo podjetja, ki preko SMS sporočil svojim strankam pošiljajo različna obvestila, spletne strani, ki svojim uporabnikom preko SMS sporočil posredujejo gesla, itd. Skratka vsi, ki ponujajo različne SMS storitve.

Gre za povsem komercialno storitev, ki omogoča avtomatizirano pošiljanje (in tudi sprejemanje) velikega števila SMS sporočil. Cene za poslano SMS sporočilo se seveda razlikujejo, prav tako kvaliteta storitve (predvsem zmogljivost oz. hitrost pošiljanja večje količine SMS sporočil), praviloma pa so cene največ nekaj centov za poslano SMS sporočilo v Slovenijo.

Za potrebe raziskave varnosti mobilne telefonije smo na spletu hitro našli ponudnika, ki omogoča pošiljanje SMS sporočil v Slovenijo po ceni 1 cent na sporočilo, ponudnik pa ob brezplačni registraciji vsakemu svojemu uporabniku celo brezplačno naloži 2 EUR dobroimetja. Za registracijo je potrebno vpisati veljaven elektronski naslov, kamor nato ponudnik pošlje podatke za aktivacijo računa.

Veljaven elektronski naslov (in IP naslov) je torej edini identifikacijski podatek morebitnega napadalca in seveda je odveč omeniti, da si potencialni napadalec lahko najprej ustvari anonimen elektronski naslov, z njim pa se nato registrira pri navedenem ponudniku s čimer pridobi možnost pošiljanja 200 brezplačnih SMS sporočil na mobilne številke slovenskih operaterjev. Za skrivanje svojega pravega IP naslova pa napadalec lahko poskrbi z uporabo anonimizacijskega omrežja ali pa do storitve dostopi preko kiberkavarne ali drugega anonimnega dostopa do interneta. Za pošiljanje dodatnih SMS sporočil je seveda potrebno na svoj račun nakazati dodatna finančna sredstva, vendar že možnost pošiljanja 200 SMS sporočil napadalcu lahko povsem zadostuje.

Pošiljanje SMS poročil je sicer mogoče na več načinov, najbolj enostaven način pa je pošiljanje preko spletnega API vmesnika. Zanimivo je, da kot številko pošiljatelja lahko vpišemo poljuben niz znakov – tako številke, kot tudi besedilo. Tako je mogoče poslati SMS sporočilo pri katerem se kot telefonska "številka" pošiljatelja izpiše npr. "*DedekMraz*" ali "*Phreaker*" (gre za izraz, ki označuje tim. telefonske hekerje, torej osebe, ki se ukvarjajo z varnostjo telefonskih sistemov).



Slika 3: SMS sporočilo z lažno identiteto pošiljatelja.

Pošiljanje SMS sporočil s poljubno identifikacijo pošiljatelja je torej povsem enostavno, z malce truda pa ga je mogoče izvesti tudi povsem anonimno. Kako pa vse skupaj v resnici poteka po tehnični plati, pa bomo prikazali na primeru vzpostavljanja govornih klicev s spremenjeno klicno identifikacijo.

4. Klicanje s spremenjeno klicno identifikacijo

Tretji primer na katerem želimo pokazati na problematiko slepega zaupanja digitalnim dokazom je primer ponarejanja klicne identifikacije pri govornih klicih. Za začetek je potrebno poudariti, da spreminjanje klicne identifikacije samo po sebi ni prepovedano in v praksi se ta tehnologija tudi razmeroma pogosto uporablja. Tipičen primer so različni klicni centri, kjer so telefoni posameznih operaterjev v klicnem centru nastavljeni tako, da se kot njihova klicna identifikacija prikazuje telefonska številka centrale ali npr. vodje centra. Prepovedana pa je seveda zloraba, ki lahko izvira iz spreminjanja klicne identitete.

Storitev spreminjanja klicne identitete ponujajo tudi različna podjetja, ki nudijo storitve ponudnikov telefonije preko interneta, npr. Vox.io, Skype ipd.. Ta podjetja svojim uporabnikom omogočajo klicanje "iz" njihove obstoječe mobilne številke preko spleta. Vendar pa omenjena podjetja pred vklopom klicanja s spremenjeno klicno identifikacijo preverijo lastništvo mobilne številke, ki jo uporabnik vpiše kot svojo.

To preverjanje poteka npr. tako, da na telefonsko številko uporabnika najprej pošljejo SMS z aktivacijsko kodo, ki jo mora uporabnik nato preko spletnega vmesnika prepisati v svoj uporabniški račun. Na ta način ponudniki teh storitev zagotovijo, da telefonska številka, ki se bo prikazovala kot klicna identifikacija pri klicih preko interneta, res pripada njihovemu uporabniku (oziroma, če smo bolj natančni, da je imel v času registracije njihov uporabnik dostop do mobilnega aparata s to številko).

Ponudnikov, ki bi omogočali povsem poljubno spreminjanje klicne identifikacije za govorne klice pa ni mogoče enostavno najti, saj gre – kot bomo pokazali v nadaljevanju – za storitev, ki omogoča resne goljufije. Takšne ponudnike je praviloma mogoče najti v tujini. Kljub temu pa smo z nekaj malega truda takšnega ponudnika hitro našli tudi v Sloveniji.

4. 1. Priprava tehnologije za klicanje s poljubno klicno identifikacijo

Za spreminjanje klicne identifikacije v primeru govornih klicev potrebujemo dostop do interneta, ustrezno programsko opremo (programsko telefonsko centralo ter programski telefon) ter povezavo do telefonskega omrežja. Najbolje je, če pridobimo tim. *medoperaterski dostop*, lahko pa uporabimo kar obstoječi SIP račun pri kakšnem ponudniku internetne telefonije, ki ne filtrira vnosov klicne identifikacije. Edini realni strošek je torej le strošek dostopa do telefonskega omrežja, pa še to ni nujno, saj napadalec lahko vdre v centralo ponudnika telefonije ali pa nekomu ukrade SIP račun za internetno telefonijo (za to so na voljo različna orodja, npr. *SIPVicious*, itd.). Vsa programska oprema, ki smo jo uporabili za potrebe prikaza je odprtokodna in je brezplačno dostopna preko interneta.

V nadaljevanju si bomo pogledali nekoliko bolj zapleteno povezavo v telefonsko omrežje, saj želimo spreminjanje klicne identifikacije izvajati čim bolj mobilno (torej iz prenosnega računalnika) in neodvisno od vrste povezave v internet, hkrati pa si želimo zagotoviti anonimnost oz. neizsledljivost.

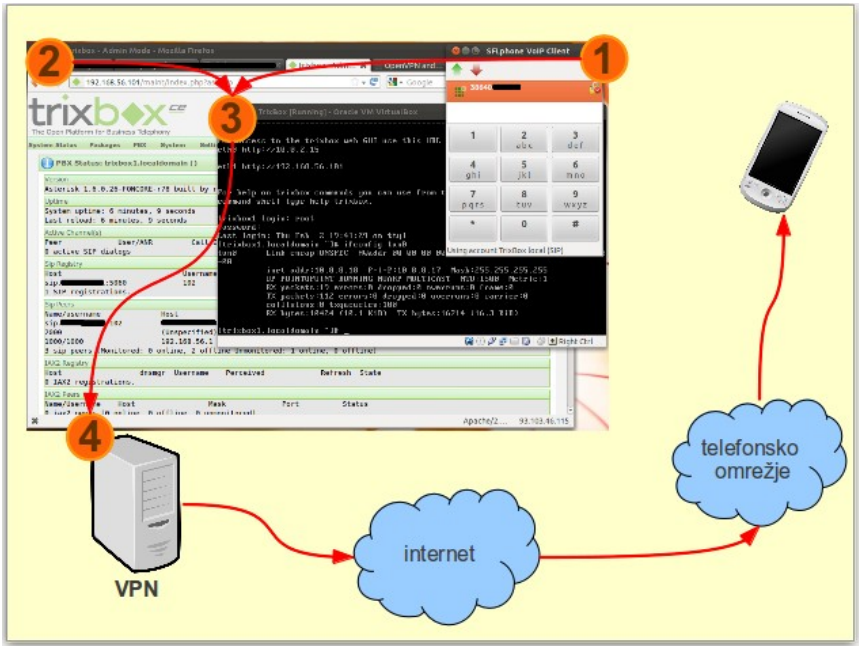
Ključen del potrebne infrastrukture je programska telefonska centrala. Za programsko telefonsko centralo smo izbrali Linux distribucijo Trixbox. Gre za posebej prilagojeno Linux distribucijo v osnovi katere je operacijski sistem Centos 5.5, na katerem teče programska oprema za internetno telefonijo Asterisk ter ustrezni podporni programi za enostavno konfiguracijo in upravljanje telefonske centrale. Vsi programi so odprtokodni in na voljo brezplačno.

Trixbox smo namestili v virtualni računalnik (izbrali smo brezplačni in odprtokodni VirtualBox), v internet in nato do telefonskega omrežja pa smo vzpostavili povezavo preko lastnega VPN omrežja (zanj smo uporabili odprtokodni OpenVPN).

Pomemben del zahtevane infrastrukture je vzpostavitev povezave do telefonskega omrežja oz. pridobitev tim. medoperaterskega dostopa. Vrsta povezave do telefonskega omrežja je seveda odvisna od tega, kakšno vrsto povezave nam sploh omogoča naš operater internetne telefonije. Zlasti je pomembno, da poiščemo operaterja, ki ne filtrira tim. CID vnosov oz. kakorkoli drugače omejuje naše povezave v telefonsko omrežje. Čeprav se to morda na prvi pogled zdi težko, je take operaterje mogoče najti tako v tujini (zlasti v kakšnih azijskih državah), kot tudi v Evropi. V Sloveniji je (bilo) mogoče najti tudi operaterje, ki zaradi slabe varnosti v svojem omrežju ne filtrirajo klicne identifikacije niti za svoje končne uporabnike SIP telefonije.

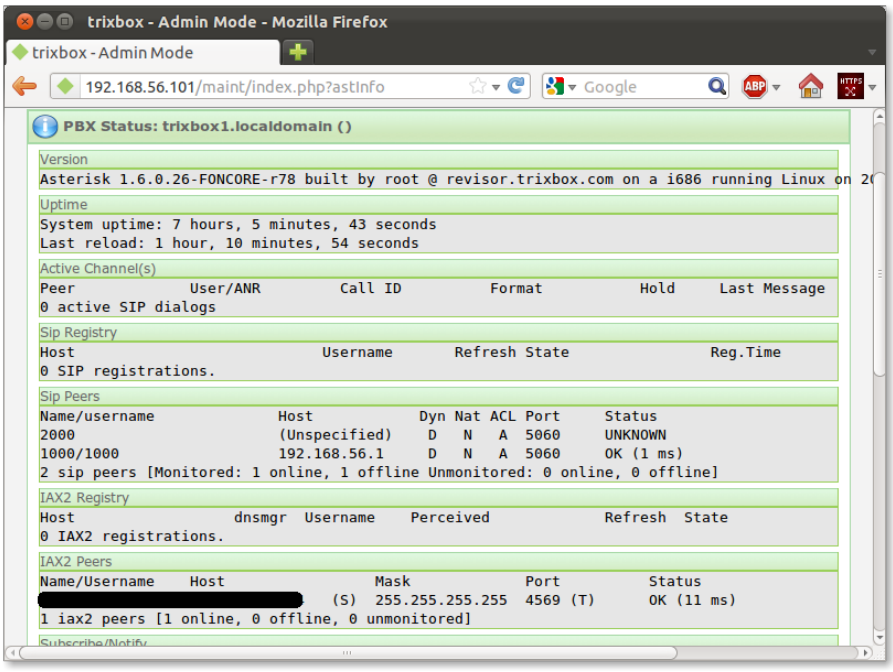
Ko nastavimo Trixbox centralo in povezavo do operaterja sledi še konfiguracija programskega telefona SIP, preko katerega bomo dejansko izvajali klicanje. V našem primeru smo uporabili odprtokodni in brezplačni SFL Phone in vanj vpisali ustrezne nastavitve za povezavo na našo virtualne Trixbox centralo.

Ko vse skupaj zaženemo torej povezava poteka takole. Fizični računalnik se v internet povezuje preko žične, brezžične ali mobilne povezave. Virtualna telefonska centrala Trixbox se preko te internetne povezave poveže na VPN strežnik, od tam pa preko našega operaterja v telefonsko omrežje. Programski telefon SFL Phone pa se preko SIP protokola iz fizičnega računalnika lokalno poveže na virtualno Trixbox centralo. Klic torej iz našega lokalnega računalnika potuje na virtualno telefonsko centralo od tam pa preko VPN povezave do našega ponudnika telefonije in do končne klicane osebe.



Slika 4: Shema naše povezave: (1) programski telefon SFL Phone, (2) vmesnik za nastavljanje telefonske centrale, (3) telefonska centrala v virtualnem stroju, (4) šifriran VPN strežnik preko katerega se povezujemo v telefonsko omrežje.

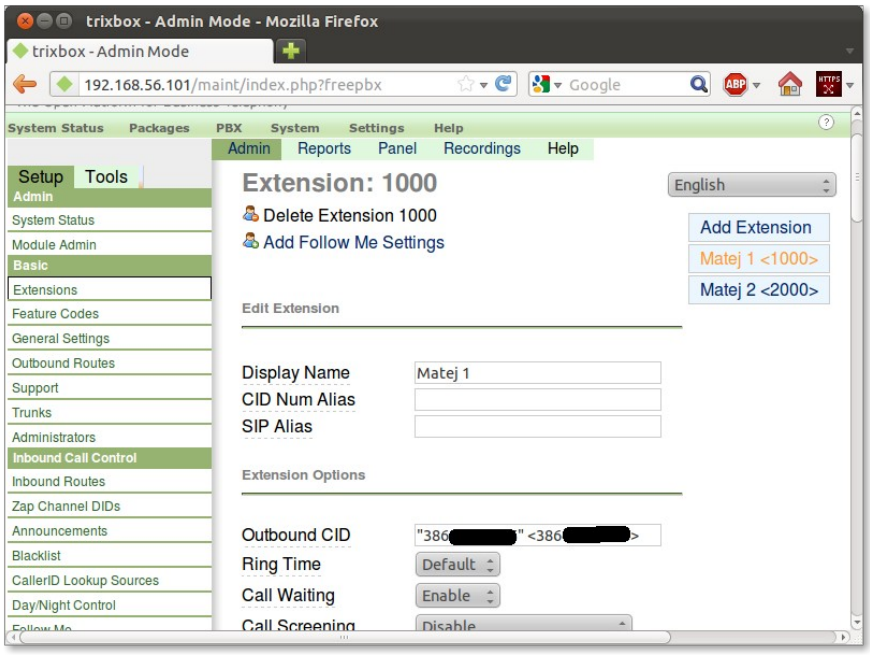
Status povezave telefonske centrale lahko preverimo preko spletnega vmesnika in če je povezava uspešna lahko skušamo opraviti prvi klic. V programskem telefonu *SFL Phone* vpišemo telefonsko številko v mednarodni obliki (če npr. želimo klicati na mobilno številko 040/123-456 v programski telefon vtipkamo 38640123456) in kliknemo gumb za klicanje. Če se klic vzpostavi, je postavitev celotnega sistema uspešna.



Slika 5: Status virtualne telefonske centrale.

4. 2. Izvedba klicanja s spremenjeno klicno identifikacijo

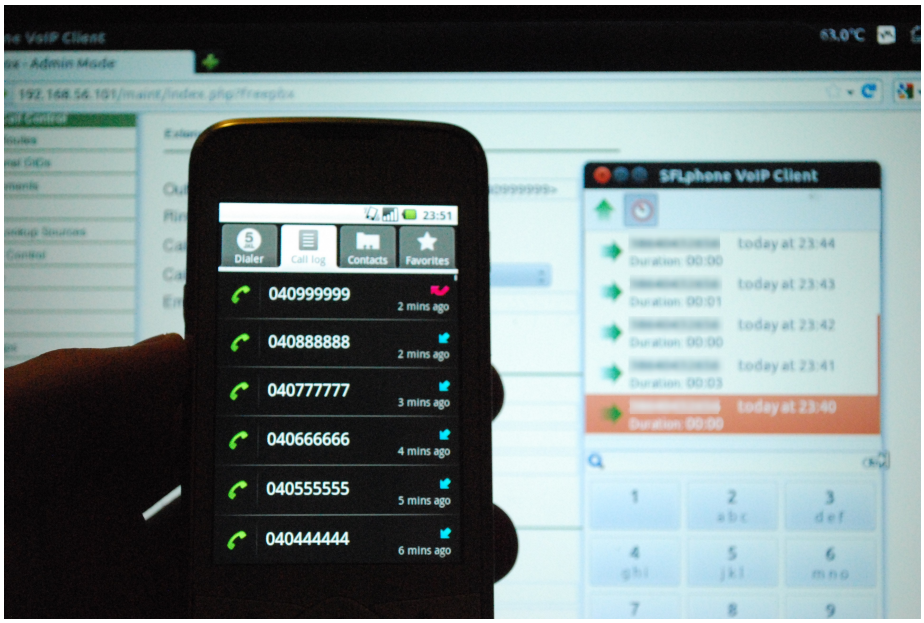
Če sedaj želimo opraviti klic s spremenjeno klicno identifikacijo, v nastavitvah telefonske centrale med nastavitvami lokalne telefonske številke (ang. *extension*) kot izhodno klicno identifikacijo (*Outbound CID*) vpišemo poljubno telefonsko številko v mednarodnem formatu.



Slika 6: Nastavitve prikaza klicne identifikacije za lokalno telefonsko številko.

Če bi se torej klicanemu radi predstavili s klicno identifikacijo npr. 040/999-999, je kot izhodno klicno identifikacijo potrebno vpisati “38640999999” <38640999999>. Nastavitve shranimo in uveljavimo spremembe na telefonski centrali. Ko bomo naslednjič poklicali na poljubno zunanjo tele-

fonsko številko, se bo tam kot klicna identifikacija klicatelja izpisala telefonska številka 040999999.



Slika 7: Prikaz prejetih klicev na mobilnem telefonu. V ozadju vmesnik za spreminjanje nastavitev telefonske centrale in programski telefon SFL Phone.

Postopek se za končnega uporabnika storitve da še nekoliko poenostaviti, saj je Trixbox centralo mogoče nastaviti tako, da sprejema dohodne klice, uporabnikom pa omogoča, da s pomočjo telefonskega aparata najprej nastavijo želeno klicno identifikacijo (vtipkajo številko, ki naj se prikaže pri izhodnem klicu), nato pa vnesejo izhodno številko kamor se klic s spremenjeno klicno identifikacijo preusmeri. Na ta način bi bilo mogoče klicanje s spremenjeno klicno identifikacijo izvajati zgolj s telefonskim aparatom, seveda pa bi nekje nekje v ozadju potrebovali ustrezno nastavljeno telefonsko centralo ter vso prej opisano infrastrukturo. Na opisan način lahko kličemo “iz” poljubne številke, tudi “iz” svoje lastne ali pa celo povsem izmišljene (neobstoječe), npr. 1116.

Klicanje s spremenjeno klicno identifikacijo je v tehničnem smislu podobno kot pošiljanje elektronske pošte s spremenjenim (lažnim) naslovom pošiljatelja (tim. “From:” polje v vzglavju elektronske pošte). Razlika je le v tem, da je izvedba nekoliko bolj zahtevna, po drugi strani pa je zlonamernega klicatelja precej težje izslediti.

* * *

Računalniško generirane podatke ljudje praviloma dojemamo kot zaupanja vredne same po sebi (tim. *inherentno zaupanje*) in praviloma ne pomislimo na možnost, da so podatki spremenjeni oz. ponarejeni. Ker pa na tej predpostavki pravilnosti in točnosti takšnih podatkov slonijo naše domneve o identiteti klicatelja, ima spreminjanje klicne identifikacije lahko resne posledice.

Tako se je po letu 2002 v ZDA pojavilo večje število zlorab, poimenovanih *swatting*. Gre za to, da napadalci s ponarejeno klicno identifikacijo kličejo na številko za klic v sili oziroma policijo (v ZDA na številko 911) in grozijo, da zadržujejo talce. Policija pa se nato odzove s prihodom specialne enote tim. SWAT (*Special Weapons and Tactics*), kar seveda povzroči nevšečnosti nič hudega slutečim pravim lastnikom telefonske številke. Od tu tudi izvira izraz *swatting*.

Na spletni strani *Dispatch Magazine On-Line*[3] je navedeno nekaj več podatkov o *swattingu*. Kot pravilno ugotavljajo avtorji prispevka, tehnični ukrepi proti spreminjanju klicne identifikacije niso mogoči, je pa *včasih* mogoče naknadno ugotavljati izvor klica.

Drugo možnost zlorabe na svojem blogu opisuje Brian Krebs. Napadalci najprej pridobijo dostop do bančnega računa žrtve, nato pa med tem, ko izvajajo bančne transakcije, žrtev zasujejo s klici iz naključno ustvarjenih telefonskih številk. S tem preprečijo, da bi banka, ki zazna sumljive transakcije uspela priklicati svojo stranko ter preveriti veljavnost sumljivih transakcij. Ker so telefonske številke naključno ustvarjene, jih žrtev tudi ne more blokirati. Kot poroča Brian Krebs, je bilo tako storitev na črnem trgu mogoče naročiti za 5 USD na uro oz. za 40 USD na dan (Krebs, 2011).

Znan je tudi primer iz Velike Britanije, kjer so v začetku leta 2012 neznani napadalci s pomočjo spremenjene klicne identifikacije izvajali masovno klicanje posameznikov (tudi do 1000 klicev na uro). Napadalci so uporabljali klicne identifikacije obstoječih podjetij ter klicne identifikacije neobstoječih številk (kar je številne klicane osebe prestrašilo), zvezo pa so vzpostavili le do točke, da je klicana številka pozvonila, nato pa prekinili. Domnevno naj bi bil razlog takega početja preverjanje katere telefonske številke sploh obstajajo (tim. *pinging*), te podatke pa bi napadalci nato lahko prodali marketinškim podjetjem za potrebe nelegalnega oglaševanja (Parnell, 2012).

4. 3. Ali je tak klic mogoče izslediti?

Zaradi zlorab se seveda postavlja vprašanje kako je z izsleditvijo takšnih klicev. Na kratko je odgovor sledeč: teoretično to je mogoče (a tudi to ne vedno), v praksi pa zelo težko. Napadalec se namreč z nekaj triki lahko dobro prikrije.

Zlonamerni klic je potrebno najprej izslediti do izvornega operaterja, ki je napadalcu omogočil medoperaterski dostop, nato pa še preko interneta do dejanskega napadalca. Sledenje izvornemu operaterju je mogoče izvesti tako, da se pri končnem operaterju (torej operaterju žrtve napada) na podlagi tim. CDR zapisa (ang. *call-detail record*, gre za zapis podatkov o telefonskih klicih) skuša ugotoviti od kje (od katerega operaterja) je prišel originalen klic.

Pri tem je potrebno vedeti, da posredovanje klicev med operaterji lahko poteka na dva načina. V prvem primeru, npr. neki manjši operater A pri večjem ponudniku telefonije B zakupi nek nabor telefonskih številk, posredovanje klicev pa nato poteka preko tega večjega operaterja. V primeru klica od operaterja A preko B do končnega operaterja C, bi končni operater C videl, da je klic prišel od operaterja B. Preiskovalci bi nato morali iti do operaterja B in pri njem pridobiti podatke o tem od kje so prišli klici iz njegovega omrežja. Vendar pa ni nujno, da operater B hrani prometne podatke o klicih, ki jih posreduje, saj za te klice hramba prometnih podatkov ni obvezna.

Druga možnost je, da ponudnik telefonije sklene neposredno pogodbo z mednarodnimi ponudniki (tim. *agregatorji*). V tem primeru končni operater vidi le, da je klic prišel iz tujine, ne pa tudi od katerega konkretnega operaterja. Podatke za sledenje je torej potrebno iskati pri agregatorju. Poleg tega gredo pri kakšnih "sivih" ponudnikih telefonije povezave pogosto preko različnih posredniških operaterjev, zato je sledenje izvora takega klica zelo težavno, če že ne povsem nemogoče. Ponudniki na mednarodnem trgu namreč ponujajo povezave različnih kvalitet. Povezave, ki so zelo poceni so navadno preusmerjene preko različnih držav in različnih ponudnikov, to pa preiskovalcem še dodatno oteži izsledite v izvora klica.

3 2. Dispatch Magazine On-Line. The 'SWATing' Pranks. Pridobljeno 20. marca 2012 na <http://www.911dispatch.com/911/swating_pranks.html>.

Podatki o klicu pri končnem operaterju izgledajo približno takole (primer izpisa iz Asterisk telefonske centrale):

```
From: "031xxxxxx" <sip:031xxxxxx@91.xxx.xxx.xxx>;tag=epKK8N443v7Hg
To: <sip:386xxxxxxxx@77.xxx.xxx.xxx:5060>
Call-ID: e34e06b6-b7c7-122f-bf9c-00163e62e8ec
CSeq: 22852192 INVITE
Contact: <sip:mod_sofia@91.xxx.xxx.xxx:5070>
User-Agent: MegaTel
P-Asserted-Identity: "031xxxxxx" <sip:031xxxxxx@91.xxx.xxx.xxx>
```

V prikazanem primeru med podatki o klicu lahko zasledimo več polj. Kot smo pokazali, je polje *From* mogoče enostavno ponarediti. Eno izmed polj, ki nam omogoča ugotavljanje prave identitete klicatelja pa je polje *P-Asserted-Identity*. Gre za polje, ki vsebuje podatek o originalnem klicatelju in na podlagi tega podatka bi bilo mogoče relativno hitro identificirati izvornega operaterja. Vendar pa se je potrebno zavedati, da se ta podatek med posredovanjem klica praviloma ne pošilja končnemu operaterju – uporablja se namreč samo med tim. zaupanja vrednimi omrežnimi vrstniki (ang. *trusted peer*). Poleg tega ga posredniški operaterji lahko tudi odstranijo ali spremenijo.

Če smo torej uspeli izslediti klic do izvornega operaterja, pa s tem še nismo na cilju. V drugem koraku je namreč potrebno izslediti klicatelja, torej osebo, ki se je preko internetne povezave do izvornega operaterja povezala v telefonsko omrežje. To je mogoče storiti preko denarnih nakazil (zakup računa je potrebno plačati) ali preko IP naslova preko katerega se je napadalec povezal na svojega ponudnika telefonije.

Napadalec se sledenju denarnega nakazila lahko izogne tako, da storitve svojemu ponudniku telefonije ne plača s pomočjo kreditne kartice, pač pa preko poštne nakaznice, PayPala ali celo s pomočjo virtualnega denarja BitCoin. Ali pa preprosto uporabi ukradeno kreditno kartico.

Ostane torej še sledenje na podlagi IP naslova. V našem zgoraj opisanem primeru bi preiskovalci zelo verjetno uspeli ugotoviti, da je bila povezava do ponudnika telefonije vzpostavljena iz IP naslova našega VPN strežnika. Potem pa bi bilo potrebno iskati dalje. Napadalec lahko oteži oziroma popolnoma onemogoči forenzično analizo vsebine strežnika tako, da na strežniku šifrira diske, za VPN povezavo pa uporablja posredniške strežnike ali anonimizacijsko omrežje Tor. Prav tako je tudi zakup VPN strežnika mogoče plačati anonimno.

Zaključimo torej lahko, da se napadalec z nekaj znanja in spretnosti lahko dobro prikrije pred preiskovalci in posledično popolnoma anonimno izvaja telefonske klice s spremenjeno klicno identifikacijo. Ostane pa še vprašanje, ali lahko napadalec s spremenjeno klicno identifikacijo zavede tudi preiskovalce, ki imajo dostop do zbirke prometnih podatkov.

4. 4. Kaj pa obvezna hramba prometnih podatkov?

Vsako komunikacijo lahko delimo na dva dela – vsebino komunikacije in prometne podatke. Pri telefonskem pogovoru je vsebina komunikacije sam zvočni zapis pogovora, prometni podatki (ali dejstva o okoliščinah komunikacije) pa so telefonska številka klicočega, telefonska številka klicanega, čas začetka in konca pogovora, v primeru mobilne telefonije morda še lokacija obeh udeležencev, itd.

Leta 2006 sprejeta *Direktiva o obvezni hrambi prometnih podatkov 2006/24/ES* od operaterjev zahteva obvezno hrambo prometnih podatkov telefonskih in internetnih komunikacij. V Sloveniji je direktivo implementiral *Zakon o elektronskih komunikacijah* (*Uradni list RS, št. 13/2007- UPB 1, 102/2007-*

ZDRad, 110/2009, 33/2011) s katero je bila uveljavljena obvezna hramba prometnih podatkov tudi pri nas.

Hramba prometnih podatkov je po našem mnenju sicer sporna iz stališča človekovih pravic, zlasti v povezavi s pravico do zasebnosti (Kovačič, 2010). Zakonodaja o hrambi prometnih podatkov namreč ne zahteva zbiranja podatkov le o posameznikih, ki so česa osumljeni, pač pa zahteva zbiranje podatkov o vseh. To po našem mnenju odpira vprašanje skladnosti z domnevo nedolžnosti, postavlja pa se tudi vprašanje, kako daleč gredo še lahko posegi v zasebnost v imenu varnosti. Če je namreč Evropsko sodišče za človekove pravice leta 1984 v primeru *Malone proti Veliki Britaniji*[4] zapisalo, da so prometni podatki integralni elementi telefonskih komunikacij (in jih zato sme operater telekomunikacij posredovati državnim organom samo na podlagi sodne odredbe ali pristanka naročnika), obvezna hramba prometnih podatkov vzpostavlja povsem drugačne standarde.

Kritiki pa s(m)o poleg pravne spornosti tega ukrepa opozarjali tudi na dejstvo, da je ta ukrep razmeroma neučinkovit (Huš, 2012). Nemški inštitut Max Planck je namreč v študiji, ki so jo leta 2011 opravili po naročilu nemškega pravosodnega ministrstva ugotovil, da hramba prometnih podatkov ne pripomore k večji preiskanosti kaznivih dejanj, niti nima preventivnih učinkov (Kilchling et. al. 2011). Vprašanje je torej ali je obvezna hramba prometnih podatkov smiselna tako iz vidika učinkovitosti boja proti kriminalu kot tudi iz stališča varstva človekovih pravic.

Kakorkoli že, ker veljavna zakonodaja zahteva, da mobilni operaterji hranijo prometne podatke svojih strank. Tako smo 27. februarja 2012 Simobil zaprosili za izpis lastnih prometnih podatkov (seznam odhodnih, dohodnih in neuspešnih dohodnih in neuspešnih odhodnih klicev) za obdobje od 13. februarja 2012 do 28. februarja 2012 – torej v času, ko se je izvajalo testiranje klicanja s spremenjeno klicno identifikacijo.

Podatki iz zbirke prometnih podatkov so na podlagi 107.č člena ZEKom dostopni preiskovalnim organom na podlagi sodne odredbe. Vendar pa posameznik v skladu s 30. členom *Zakona o varstvu osebnih podatkov (ZVOP-1)* od upravljavca zbirke osebnih podatkov lahko zahteva izpis svojih lastnih osebnih podatkov. Konec koncev gre pri pravici do vpogleda v lastne osebne podatke tudi za ustavno pravico, saj 38. člen *Ustave RS* določa, da ima vsakdo pravico seznaniti se z zbranimi osebnimi podatki, ki se nanašajo nanj. Ker 6. člen ZVOP-1 določa, da je osebni podatek katerikoli podatek, ki se nanaša na posameznika, ne glede na obliko, v kateri je izražen, so torej prometni podatki o klicih tudi osebni podatki.

Seveda je pri posredovanju osebnih podatkov potrebno biti pozoren tudi na varstvo pravic tretjih oseb, kar pomeni, da je potrebno poskrbeti za ustrezno anonimizacijo klicočih številk. *Direktiva 2002/58/ES Evropskega parlamenta in Sveta z dne 12. julija 2002 o obdelavi osebnih podatkov in varstvu zasebnosti na področju elektronskih komunikacij* v 33. členu določa, da lahko države članice od izvajalcev zahtevajo, da ponudijo svojim naročnikom takšno obliko razčlenjenega računa, v katerem je izbrisano določeno število števk klicane številke. Zato slovenski operaterji številke na razčlenjenem računu naročnikom posredujejo na voljo v obliki, ki ne vsebuje prikaza zadnjih treh števk klicanih številk. In po isti logiki lahko operaterji na enak način zabrišejo tudi podatke o klicočih številkah iz zbirke prometnih podatkov, ki jih na podlagi ZVOP-1 posredujejo posameznikom.

Na podlagi zahteve za izpis prometnih podatkov smo od našega operaterja (Simobil) 8. marca 2012 pridobili izpis podatkov o dohodnih in odhodnih klicih. Na izpisku se nahaja samo seznam klicev, kjer je bila zveza vzpostavljena, saj naj Simobil po ustnem zagotovilu zaposlenih na naročniškem oddelku ne bi beležil podatkov o neuspešnih klicih.

4 Malone v. Velika Britanija, odločba z dne 02. 08. 1984.

Pri testiranju klicanja s spremenjeno klicno identifikacijo smo 25. februarja 2012 zvečer večkrat zaporedno klicali na naš mobilni telefon v omrežju Simobil z naslednjimi spremenjenimi klicnimi identifikacijami: 040/111-111, 040/222-222, 040/333-333, 040/444-444, 040/555-555, 040/666-666, 040/777-777, 040/888-888 in 040/999-999. Pri klicih identifikacijo 222-222, 444-444, 666-666 ter 888-888 pa smo tudi vzpostavili zvezo za nekaj sekund.

25.02.2012	23:41:22	0:00:04	0	SVNSM-Si.mobil	38640222xxx	In
25.02.2012	23:43:21	0:00:02	0	SVNSM-Si.mobil	38640444xxx	In
25.02.2012	23:45:04	0:00:02	0	SVNSM-Si.mobil	38640666xxx	In
25.02.2012	23:46:37	0:00:02	0	SVNSM-Si.mobil	38640888xxx	In

Slika 8: Izpisek seznama dohodnih klicev 25. februarja 2012 zvečer.

Iz Simobilovega izpiska se – kljub temu, da so zadnje tri številke klicoče številke zabrisane – jasno vidijo vzpostavljeni klici iz navedenih dohodnih številk v času od 23:41 do 23:46. To torej pomeni, da operater dejansko zabeleži klicno identifikacijo, ki jo nastavimo sami in ne prave klicne identifikacije.

Zaključimo lahko, da je na podatke v zbirki prometnih podatkov o telefonskih klicih pri operaterju mogoče vplivati, oziroma podatke ponarediti tako, da ne prikazujejo dejanskega stanja (prave identitete klicatelja). Kaj to pomeni za dokazno vrednost teh podatkov, pa si ni težko zamisliti.

5. Varnost GSM telefonije in prometni podatki v mobilni telefoniji

V sredini leta 2012 smo avtorji Jaka Hudoklin, Matej Kovačič in Klemen Rupnik ob pomoči Primoža Brataniča izvedli varnostno analizo slovenskih GSM omrežij. Varnostno analizo smo opravili v prvi polovici leta 2012, njen namen pa je bil opozoriti na varnostne ranljivosti v slovenskih GSM omrežjih, ki omogočajo nepooblaščeno prestrezanje mobilnih komunikacij in ponarejanje prometnih podatkov v mobilni telefoniji. Raziskava pa je tudi pokazala na nekatere zaskrbljujoče možnosti vplivanja na točnost in pravilnost prometnih podatkov o telefonskih klicih v GSM omrežjih.

Posebej poudarjamo, da smo pri izvedbi varnostne analize pazili na zakonitost izvedbe le-te. Tako smo uporabljali atestirano opremo (mobilni telefon, ki ga nismo stojno predelali), prestrezali pa smo izključno lastne komunikacije. Za potrebe varnostnega pregleda smo namreč kupili več SIM kartic različnih operaterjev, prestrezanje komunikacij pa smo izvedli le pri izmenjavi SMS sporočil med temi SIM karticami.

Prva faza pregleda je obsegala poslušanje tim. tehničnih sporočil omrežja mobilnim telefonom na tim. "broadcast kanalu" (BCCH kanal). Gre za sporočila, ki jih omrežje pošilja vsem telefonom (tudi tistim, ki še niso povezani v omrežje). V nadaljevanju smo enemu izmed naših mobilnih telefonov (tim. tarči) pričeli pošiljati tiha SMS sporočila (gre za SMS sporočila, ki jih mobilni telefon ne prikaže uporabniku) oz. ga začeli klicati. Hkrati smo na tim. "broadcast kanalu" gledali kateri TMSI številki bo mobilno omrežje posredovalo zahtevek za posredovanje SMS sporočila oz. zahtevek za sprejem klica. Lociranju napačne TMSI številke smo se dodatno izognili tako, da smo identificirali le tiste TMSI številke, kjer smo lahko zaznali SABM (*Set Asynchronous Balance Mode*) sporočila. Gre za sporočila, ki se prenašajo po tim. navzgornji povezavi in smo jih z našo opremo lahko zaznali le v oddaljenosti 2 metra od tarče. S tem smo zagotovili, da ni bilo mogoče izvesti nepooblaščenega prestrezanja tujih komunikacij, pač pa smo prestrezali le naše lastne komunikacije (naš lasten telefon, ki je bil lahko največ 2 metra oddaljen od opreme za prestrezanje), kar ni nezakonito.

Ko smo identificirali TMSI številko smo počakali na zahtevo za preklop na podatkovni kanal in nato tej zahtevi sledili - preklopili na podatkovni kanal, kjer je naš telefon prejel šifrirane podatke (SMS sporočilo).

Nad šifriranimi podatki smo nato izvedli kriptoanalizo. Gre za uporabo posebnih matematičnih postopkov, ki nam omogočajo rekonstrukcijo sejnega šifrirnega ključa Kc, ki se uporablja za šifriranje podatkov v GSM omrežju med uporabnikom in bazno postajo. Ta ključ izvira iz SIM kartice (iz Ki ključa), ni pa zapisan na njej. S postopkom kriptoanalize smo se torej izognili kloniranju SIM kartice oziroma dostopa do SIM kartice sploh nismo potrebovali. S pomočjo rekonstruiranega šifrirnega ključa smo nato dešifrirali SMS sporočilo, ki smo ga iz našega prvega telefona poslali na naš drugi mobilni telefon.

Poudarjamo tudi, da smo se pri izvajanju varnostne analize izognili povzročanju kakršnihkoli motenj v omrežju. Rezultate varnostne analize smo objavili v več člankih, da pa bi preprečili morebitne zlorabe, so bili članki napisani tako, da ponovitev opisanih postopkov ni mogoča na enostaven način.

5. 1. Potrebna oprema

Za izvedbo varnostne analize GSM omrežja je potrebno imeti ustrezno strojno in programsko opremo. Za izvedbo analize smo uporabili strojno in programsko opremo, ki smo jo pripravili in

predelali sami. Strojni del opreme obsega točno določen starejši model mobilnega telefona (ki ga je mogoče rabljenega kupiti za nekaj deset EUR na spletu). Kot programski del opreme pa smo uporabili posebej prilagojeno strojno programsko opremo, ki omogoča nefiltrirano sprejemanje signalov in predvsem sporočil v GSM omrežju. Gre za brezplačno in odprtokodno programsko opremo OsmocomBB, ki je prosto dostopna na spletu. Za potrebe našega pregleda smo jo na več mestih temeljito predelali.

Slika 9: Strojna oprema za zajem in analizo GSM podatkov.

Uporaba te strojne in programske opreme nam omogoča prestrezanje (šifriranih) mobilnih komunikacij v GMS omrežju. Z njo lahko mobilne komunikacije uporabnika posredujemo računalniku, same vsebine pa ne moremo videti, saj je šifrirana.

5. 2. Kriptoanaliza

V mobilni telefoniji se za šifriranje komunikacij med telefonom in bazno postajo uporablja več šifrirnih algoritmov.

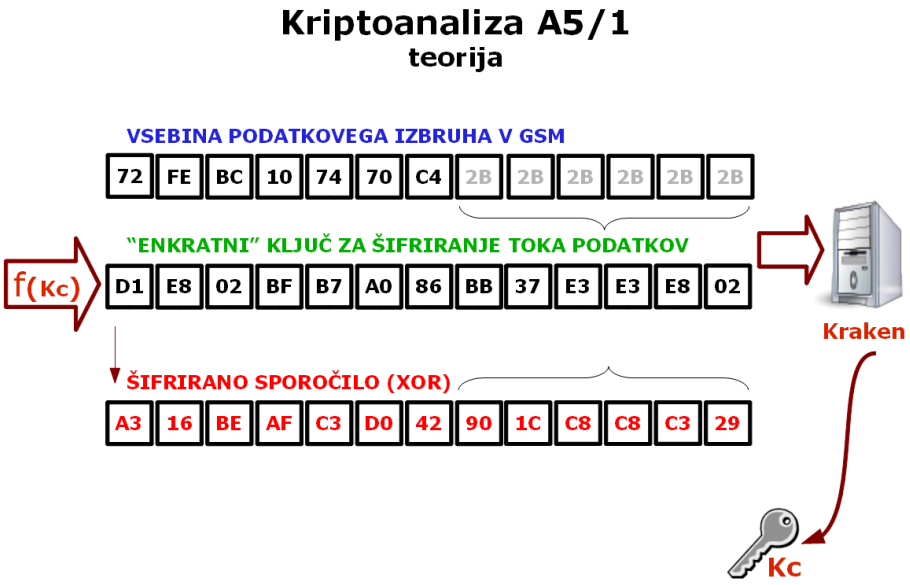
V osnovi sta bila za šifriranje pogovorov razvita algoritem A5/1 (ki omogoča močnejše šifriranje) in algoritem A5/2 (ki omogoča šibkejše šifriranje podatkov). Kasneje sta bila razvit še algoritma A5/3 in A5/4, ki sta precej močnejša kot A5/1. Prenos pogovorov ali SMS sporočil v GSM omrežju lahko poteka tudi nešifrirano - včasih se zato navaja, da se za prenos uporablja "šifrirni" algoritem A5/0.

Vendar pa je s sodobno tehnologijo in sodobno matematično analizo nekatere šifrirne algoritme, ki se uporabljajo v GSM omrežjih mogoče zlomiti. To pomeni, da je podatke šifrirane s temi algoritmi mogoče dešifrirati brez predhodnega poznavanja šifrirnega ključa. S tem se ukvarja posebna znanstvena disciplina – kriptoanaliza.

Težava je v tem, da so bili nekateri šifrirni algoritmi, ki se v GSM omrežju uporabljajo za zaščito vsebine komunikacij razviti z vgrajenimi varnostnimi ranljivostmi. Šifrirni algoritem A5/1 je bil razvit leta 1987, A5/2 pa leta 1989 in sicer kot oslabljena različica algoritma A5/1. Oba algoritma sta bila razvita na skrivaj (brez odprtega sodelovanja mednarodne znanstvene javnosti) in ob sodelovanju tajnih služb, po mnenju nekaterih (prof. Rossa Andersona iz University of Cambridge), pa je bila šibka zasnova algoritmov namerna.

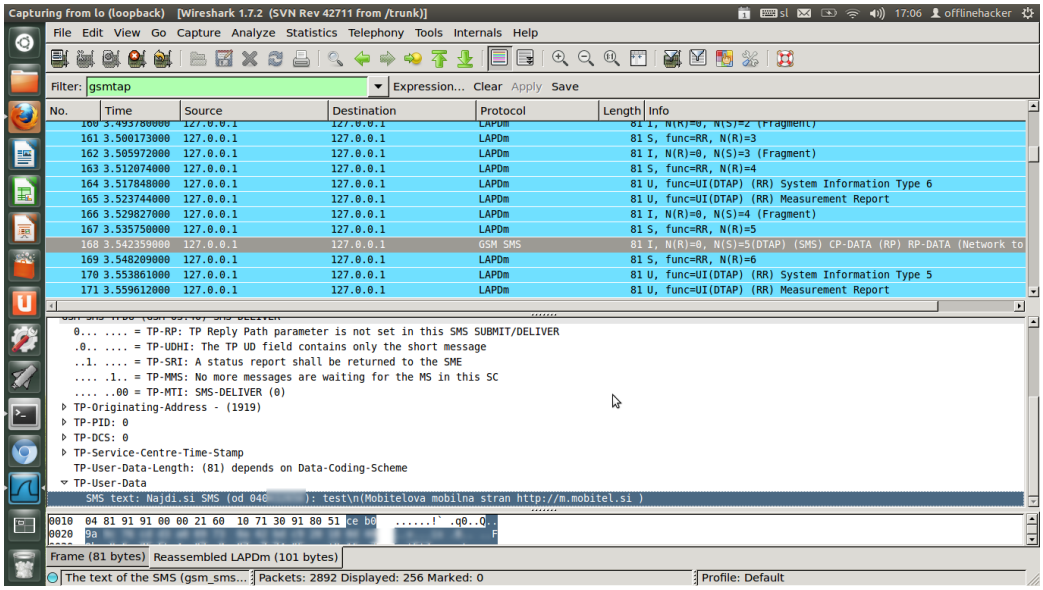
Tako ne preseneča, da je mogoče varnost šifrirnega algoritma A5/1, ki se še vedno uporablja v nekaterih slovenskih GSM omrežjih, relativno hitro zlomiti.

V postopku raziskave varnosti slovenskih GSM omrežij smo prestrežene podatke v šifrirani obliki s pomočjo razmeroma zapletenih, a na internetu javno objavljenih matematičnih postopkov kriptoanalize, izvedli rekonstrukcijo sejnega šifrirnega ključa Kc, ki se uporablja za šifriranje podatkov v GSM omrežju med uporabnikom in bazno postajo. Sejni šifrirni ključ je za vsakega uporabnika drugačen in se občasno tudi spreminja. Sejnega ključa enega uporabnika tako ni mogoče uporabiti za dešifriranje mobilnih komunikacij drugega uporabnika. Še več, ko se sejni šifrirni ključ spremeni (npr. ob tim. lokacijski posodobitvi, oziroma vedno ko mobilno omrežje to zahteva), starega sejnega šifrirnega ključa ni mogoče uporabiti za dešifriranje novejših komunikacij danega uporabnika.



Slika 10: Kriptoanaliza GSM podatkov.

S pomočjo matematične rekonstrukcije sejnega šifrirnega ključa (postopek traja od 30 sekund do nekaj ali nekaj deset minut – odvisno od zmogljivosti računalnika), je nato mogoče dešifrirati šifrirana SMS sporočila mobilnega uporabnika oziroma poslušati njegove govorne klice. To seveda velja samo v omrežjih, ki za zaščito uporabljajo šifrirni algoritem A5/1.



Slika 11: Dešifrirano SMS sporočilo.

5. 3. Prevzemanje mobilne identitete drugega uporabnika

V nadaljevanju varnostne analize pa smo tudi ugotovili, kako je mogoče v mobilnem omrežju prevzeti mobilno identiteto drugega uporabnika in tako v njegovem imenu in na njegov račun vzpostavljati govorne klice in pošiljati SMS sporočila, v določenih okoliščinah pa tudi sprejemati klice in SMS sporočila namenjena njemu.

Pri vsem tem pa operater zabeleži tudi napačne prometne podatke o telefonskih klicih, saj operater ne zmore ločiti med klici legitimnega uporabnika in klici, ki jih je v njegovem imenu izvedel napadalec. Posebej zaskrbljujoče je tudi dejstvo, da se poleg običajnih podatkov o klicih (številka klicočega, številka klicane osebe, itd.) v zbirki prometnih podatkov zabeleži tudi (lažna) lokacija mobilnega uporabnika.

Naj pa poudarimo, da so po našem opozorilu nekateri operaterji svoja omrežja varnostno nadgradili, tako da opisani postopek sedaj ne deluje več.

Mobilni uporabnik se v mobilnem omrežju ne identificira s svojo telefonsko številko, pač pa so za njegovo identifikacijo potrebni štirje parametri: IMSI številka, TMSI številka, sejni šifrirni ključ Kc in sekvenčna številka sejnega šifrirnega ključa (ang. *key sequence number*).

Pri ugotavljanju identitete mobilnih telefonov si v prvem koraku lahko pomagamo s SS7 omrežjem. Gre za omrežje (in signalni protokol), preko katerega se med seboj povezujejo vsi mobilni operaterji, omogoča pa (med drugim) tudi vpoglede v nekatere informacije o naročnikih mobilne telefonije iz tim. domačega registra (HLR - *Home Location Register*), ki ga za svoje naročnike vzdržuje posamezni operater.

Omrežje sicer ni javno dostopno, a na spletu obstajajo ponudniki, ki omogočajo HLR vpoglede (ang. *HLR lookup*) za zelo dostopno ceno (nekaj centov) na vpogled. Ponudniki omogočajo, da s pomočjo telefonske številke pridobimo IMSI številko uporabnika, kodo države (MCC) in omrežno kodo (MNC) njegovega operaterja, ime domačega operaterja in države le tega ter kodo MSC centra (*Mobile switching center*).[5]

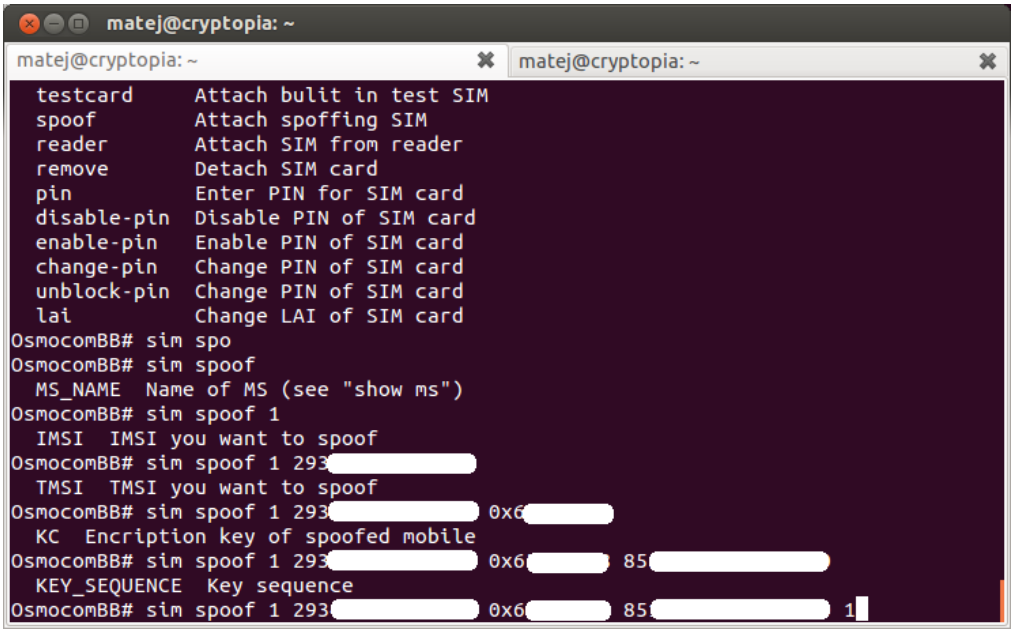
Tako je na podlagi telefonske številke s pomočjo vpogleda v HLR register preko spleta mogoče na zelo enostaven način identificirati IMSI številko mobilnega uporabnika.

Za uspešno prevzemanje mobilne identitete uporabnika pa je potrebno identificirati oziroma rekonstruirati še ostale tri zgoraj navedene parametre.

TMSI številko lahko identificiramo s pomočjo pošiljanja tihih SMS sporočil, sejni šifrirni ključ Kc lahko rekonstruiramo s pomočjo kriptoanalize (če omrežje za šifriranje podatkov uporablja šifrirni algoritem A5/1), sekvenčno številko sejnega šifrirnega ključa pa preberemo iz komunikacijskih paketov, ki jih GSM omrežje pošilja mobilnemu uporabniku.

Za potrebe naše raziskave smo na naš mobilni telefon na katerem je tekla OsmocomBB strojna programska oprema naložili posebno aplikacijo, ki omogoča vzpostavljanje govornih klicev in pošiljanje SMS sporočil, aplikacijo pa smo predelali na tak način, da nam omogoča prevzemanje identitete drugega uporabnika v mobilnem omrežju. Pri tem je seveda v aplikacijo potrebno ročno vpisati ustrezne zgoraj navedene podatke oziroma parametre, s katerimi se mobilni telefon predstavi omrežju.

5 MSC koda nam omogoča tudi grobo lociranje uporabnika mobilnega telefona. S pomočjo MSC kode lahko ugotovimo v kateri državi oziroma na katerem območju posamezne države se nahaja dani uporabnik mobilnega telefona. Postopka lociranja oz. HLR vpogleda mobilni uporabnik ne more zaznati.



Slika 12: Prevzemanje mobilne identitete drugega uporabnika.

Na ta način smo uspeli vzpostaviti govorni klic z identiteto drugega mobilnega uporabnika, prav tako pa smo uspeli z identiteto drugega mobilnega uporabnika poslati SMS sporočilo. Potreben čas za to je nekaj minut – časovno najbolj zahteven je postopek kriptoanalitične rekonstrukcije sejnega šifrirnega ključa Kc. Naj pa omenimo, da mora biti napadalec v primeru tega postopka prijavljen na isto bazno postajo kot napadeni uporabnik, torej se mora napadalec fizično nahajati v bližini uporabnika katerega mobilno identiteto želi prevzeti (do nekaj sto metrov oziroma do nekaj kilometrov).

Na enak način bi lahko v imenu in na račun drugega uporabnika izvedli npr. storitev plačila, mogoče pa je tudi prevzemanje dohodnih klicev in SMS sporočil, kar smo tudi preiskusili. Varnostni pregled je tudi pokazal, da je prevzemanje mobilne identitete še posebej enostavno v omrežjih, ki dovolijo izklop šifriranja oziroma uporabo tim. A5/0, saj je tam mogoče uporabiti izmišljen sejni šifrirni ključ Kc in zamudna kriptoanaliza ni potrebna. To varnostno ranljivost so sicer slovenski operaterji mobilne telefonije po našem opozorilu nemudoma odpravili.

5. 4. Posledice za obvezno hrambo prometnih podatkov

Postopek prevzemanja mobilne identitete se od postopka klicanja s spremenjeno klicno identifikacijo (opisanega v četrtem poglavju) bistveno razlikuje.

Pri klicu s spremenjeno klicno identifikacijo operater vsaj teoretično lahko zabeleži oz. zazna dejstvo, da klic izvira izven njegovega omrežja. Poleg tega se tak klic ne zaračuna uporabniku, katerega identiteta je bila prevzeta. V primeru mobilne telefonije v bazi prometnih podatkov tudi ne bodo zabeleženi nekateri podatki, npr. lokacija mobilnega telefona, itd. kar preiskovalcem lahko predstavlja namig, da zabeleženi prometni podatki morda niso verodostojni.

Pri klicih, opravljenih s pomočjo prevzemanja mobilne identitete drugega uporabnika, pa operater v bazi prometnih podatkov zabeleži izvor klica v svojem omrežju, zabeleži tudi lokacijo (napadalca) in stroške klica dejansko obračuna napadalčevi tarči. Uporabnik katerega mobilna identiteta je bila prevzeta bo tako zelo težko dokazal, da klica ni opravil on, saj prav vsi podatki iz operaterjeve zbirke prometnih podatkov kažejo nasprotno.

6. Sklep

Varnostna analiza slovenskih GSM omrežij je po našem mnenju pokazala zaskrbljujoče varnostne pomanjkljivosti pri slovenskih mobilnih operaterjih. Z izrabo odkritih ranljivosti bi napadalec lahko nepooblaščeno, predvsem pa nezaznavno (opisani postopek prestrezanja je namreč povsem pasiven) prestrezal vsebino SMS sporočil in pogovorov v 2G omrežju, izvajal sledenje uporabnikom ali s pomočjo kraje identitete mobilnega uporabnika le-temu povzročal neupravičene stroške ali ga celo spravil v kazenski pregon. Odkrite varnostne pomanjkljivosti so po našem mnenju v slovenskih GSM omrežjih omogočale nepooblaščeno prestrezanje komunikacij tako s strani kriminalnih združb kot tudi tujih ter domačih varnostno-obveščevalnih organov.

Rezultate varnostne analize smo zato predstavili v več člankih (na voljo so tudi videoponsketki s prikazom izvedbe opisanih postopkov) in na nekaj strokovnih konferencah, s podrobnostmi pa smo seznanili tako operaterje kot nekatere državne organe (policijo, APEK, Informacijskega pooblaščenca).

Odzivi operaterjev so bili različni. Predstavniki enega izmed operaterjev so zaprosili za nekatere dodatne informacije ter z veseljem sprejeli naše predloge za izboljšanje varnosti. Eden od operaterjev se razen z nekaj kratkimi sporočili za javnost na naše ugotovitve ni odzval. Odzivi tretjega operaterja pa so bili bistveno drugačni - najprej so preko svoje službe za stike z javnostjo razkrite ranljivosti večkrat izrecno zanikali, deležni pa smo bili tudi nekaterih groženj s civilnim in kazenskim pregonom. Naj tudi poudarimo, da za izvedbo raziskave in svetovanje glede izboljšanja varnosti nismo dobili, niti zahtevali ali pričakovali kakršnegakoli plačila od kogarkoli.

Po naših opozorilih so skoraj vsi operaterji izboljšali varnost svojih omrežij in da sedaj slovenskim uporabnikom mobilne telefonije zagotavljajo višjo stopnjo varnosti in zaupnosti njihovih komunikacij. Kljub temu pa ugotavljamo, da navedeni ukrepi zlasti s strani določenih operaterjev niso bili zadostni, zato je nezakonito prestrezanje komunikacij z relativno poceni opremo v določenih okoliščinah še vedno mogoče.

* * *

Po drugi strani pa smo z navedenimi raziskavami pokazali na resne pomanjkljivosti pri hrambi prometnih podatkov v telefoniji oziroma prikazali, da je njihova verodostojnost lahko zelo vprašljiva.

V današnjem času – še bolj pa bo to veljalo v prihodnosti – je sodiščem predloženih čedalje več dokazov v digitalni obliki. Za razliko od drugih vrst dokazov pa sodišča (in enako velja za preiskovalce) digitalne dokaze, zlasti računalniško ustvarjene, preveč samoumevno dojemajo kot zaupanja vredne, nepristranske in zanesljive. Da temu ni tako, smo pokazali na primeru forenzične analize SIM kartic ter tudi na primeru prometnih podatkov v mobilni telefoniji.

Kot smo prikazali v prispevku, so (bili) stroški za izvajanje opisanih postopkov minimalni, digitalne dokaze v zbirki prometnih podatkov pa je (bilo) mogoče ponarediti v nekaj minutah. Ta ugotovitev pa ima seveda posledice tudi za kazenski postopek.

Dejstvo namreč je, da računalniki že dolgo časa niso več zgolj »stroji« (že sama beseda *stroj* predpostavlja razmeroma zanesljivo, mehansko napravo), ki bi jim veljalo slepo zaupati. Pri obravnavi digitalnih in računalniško ustvarjenih dokazov bi bilo namreč potrebno vedno pomisliti tudi na možnost, da so spremenjeni ali ponarejeni in se znebiti predpostavk na katerih temelji zaupanje vanje.

Rezultati navedenih raziskav in video prikazi

1. Slepo zaupanje digitalnim dokazom – primer SIM kartic, 13. januar 2012, <http://hr-cjpc.si/pravokator/index.php/2012/01/13/slepo-zaupanje-digitalnim-dokazom-primer-sim-kartic/>.
2. Ko pokličejo hekerji – spreminjanje klicne identifikacije telefonskih klicev, 18. marec 2012, <http://hr-cjpc.si/pravokator/index.php/2012/03/18/ko-poklicejo-hekerji-spreminjanje-klicne-identifikacije-telefonskih-klicev/>.
3. Varnost slovenskih GSM omrežij, 16. juij 2012, <http://hr-cjpc.si/pravokator/index.php/2012/06/16/varnost-slovenskih-gsm-omrezij/>.

Viri in literatura

1. Bratus, Ashlyn in Shubina. 2010. Software on the Witness Stand: What Should It Take for Us to Trust It? Pridobljeno 20. marca 2012 na <http://www.cs.dartmouth.edu/~sergey/trusting-e-evidence.pdf>.
2. Dispatch Magazine On-Line. The 'SWATing' Pranks. Pridobljeno 20. marca 2012 na <http://www.911dispatch.com/911/swating_pranks.html>.
3. Goldberg in Briceno. 1998 GSM Cloning. Pridobljeno 20. marca 2012 na <http://www.isaac.cs.berkeley.edu/isaac/gsm-faq.html>.
4. Huš. 2012. Študija: hramba prometnih podatkov ne pomaga pri preiskavi kaznivih dejanj. Pridobljeno 20. marca 2012 na <https://slo-tech.com/novice/t504584>.
5. Kilchling et. al. 2011. Schutzlücken durch Wegfall der Vorratsdatenspeicherung? Pridobljeno 20. marca 2012 na <http://www.bmj.de/SharedDocs/Downloads/DE/pdfs/20120127_MPI_Gutachten_VDS_Langfassung.pdf?__blob=publicationFile>
6. Kovačič. 2010. Nemško ustavno sodišče razveljavilo obvezno hrambo prometnih podatkov v Nemčiji. Pridobljeno 20. marca 2012 na <http://hr-cjpc.si/pravokator/index.php/2010/03/05/nemsko-ustavno-sodisce-razveljavilo-obvezno-hrambo-prometnih-podatkov-v-nemciji/>
7. Krebs. 2012. Busy Signal Service Targets Cyberheist Victims. Pridobljeno 20. marca 2012 na <https://krebsonsecurity.com/2011/12/busy-signal-service-targets-cyberheist-victims/>
8. Parnell. 2012. Thousands of Brits bombarded in caller spoofing riddle. Pridobljeno 20. marca 2012 na <http://www.theregister.co.uk/2012/03/12/caller_id_spoofing_uk/>.
9. Resman. 2009. Napaka v alkotestu. Pridobljeno 20. marca 2012 na <https://slo-tech.com/novice/t358964/0>.

Pravni dokumenti

1. Odločitev Vrhovnega sodišča ZDA v primeru State v. Chun. Supreme Court of New Jersey A-96-06, Docket No. 58,879.
2. Zakon o elektronskih komunikacijah. Uradni list RS, št. 13/2007- UPB 1, 102/2007-ZDRad, 110/2009, 33/2011.
3. Direktiva 2006/24/ES Evropskega parlamenta in Sveta z dne 15. marca 2006 o hrambi podatkov, pridobljenih ali obdelanih v zvezi z zagotavljanjem javno dostopnih elektronskih komunikacijskih storitev ali javnih komunikacijskih omrežij, in spremembi Direktive 2002/58/ES (*Directive 2006/24/EC of the European Parliament and of the Council of 15 March 2006 on the retention of data generated or processed in connection with the provision of publicly available electronic communications services or of public communications networks and amending Directive 2002/58/EC*), sprejeta 14. 12. 2005. Official Journal L 105, 13/04/2006, p. 0054 – 0063.
4. Odločitev Evropskega sodišča za človekove pravice: Malone v. Velika Britanija, odločba z dne 02. 08. 1984.