Zagotavljanje varnosti v celičnih omrežjih

Jernej Mušič, Boštjan Batagelj

Univerza v Ljubljani, Fakulteta za elektrotehniko, Tržaška cesta 25, 1000 Ljubljana
E-pošta: music.jernej@gmail.com

Ensuring security in cellular networks

Abstract. *This paper will discuss the properties of 2G and 4G cellular networks including the main components and authentication process during the primary tracking area update process. The authentication process walkthrough will show us the main security risks of previous generations of cellular networks and their negative influence on newer generations which inherit them. Inheriting these security risks show the negative side of providing backward compatibility to users which is one of the goals the provider wants to achieve during implementation. Security risks which are discussed in this paper will be listed and complimented with security solutions which have emerged during the years. Some of these are provided as integrated solutions where the whole cellular infrastructure and authentication is changed and is therefore in theory the responsibility of each provider to implement them.*

1 Uvod

S postopnim uvajanjem mobilnega omrežja pete generacije (5G) se soočamo s problematiko varnosti omrežja, predvsem z vidikov kakšne spremembe na tem področju prinaša nova generacija celičnega omrežja in ali bo ta podedoval ranljivosti prejšnjih generacij. V prispevku se osredotočimo na četrto generacijo (4G/LTE) celičnih omrežij ter na ranljivosti v protokolu, ki omogočajo potencialnemu napadalcu zlorabo celovitosti, integritete in dostopnosti omrežja.

Potrebno se je zavedati, da je LTE še vedno izpostavljen ranljivostim omrežjem predhodnih generacij. V nadaljevanju bomo za razumevanje omenjenih slabosti opisali protokol navezovanja in vanj umestili možnosti napadov. Od možnih napadov se bomo osredotočili tudi na uporabo naprav za prestrezanje celične komunikacije . Omenjene naprave namreč izkoriščajo ranljivosti protokolov omrežij prejšnje generacije, zato bomo v prispevku opisali tudi oblike napada le-teh.

2 Protokoli in gradniki v celičnem omrežju

Temeljni cilj ponudnikov ob vzpostavljanju novih generacij celičnega omrežja je skrb za nemoteno delovanje storitev, z namenom zagotavljanja kakovostne uporabniške izkušnje. Ob vzpostavljanju nove generacije celičnega omrežja se le to zaradi več razlogov vzpostavlja postopoma. V prvi vrsti se ob vzpostavitvi novih tehnologij ustvari cela veriga naprav, ki so zastarela oz. ne ustrezajo novemu standardu. Kot se je pokazalo že v preteklosti, je ob izgradnji nove generacije omrežja nujno potrebno stare tehnologije integrirati v novo generacijo. Z zagotavljanjem združljivosti s starejšo tehnologijo nova generacija podeduje tudi prednosti in slabosti prejšnje generacije, vključno s varnostnimi težavami. V tem prispevku bomo zato tudi obravnavali komponente in postopek preverjanja istovetnosti identitete v omrežju 2G in 4G, tipe najbolj pogostih napadov na omrežje 4G in varnostne izzive, ki jih je ta podedoval od svojih predhodnikov.

2.1 Gradniki omrežja 2G

Omrežje GSM je sestavljeno iz naslednjih osnovnih komponent, in sicer:

Mobilne postaje (ang. mobile station – MS) so kakršnekoli naprave, ki vsebujejo odstranljive Subscriber Identification Module (SIM) kartice [1]. V splošnem to velja za mobilne telefone in ostale naprave, ki omogočajo povezovanje z mobilnim omrežjem. MS-ju je dodeljen tudi unikatni identifikator (ang. International Mobile Equipment Identification – IMEI), ki v primeru odtujitve omogoča omrežju identifikacijo in zavračanje povezovanja naprave v omrežje [1].

Bazne postaje (ang. base stations – BS), ki direktno komunicirajo z MS in upravljajo celico v celičnem omrežju. Velikost celice je odvisna od geografskih značilnosti terena in gostote uporabnikov. Celice so manjše v gosto poseljenih območjih, kjer je večje število porabnikov. BS zagotavljajo tudi šifriranje in dešifriranje podatkovne komunikacije [1].

Krmilnik baznih postaj (ang. Base Station Controller – BSC) upravlja množico BS. Opravlja postopek predaje MS iz ene BS na drugo v primeru prehoda iz ene celice v drugo [1]. Njihova naloga je torej zagotavljati kakovosten prehod MS brez prekinitev v komunikaciji.

Preklopni center za mobilne usluge (ang. Mobile Services switching Center – MSC) upravlja mobilnost storitev in je zadolžen za usmerjanje telekomunikacijskih storitev ter komuniciranje z zunanjimi omrežji [1]. V njegovi sestavi so tudi naslednje podatkovne baze:

Register lokacij MS (ang. Home Location Register – HLR), vsebuje vse podatke o uporabnikih in njihovi dodeljeni mednarodni identiteti (ang. International Mobile Subscriber Identity – IMSI). Vsako omrežje ima samo en register lokacij MS [1].

Register lokacij gostujočih uporabnikov (ang. Visitor Location Register – VLR), je dodeljen posameznemu preklopnemu centru mobilnih uslug in

vsebuje podatke o uporabnikih, ki spadajo v območje odgovornosti posameznega MSC [1].

Register naprav (ang. Equipment Identity Register – EIR), vsebuje podatke o MS, ki nimajo dovoljenja za dostop do omrežja. V tem primeru gre za IMEI naprav, ki so bile prijavljene kot odtujene ali prepovedane [1].

Avtentikacijski center (ang. Authentication Center – AuC), vsebuje uporabniške podatke za dostop do omrežja, ki so tudi hranjeni v SIM, in sicer skriti ključ K_i[1, 2].

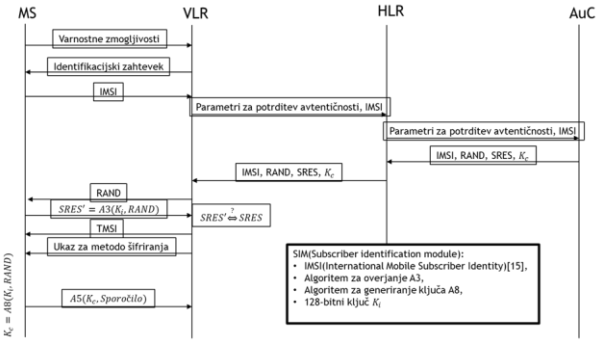
2.2 Postopek avtentikacije v omrežju 2G

MS se ob vklopu želi povezati z omrežjem, kar izvede z zahtevkom za povezavo na omrežje, del katerega je tudi nabor varnostnih zmogljivosti naprave. [1] V tem koraku je potrebno poudariti, da varnostne zmogljivosti MS zaostajajo za potrebami, še posebej na hitro rastočem in konkurenčnem trgu. Te razlike se sicer zmanjšujejo, vendar pa omogočanje uporabe predhodnih algoritmov za šifriranje kljub odkritim ranljivostim v omrežju predstavlja resen varnostni izziv. Vsaka MS ima vgrajen protokol A5, ki ga uporablja za šifriranje komunikacijskih podatkov. MS posreduje zahtevek za povezavo, ki vključuje varnostne zmogljivosti naprave, preko BS v VLR. Ta odgovori MS z zahtevkom po identificiranju s svojo številko IMSI, ki jo pošlje preko omrežja v odprti oz. nešifrirani obliki. VLR nato sestavi zahtevek za avtentikacijo uporabnika na podlagi prejete številke IMSI do registra lokacij mobilnih postaj (HLR), ki preveri uporabnika in od avtentikacijskega centra (AuC) zahteva generiranje naključnega 128-bitnega števila, imenovanega RAND. AuC nato na podlagi števila RAND in ključa K_i v algoritmu A3 izračuna 32-bitni odgovor imenovan SRES (ang. Signed RESponse). Ključ K_i in algoritma A3 in A8 se tudi nahajata v kartici SIM v MS. V naslednjem koraku AuC s pomočjo algoritma A8 in števila RAND izračuna 64 bitni sejni ključ K_C. SRES, RAND in K_C nato posreduje v VLR, ki do MS posreduje le RAND. S podatki, ki jih ima MS shranjene na SIM, izračuna svoj odziv SRES ter ga posreduje v VLR. Na tem mestu se obe različici SRES primerjata in v primeru ujemanja VLR dodeli MS številko TMSI (ang. Temporary Mobile Subscriber Identification) ter katero različico šifriranja A5 uporabiti. Kot je vidno na Slika 1, MS nato generira lasten sejni ključ K_C, ki ga uporablja v izbrani različici šifriranja A5. [1, 2] IMSI se torej izpostavi omrežju le med začetnim navezovanjem MS in po poteku veljavnosti TMSI, ki je namenjen onemogočanju sledenja uporabnikom storitev.

Simetrični tokovni šifrirni algoritem v rabi za šifriranje uporabniških komunikacijskih podatkov, se imenuje A5 in je vgrajen v vsak MS. Zasnova različic A5 je v osnovi enaka in se razlikuje le v generiranju psevdonaključnega 228-bitnega toka ključev. Za generiranje le-tega, algoritem prejme sejni ključ K_C, ki ga MS generira po uspešni avtentikaciji in števec okvirjev F_n. Ta je nato skupaj z 228-bitnim segmentom odprtih podatkov poslan skozi funkcijo izključujoči ALI (XOR), katere rezultat je 228-bitni tok šifriranih podatkov. Edina razlika med različnimi tipi A5 algoritma je način generiranja psevdonaključnih 228-bitov (GEN), medtem ko je XOR funkcija skupna. [3]

MS imajo na voljo naslednje različice A5 šifriranja:

A5/0, ki splošno predstavlja komunikacijo brez uporabe šifriranja se uporablja v državah, ki so pod sankcijami Združenih narodov in ostalih državah tretjega sveta. Uporaba A5/0 se v tem primeru ne zdi smiselna, saj je to eden od možnih vektorjev napada na omrežje. Njen namen je torej odpravljanje tehničnih težav ali preobremenjenosti v omrežju s strani ponudnika oz. upravitelja omrežja. [2, 3]



Slika 1: Postopek avtentikacije MS v omrežje 2G [1]

A5/1 generira tok ključev s pomočjo treh pomikalnih registrov z linearno povratno vezavo (LFSR), kjer ima vsak LFSR določene prioritetne bite, ki predstavljajo njihov status [3].

A5/2 je manj varna različica šifriranja, ki je bila izdelana zaradi lokalnih omejitev v nekaterih državah in velja za razbito in je zato njena raba tudi odsvetovana. [3]

A5/3 ali KATSUMI je različica s tokovnim šifrirnim algoritmom, ki temelji na blokovnem algoritmu MISTY. Vsebuje 64-bitne bloke, 128-bitni ključ in kompleksne rekurzivne Feistel-ove strukture z osmimi koraki. Znane so nekatere delne analize šifriranja A5/3, medtem ko algoritem do sedaj še ni bil razrešen v celoti ali vsaj ne v realnem času.[4]

2.3 Gradniki omrežja 4G

Struktura celičnega omrežja 4G se po osnovni zasnovi bistveno ne razlikuje od 2G. Pri 4G se nekateri gradniki združujejo, kar samo strukturo naredi manj kompleksno. Struktura omrežja 4G je sledeča:

Uporabniška oprema (ang. User Equipment – UE), predstavlja mobilno napravo, ki jo uporablja uporabnik za povezovanje z mobilnim omrežjem. Ta vsebuje univerzalno kartico z integriranim vezjem (ang. Iniversal Integrated Circuit Card – UICC) s pripadajočo programsko opremo in univerzalnim modulom z identiteto uporabnika (ang. Universal Subscriber Identification Module – USIM). USIM vsebuje enake podatke kot SIM pri omrežju 2G in sodeluje pri avtentikaciji UE ob vstopu v omrežje. Modul posreduje podatke o uporabniku, in sicer njegovo številko IMSI, skriti ključ in identifikacijsko številko mobilnega naročnika (ang. Mobile Subscriber Identification Number – MSIN). Iste podatke vsebuje tudi AuC v domačem omrežju za namene avtentikacije. [5]

Vozlišča (ang. evolved Node B – eNodeB), ki so temeljna komponenta razvitega univerzalno zemeljskega radijskega dostopovnega omrežja (ang.

evolved universal terrestrial radio access network – E-UTRAN), predstavljajo BS, ki omogočajo povezovanje MS z omrežjem. Z namenom zmanjšanja časovnega zamika in izboljšanja delovanja, so omenjena vozlišča med seboj tudi neposredno povezana. [5]

Entiteta za upravljanje mobilnosti (ang. Mobility Management Entity – MME) predstavlja glavno krmilno vozlišče omrežja, katerega naloge so vodenje avtentikacije uporabnika, upravljanje z nosilci, spremljanje lokacije uporabniške opreme in upravljanje prehodov za podatkovne pakete. [5]

Strežnik za upravljanje z uporabniki (ang. Home Subscriber Server – HSS), hrani in upravlja uporabniške podatke in skrite ključe. V primerjavi z gradniki omrežja 2G gre tukaj za združitev AuC s HLR, ki hranita in generirata ves potrebni šifrirni material za izvajanje avtentikacije in jih zagotavlja MME. [5]

Omrežni prehod paketnih podatkov (ang. Packet data network GateWay – P-GW) zagotavlja povezavo osrednjega omrežja z zunanjimi omrežji in zagotavlja uporabniški opremi IP-naslov. Poleg omenjenega je namenjen tudi za vodenje vrednosti porabljenih storitev in zagotavljanje izvajanja storitev skladno s politiko omrežja. [5]

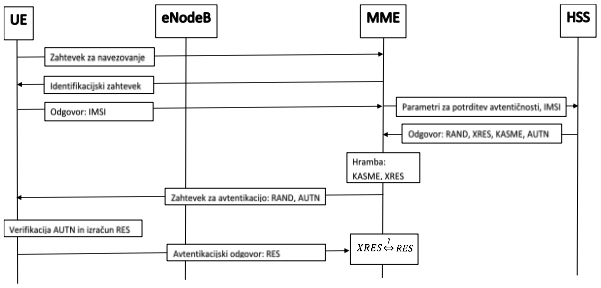
Strežniški prehod (ang. Serving GateWay – S-GW) zajame podatkovni nosilec in usmerja podatkovne paketke uporabniški opremi med proženjem MME. S-GW velja za vmesno opremo za izogibanje konstantnemu preusmerjanju podatkov na nivo P-GW ob vsakem premiku uporabniške opreme iz ene celice v drugo. [5]

2.4 Avtentikacijski postopek v omrežju 4G

Avtentikacijski postopek v omrežju 4G se deli glede na klasifikacijo naprav, ki se želijo povezati v omrežje. Te se delijo na zaupanja vredne in ne zaupanja vredne naprave, ki so ali niso del sporazuma partnerskega projekta tretje generacije (ang. 3rd Generation Partnership Project – 3GPP). V omrežju pa je operater tisti, ki odloča o tem, katera dostopna omrežja, ki niso del sporazuma so zaupanja vredna ali ne. [5]

Upravljanje dostopov s strani naprav, ki niso del sporazuma 3GPP, izvajata strežnik za avtentikacijo, avtorizacijo in obračunavanje (ang. Authentication, Authorization and Accounting – AAA) in prehod paketnih podatkov (ang. Evolved Packet Data Gateway – EPDG) [5].

Proces avtentikacije omrežij 3GPP, kot je vidno na Slika 2, se izvaja s pomočjo protokola Authentication and Key Agreement (EPS-AKA) med UE ter MME in deluje po principu medsebojne avtentikacije. [5] To pomeni, da omrežje avtenticira UE in obratno, kar je rešitev problematike v omrežjih 2G, kjer je ta proces le enosmeren. Rešitev je bila že del omrežja 3G z uvedbo protokola UMTS-AKA. Celoten postopek se začne z zahtevkom za navezovanje (ang. attach request), ki vsebuje IMSI ali GUTI (ang. Global Unique Temporary Identifier). Slednji ima enako funkcijo kot TMSI, in sicer preprečevanje pogostega izpostavljanja številke IMSI in njenega izpostavljanja potencialnemu sledenju uporabnika s strani nepooblaščene osebe. Na Slika 2 je viden postopek, kjer ima uporabniška oprema že dodeljeno GUTI, vendar je ta že potekla, kar pomeni, da je čas za dodelitev nove. MME v takšnem primeru pošlje UE zahtevek za identifikacijo in ta odgovori s svojo številko IMSI, ki je nato posredovana dalje v HSS. Ta v svoji podatkovni bazi poseduje podatke o uporabniku, in sicer njegov IMSI in SNid (ang. Serving Network identifier). S pomočjo slednjega strežnik za upravljanje z uporabniki generira ključ K_{ASME}, ki je specifičen za storitveno omrežje. HSS nato generira naključni izziv RAND ter ga skupaj z uporabniškim skritim ključem *K*, ki ga hrani v podatkovni bazi uporabi za generiranje avtentikacijskih vektorjev s pomočjo šifrirnih funkcij. Vektorji so sestavljeni iz RAND, XRES (odziv generiran s pomočjo skritega ključa *K in RAND*), K_{ASME} in AUTN (avtentikacijski žeton). Avtentikacijski vektor vsebuje tudi števec *SQN*, ki je namenjen preprečevanju ponovne rabe vektorjev, kar se dogaja med napadi s ponovno rabo (ang. replay attacks). Avtentikacijski vektor HSS nato posreduje MME, ki obdrži XRES in K_{ASME} ter posreduje AUTN in RAND uporabniški opremi UE. Ta iz parametra AUTN razbere vrednost SQN s pomočjo skritega ključa *K* in RAND. Nato UE generira vrednost XMAC, ki jo pridobi iz parametra SQN, RAND in AMF (del AUTN) ter jo primerja z vrednostjo MAC, ki je tudi del avtentikacijskega žetona. V naslednjem koraku preveri še vrednost parametra SQN in lastnega parametra SQN, katerih vrednost se ne sme razlikovati preveč. S tem je avtentikacija omrežja zaključena, in UE lahko generira ključ K_{ASME}, s čimer imata sedaj UE in omrežje enak ključ za vzpostavitev varne komunikacije. V odgovor omrežju UE generira tudi lastni odgovor RES, ki se nato na nivoju MME primerja z XRES in v primeru ujemanja zaključi postopek avtentikacije in dogovora o ključu. [5]



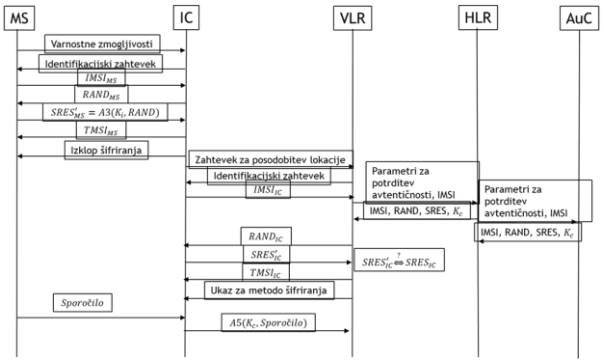
Slika 2: Avtentikacijski postopek v omrežju 4G

3 Ranljivosti v celičnem omrežju

Kot prikazuje **Error! Reference source not found.**, kjer je v postopku navezovanja v omrežju 2G prikazana metoda napada »man in the middle« (MitM), kjer naprava, imenovana lovilec IMSI (ang. IMSI catcher), prestreza paketke med MS in BS.

Lovilec IMSI enostavno spremeni vrednosti paketa, ki vsebuje varnostne zmogljivosti MS na vrednost, da MSni zmožna šifrirati komunikacije ali pa da je zmožna šifrirati samo z algoritmi, ki jih je možno s pomočjo mavričnih tabel dešifrirati v realnem času [1, 2]. Tovrstne naprave imajo za cilj znižanje varnostnega nivoja MS in s prestrezanjem paketkov z informacijami

za avtentikacijo prestrežejo informacije o uporabniku za lažje sledenje, brez da zmotijo postopek avtentikacije. [1, 2] Poznamo torej tri načine spremljanja celične komunikacije, in sicer pasivno, hibridno in aktivno obliko. Kot smo že omenili, je v nekaterih državah zaradi slabe infrastrukture celičnega omrežja in tehničnih težav na voljo le algoritem A5/0, ki pa je enostavno oznaka za to, da šifriranje ni v uporabi in so zato podatki v odprti obliki. Samo v teh primerih je možno povsem pasivno spremljanje mobilnih komunikacij, saj naprava potrebuje le pasivne komponente, in sicer prilagojene sprejemnike.



Slika 3: MITM napad značilen za lovilca IMSI

Na območjih, kjer ni omejitev in je raba šifrirnih algoritmov omogočena, je raba pasivne metode onemogočena. Tukaj pride v poštev hibridna in aktivna metoda, kjer obe vsebujeta tudi aktivno komponento, ki je namenjena posnemanju obnašanja MS ter BS. Temeljna razlika med hibridno in aktivno metodo spremljanja mobilnih komunikacij je v tem, da hibridna uporablja aktivno komponento le v procesu avtentikacije, kjer zagotovi znižanje šifriranja na nivo, katerega lahko v realnem času tudi dešifrira in s tem zagotovi pogoje pasivnega spremljanja. Aktivna metoda, ki je poimenovana tudi lažna BS (ang. fake BS) izvaja enake naloge, kot BS vendar v zmanjšanem obsegu, saj so takšne naprave mobilne in imajo zaradi tega tudi določene omejitve. [1, 2]

V celičnih omrežjih 3G in 4G so takšni napadi omejeni, saj kot smo videli uporabljajo vzajemno metodo avtentikacije, kjer se uporabniku identificira tudi samo omrežje in s tem v določeni meri prepreči vzpostavitev lažnih BS. Na podlagi virov [5, 6, 7] obstajajo v omrežju 4G določene oblike groženj, ki med drugim razkrivajo podatke o opremi v omrežju, pri čemer ni nobenega razloga, da bi bili znani uporabnikom. S pomočjo GPRS tunelskega protokola (ang. tunneling protocol – GTP) lahko uporabnik skenira omrežje in pridobi podatke o fizičnih napravah, ki so v rabi v omrežju, kar je enakovredno izvidovanju pred napadom. [7] Med možne napade spadajo tudi napadi za preprečevanje storitev (ang. denial of service – DoS), kjer z velikim številom sporočil create session v GTP protokolu lahko izkoristimo vsa razpoložljive vire in s tem onemogočimo rabo omrežja ostalim uporabnikom. [7, 8]

Pri možnost napada, ki je opisan v [8] lahko napadalec pridobi tudi telefonsko številko in IMSI uporabnika na omrežju 4G s tem, da mu moti možnost rabe omrežja, kar ima za posledico uporabo omrežja 2G. S tem lahko napadalec pridobi dovolj podatkov, da s svojo napravo oponaša napadeno in z iniciacijo klica na drugo napravo na tej pridobi tudi uporabnikovo telefonsko številko. Napad, opisan v [8], je tipični primer, kako novejše generacije celičnega omrežja zaradi povratne združljivosti lahko podedujejo varnostne luknje svojih predhodnikov, kljub temu da imajo bolj učinkovito varnostno politiko. Kot najbolj učinkovito obrambo pred temi napadi v [7, 8] navajajo opustitev zagotavljanja storitev omrežja 2G pod pogojem, da sta omrežji 3G in 4G v celoti zgrajeni in brez tehničnih pomanjkljivosti. Kot rešitev na varnostne grožnje, ki jih navajajo v viru [6] je predlagana raba asimetričnega šifrirnega algoritma in digitalnega podpisovanja, z namenom preprečevanja prestrezanja oz. zlorabe nekaterih podatkov, ki se med postopkom preverjanja istovetnosti prenašajo v odprti obliki. Vendar pa asimetrični šifrirni algoritmi zahtevajo več virov kot simetrični, ki so v trenutni rabi v omrežju 3G in 4G, kar pomeni dodatno obremenitev za fizične naprave v omrežju.

4 Zaključek

Celično omrežje 3G in 4G na nivoju varnosti zagotavlja velik napredek v primerjavi s svojim predhodnikom (2G) vendar pa ni brez pomanjkljivosti. Kot najbolj očitno grožnjo predstavlja prenos nekaterih občutljivih informacij v postopku navezovanja z omrežjem v odprti obliki. Velika slabost je tudi dedovanje varnostnih groženj s strani omrežja 2G, ki ga ponudniki na območjih kljub izgradnji omrežja 3G in 4G še vedno vzdržujejo. Ker smo trenutno v fazi izgradnje omrežja 5G, se postavlja vprašanje, ali bo omrežje 5G kljub vsem novostim tudi na področju varnosti ogroženo zaradi težav svojih predhodnikov. Treba se je zavedati kritičnosti obdobja med začetkom in koncem izgradnje 5G in pomena ukinitve prejšnjih generacij. Ranljivosti omrežja prejšnjih generacij bodo po izgradnji 5G in ukinitvi prejšnjih generacij postale brezpredmetne. To je le eden od predlogov, ki pa je ekstremno optimističen, saj bodo najverjetneje ponudniki storitev še nekaj časa po izgradnji 5G zagotavljali storitve omrežja 3G in 4G. Kot druga rešitev se ponuja vsaj ukinitev omrežja 2G in izvedba rešitev, ki temeljijo na asimetričnem šifriranju in uporaba digitalnega podpisovanja v postopkih avtentikacije.

Literatura

[1] J. Ooi, IMSI Catchers and Mobile Security, University of Pennsylvania, April 29 2015.

[2] S. Meyer, Breaking GSM with rainbow Tables, Marec 2010, arXiv:1107.1086

[3] O. D. Jensen, K. A. Andersen, A5 Encryption in GSM, Junij 2017

[4] O. Dunkelman, et al., A Practical-Time Attack on the A5/3 Cryptosystem Used in Third Generation GSM Telephony, 2010

[5] S. Behrad, E. Bertin, N. Crespi, Securing Authentication for Mobile Networks, A Survey on 4G issues and 5G answers, ICIN, Pariz, 19-22 Feb. 2018

[6] L. Qiang, et al., Security Analysis of TAU Procedure in LTE Network, Ninth International Conference on P2P, Parallel, Grid, Cloud and Internet Computing, 2014

[7] S. Park, et al., Threats and countermeasures on a 4G Mobile Network, 8th Int. Conf. on Innovative Mobile and Internet Services in Ubiquitous Computing, 2014

[8] C. Yu , et al., LTE Phone Number Catcher: A Practical Attack against Mobile Privacy, College of Computer, Security and Communication Networks, 2019