UO‘K 004.056.55

GSM TARMOG‘INING XAVFSIZLIK ZAIFLIKLARI VA ULARNI BARTARAF ETISH USULLARI

Mamatov M.[1]
[1] Samarqand davlat chet tillar instituti, Samarqand, O‘zbekiston
mamatov_m@mail.ru

Annotatsiya. *Mobil aloqa industriyasi foydalanuvchilar sonining jadal o‘sishini kuzatilmoqda, dunyo bo‘ylab eng ommabop bo‘lgan GSM tarmog‘i bir qator xavfsizlik zaifliklariga duch kelmoqda. Zamonaviy texnologiyalarning rivojlanishi natijasida yuqori avlod tarmoqlarida ushbu muammolarning ayrimlari hal etilgan bo‘lsa-da, ko‘plab operatorlar hali ham 2G va 3G tizimlaridan foydalanishda davom etmoqda. Mazkur maqolada GSM tarmog‘i va uning ma’lumot uzatish kanallaridagi eng dolzarb xavfsizlik kamchiliklarini tahlil qilib, 2G va 3G tizimlarining xavfsizligini zamonaviy texnologiyalar yordamida oshirish uchun samarali va innovatsion yechimlarni taklif etadi*.

Kalit so‘zlar: *mobil aloqa, GSM, 2G, 3G, xavfsizlik, ma’lumot uzatish kanallari.*

I. KIRISH

Mobil aloqa dunyo bo‘ylab keng tarqalgan va katta ommalashuvga erishgan. U inson hayotining ko‘plab jabhalarini o‘zgartirib, rivojlantirishga yordam berdi. Mobil telefon orqali insonlarni dunyoning istalgan joyida bog‘lash mumkin. 2024-yil boshiga kelib, dunyo bo‘ylab mobil telefonlardan foydalanuvchilar soni 5,61 milliard kishiga yetdi, bu umumiy aholi sonining 69,4% ni tashkil etadi [1]. GSMA ning 2023-yilgi hisobotiga ko‘ra, GSM (Global Service for Mobile communications) tizimidan foydalanuvchilar soni 4,3 milliardga yetdi, bu esa o‘z navbatida umumiy umumiy telefondan foydalanuvchilarning 77% ni tashkil etadi. GSMA hisobotida turli mintaqalar va davlatlar o‘rtasidagi tengsizliklar aniqlandi. Masalan, Shimoliy Amerika, Sharqiy Osiyo va Tinch okeani mintaqasidagi smartfon egalarining 69 foizi 4G tarmog‘idan foydalanadi. Biroq, Afrikadagi va O‘rta Osiyo va yaqin sharq mamlakatlari aholisi ko‘proq 3G tarmog‘idan foydalanmoqda [2]. GSM tizimi va uning asosiy tarkibiy qismlari 1-rasmda aks ettirilgan [3]. GSM texnologiyasi doimiy takomillashib, GSM1800, HSCSD (High Speed Circuit Switched Data), EDGE (Enhanced Data rates for GSM Evolution), va GPRS (General Packet Radio Service), 3G, 4G, 5G kabi yangi versiyalarni yuzaga keltirdi. Aksariyat tahlillarga ko‘ra, GSM tizimida tug‘ma xavfsizlik zaifliklari mavjud, va ba’zi zaifliklar 4G va 5G kabi keyingi avlod tizimlarida bartaraf etilgan. Biroq, rivojlanayotgan mamlakatlardagi ko‘plab operatorlar hanuzgacha xavfsizlik kamchiliklariga ega bo‘lgan GSM tarmog‘laridan foydalanishda davom etmoqda.

Garchi ba’zi tadqiqotlarda [4-6] GSM xavfsizligi masalalari ko‘rib chiqilgan bo‘lsa-da, ular to‘liq xavfsizlik tahlili yoki amaliy yechimlarni taklif qilishmagan. Ushbu maqola GSM xavfsizlik zaifliklarini qisqacha tahlil qilib, hozirgi foydalanilayotgan GSM tizimlarining xavfsizligini oshirish uchun amaliy va samarali yechimlarni taklif qiladi.

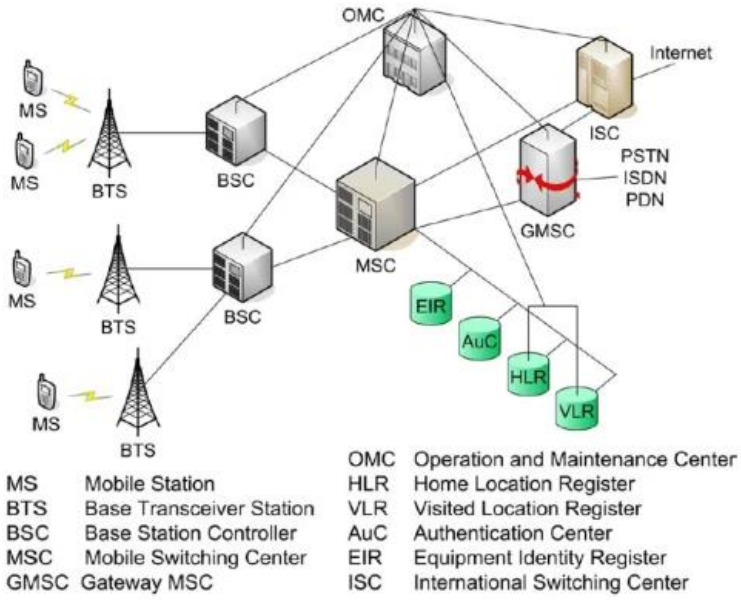
II. GSM TARMOG‘INING XAVFSIZLIK ARXITEKTURASI

GSM tarmog‘ining xavfsizlik arxitekturasi dastlab foydalanuvchi ma’lumotlari va signalizatsiya axborotining anonimligini, autentifikatsiyasini va maxfiyligini ta’minlash kabi xavfsizlik xizmatlarini taqdim etish uchun mo‘ljallangan edi [7]. GSM tizimining xavfsizlik maqsadlari quyidagilarni o‘z ichiga oladi:

- mobil foydalanuvchilarni tarmoqqa autentifikatsiya qilish;
- foydalanuvchi ma’lumotlari va signalizatsiya axborotining maxfiyligini ta’minlash;
- foydalanuvchi shaxsiyatining anonimligi;
- SIM (Subscriber Identity Module) ni xavfsizlik moduli sifatida ishlatish.

Mobil stansiya Mobil uskunadan va SIM kartasidan iborat. SIM – bu GSMga xos dasturlar yuklangan kriptografik aqlli kartadir. Aqlli karta sifatida, unda aqlli kartalarga xos ba’zi xavfsizlik funksiyalari mavjud [8]. Uning operatsion tizimi va chip apparatida bir nechta xavfsizlik atributlari mavjud. SIM kartasi obunachining hisobiga kirish uchun zarur bo‘lgan barcha ma’lumotlarni o‘z ichiga oladi. IMSI va Ki har bir SIM kartasida saqlanadi. IMSI – bu xalqaro mobil obunachi identifikatori bo‘lib, dunyodagi har bir mobil obunachi uchun unikal bo‘lgan, eng ko‘pi bilan 15 raqamdan iborat. Ki (Individual subscriber authentication Key) – bu tasodifiy 128-bitli raqam

bo‘lib, u sessiya kalitlarini yaratish va mobil foydalanuvchilarni tarmoqqa autentifikatsiya qilish uchun ishlatiladigan asosiy kriptografik kalitdir. Ki qat’iyan himoyalangan va obunachining SIM kartasida va AuC (Authentication Center)da saqlanadi. SIM karta o‘zini o‘zi shaxsni aniqlash raqami (PIN) bilan himoyalaydi. Har bir foydalanuvchi PINni kiritishni so‘raydi, agar bu funksiya foydalanuvchi tomonidan o‘chirilmagan bo‘lsa. Bir nechta xato kiritishlar (odatda 3 marta)dan so‘ng SIM kartasi PINni bloklaydi va PUK (PINni blokdan chiqarish) raqami so‘raladi. Agar PUK ham bir nechta marta noto‘g‘ri kiritilsa (odatda 10 marta), SIM karta o‘zining maxsus ma’lumotlariga va autentifikatsiya funksiyalariga mahalliy kirishni rad etadi va o‘zini ishlamay qolgan holatga keltiradi.

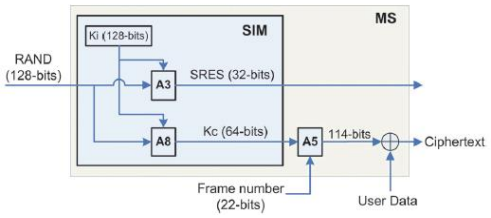


1-rasm. GSM tarmog‘ining arxitekturasi

Foydalanuvchi ma’lumotlarining autentifikatsiyasi va maxfiyligi IMSI va Ki raqamlarining sir saqlanishiga bog‘liq. Bunday raqamlar oshkor qilingan taqdirda, har kim qonuniy foydalanuvchini taqlid qilishi mumkin. Har bir SIM kartada A3 va A8 algoritmlari amalga oshirilgan. Bu, har bir operator boshqa operatorlar va apparat ishlab chiqaruvchilaridan mustaqil ravishda ushbu algoritmlarni aniqlash va o‘zgartirish imkonini beradi. Shuning uchun autentifikatsiya foydalanuvchi boshqa mamlakatlarda yoki operatorlarda roumingda bo‘lsa ham ishlaydi, chunki mahalliy tarmoq natijalar uchun uy tarmog‘ining HLR (Home Location Register) ga so‘rov yuboradi va uy tarmog‘ining A3/A8 algoritmini bilish shart emas. A3 asosan foydalanuvchini tarmoqqa autentifikatsiya qilish uchun ishlatiladi, A8 esa shifrlash uchun sessiya kaliti Kc ni yaratish uchun ishlatiladi. Tarmoq foydalanuvchiga tasodifiy chaqiruv yuboradi, shunda SIM kartasi Kc va SRES ni hosil qiladi. Foydalanuvchi autentifikatsiya qilingandan so‘ng, tarmoq telefonni shifrlashni boshlash uchun yaratgan sessiya kaliti Kc ni ishlatishni buyurishi mumkin.

Kriptografik algoritmlar mobil telefonlarning apparatida amalga oshiriladi. Tarmoq telefonlarda amalga oshirilgan algoritmni tanlashi mumkin, jami 7 xil shifrlash algoritmidan (yoki shifrlashsiz rejim) tanlash imkoniyati mavjud, ammo u telefonlarda amalga oshirilgan algoritmni tanlashi kerak. Telefonning imkoniyatlarini tarmoqqa bildirish uchun avvaliga Classmark xabari yuborilgan. Umuman olganda, uchta algoritm mavjud: A5/1, A5/2 va A5/3. A5/1 va A5/2 – bu aslida GSM standartlari tomonidan belgilangan ikkita oqimli shifrlash algoritmi. A5/1 kuchliroq, ammo eksportni nazorat qilishga sub’ect bo‘lib, faqat CEPT (Yevropa Telekommunikatsiya Ma’muriyati) a’zosi bo‘lgan davlatlarda ishlatilishi mumkin. A5/2 esa xususan zaiflashtirilgan bo‘lib, boshqa mamlakatlar tomonidan ishlatilishi uchun mo‘ljallangan. Bunday algoritmlardan foydalanish GSMning MoU (Memorandum of Understanding) orqali nazorat qilinadi. A5/3 esa 3GPP tomonidan 2002-yilda belgilangan Kasumi algoritmiga asoslangan blokli shifrlash algoritmi bo‘lib, dual-rejimli telefonlar tomonidan qo‘llab-quvvatlanadi, ya’ni ular 2G va 3G tizimlarida ham

ishlay olishadi. GSM autentifikatsiyasi, sessiya kalitini yaratish va shifrlash jarayonlari 2-rasmda tasvirlangan [3].



2-rasm. GSM autentifikatsiyasi, sessiya kalitini yaratish va shifrlash

GSM tarmog‘ida anonimlikni ta’minlash uchun IMSI o‘rniga 32-bitli Vaqtinchalik Mobil Obunachi Identifikatori (TMSI) ishlatiladi. TMSI, odatda, VLR (Visitor Location Register) tomonidan boshqariladi va ma’lum bir Joylashuv Hududi doirasida amal qiladi. TMSI, shuningdek, har bir joylashuv yangilanishi jarayonida muntazam ravishda yangilanadi, ya’ni obuna harakatlanayotgan hududga qarab yangi TMSI tayinlanadi. Bu TMSI faqat bir vaqtning o‘zida ishlatiladi va shu sababli obunachining real IMSI raqami ochiqdan-ochiq ishlatilmaydi. Shuningdek, TMSI obunachining SIM kartasida saqlanadi, bu esa uning doimiy ravishda yangi raqam bilan yangilanishini ta’minlaydi. Bu usul tarmoqni tinglovchilardan himoya qiladi, chunki ular faqat TMSI orqali obunachining joylashuvi va tarmoqdagi holatini kuzatib borishi mumkin, ammo haqiqiy IMSI raqamini bilishlari imkonsiz. Shunday qilib, TMSI foydalanuvchining identifikatsiyasini yashirishga yordam beradi va uning shaxsini aniqlashni qiyinlashtiradi.

III. GSM XAVFSIZLIGIGA TAHDIDLAR

Simli aloqa tarmoqlarining ochiqligi aloqada bo‘lgan tomonlarni xavfsizlik tahdidlari uchun yanada zaiflashtiradi. GSM turli texnikalarni, masalan, chastota sakrashni qo‘llab, tinglashni qiyinlashtirishga harakat qilgan bo‘lsa-da, almashinuv axborotlarini real vaqt rejimida tinglash mutlaqo amaliy hisoblanadi [9]. Hozirgi kunda bir nechta joylashgan obunachilarni bir vaqtning o‘zida tinglashga qodir tijorat uskunalari mavjud [10,11]. GSM xavfsiz simsiz tizim bo‘lishi maqsadida ishlab chiqilgan va foydalanuvchini autentifikatsiya qilish hamda havodan shifrlashni ta’minlashni ko‘zda tutgan bo‘lsa-da, u bir qator hujumlarga mutlaqo zaifdir, har biri tarmoqning bir qismiga qaratilgan. Quyida GSM tarmog‘ining eng muhim xavfsizlik xatoliklari qisqacha keltirilgan. Ushbu zaifliklardan noto‘g‘ri foydalanish uchun bir nechta amaliy senariylar ham ishlatilishi mumkin, ularning barchasi qisqalik uchun e’tibordan chetda qolgan.

GSM tarmog‘ining xavfsizligi bir qator tahdidlarga duch kelmoqda, bu esa uning foydalanuvchilari va tarmoqlariga jiddiy xavf solishi mumkin. Quyida GSM tarmog‘iga qaratilgan asosiy xavfsizlik tahdidlari kengroq bayon etilgan:

1. Tinglash va ma’lumotlarni o‘g‘irlash. GSM tarmog‘ining ochiq simsiz aloqalari foydalanuvchi ma’lumotlarini o‘g‘irlash va tinglash uchun oson imkoniyat yaratadi. Garchi tarmoqda shifrlash texnologiyalari mavjud bo‘lsa-da, bu texnologiyalarni teskari muhandislik orqali o‘rganish va noto‘g‘ri ishlatish mumkin. Shuningdek, ayni paytda bir qator tijorat asbob-uskunalari, masalan, "sniffer"lar, tarmoqda harakatlanayotgan ma’lumotlarni real vaqt rejimida o‘g‘irlashga qodir.

2. Chastota sakrashi (Frequency Hopping) va uning zaifligi. GSM tarmog‘ida chastota sakrashi usuli, aloqalarni boshqalardan himoya qilish uchun ishlatiladi. Ushbu texnologiya, albatta, ma’lumotlarni o‘g‘irlashni qiyinlashtiradi, ammo u hali ham teskari muhandislik yordamida buzilishi mumkin. Hujumchi bir necha usullar orqali chastotani aniqlash va o‘z manfaatlariga ishlatish imkoniyatiga ega.

3. IMSIning oshkor bo‘lishi. IMSI (Xalqaro Mobil Obunachi Identifikatori) raqami GSM tarmog‘ida foydalanuvchini identifikatsiya qilishda ishlatiladi. Agar IMSI raqami oshkor bo‘lsa, bu tahdid foydalanuvchini taqlid qilish (spoofing) uchun ishlatilishi mumkin. Hujumchi foydalanuvchining IMSI raqamini o‘g‘irlab, tarmoqda uning o‘rniga o‘zini ko‘rsatishi mumkin, bu esa tarmoqni noto‘g‘ri identifikatsiya qilishga olib keladi.

4. Man-in-the-Middle hujumlari. GSM tarmog‘ida ma’lumotlar o‘tkazilayotganda, hujumchi o‘rtadagi odam (man-in-the-middle) usulidan foydalanib, aloqani o‘rtada to‘xtatib, ma’lumotlarni o‘zgartirishi yoki o‘g‘irlayishi mumkin. Ushbu hujumlar foydalanuvchi va tarmoq orasidagi ma’lumotlarni manipulyatsiya qilish va tarmoqdagi xavfsizlikni buzish uchun ishlatiladi.

5. SIM kartalarining zaifligi. SIM kartalari tarmoqni xavfsiz saqlash uchun ishlatiladi, ammo ular teskari muhandislik orqali o‘rganilishi yoki ishlab chiqilgan maxfiy kalitlarni o‘g‘irlash orqali buzilishi mumkin. SIM kartalarining xavfsizligi ba’zida noaniq bo‘lishi mumkin, bu esa uni noxush maqsadlarda ishlatishga imkon beradi.

6. Key Exchange (Kalit almashish) zaifliklari. GSM tarmog‘ida sessiya kalitlarini almashish jarayonlari ba’zida zaif bo‘lishi mumkin. Hujumchi tarmoqda o‘tkazilayotgan kalitlarni qayta tiklash orqali shifrlashni o‘zgartirish yoki foydalanuvchi ma’lumotlarini dekodlashga qodir bo‘lishi mumkin. Bu turdagi hujumlar tarmoqning butun xavfsizligini xavf ostiga qo‘yadi.

7. Jismoniy qurilmalarga hujumlar. GSM tarmog‘ining jismoniy qurilmalari, masalan, mobil stansiyalar yoki bazaviy stansiyalar, xavfsizlikka qarshi hujumlarga uchraydi. Ushbu qurilmalarga jismoniy kirish orqali tajovuzkorlar tarmoq ma’lumotlarini o‘g‘irlashi yoki qurilmalarni buzishi mumkin. Boshqa qurilmalar orqali tarmoqni manipulyatsiya qilish va xatolarni kiritish imkoniyati mavjud.

8. Xavfsiz bo‘lmagan qurilmalarning ulanishi. GSM tarmog‘iga xavfsiz bo‘lmagan qurilmalar ulanishi mumkin. Ba’zan, qurilmalar xavfsiz bo‘lmagan holatlarda tarmoqqa ulanadi, bu esa foydalanuvchilarning ma’lumotlarini o‘g‘irlash yoki zarar etkazishga olib kelishi mumkin. Tarmoqda xavfsiz bo‘lmagan qurilmalar orqali kirish imkoniyati tarmoqni zaiflashtiradi.

9. Tarmoqni qayta ishlatish (Replay Attacks). Replay hujumlari tarmoqdagi oldingi aloqalarni qayta ishlatib, foydalanuvchi ma’lumotlarini ushlab turish yoki noto‘g‘ri identifikatsiya qilishga imkon beradi. Bu turdagi hujumlar tarmoq xavfsizligiga jiddiy tahdid soladi va foydalanuvchilarning ishonchini suiste’mol qilish uchun ishlatilishi mumkin.

10. Havoda shifrlashning zaifligi. GSM tarmog‘ida havoda shifrlash texnologiyasi (Kc) ba’zi hollarda yetarli xavfsizlikni ta’minlamaydi. Bu esa foydalanuvchi ma’lumotlarini o‘g‘irlash yoki tarmoqda noto‘g‘ri foydalanishga olib keladigan xavfsizlik muammolarini yuzaga keltiradi. Shifrlashning zaifligi tarmoqdagi boshqa xavfsizlik muammolariga ham sabab bo‘lishi mumkin.

IV. TRANSPORT KANALLARINING XAVFSIZLIGI

GSM tarmog‘ida bir nechta transport kanallari mavjud: qisqa xabarlar xizmati (SMS), tuzilmagan qo‘shimcha xizmat ma’lumotlari (USSD), simsiz ilovalar protokoli (WAP) va ovozli kanal. Shuningdek, GSM yangilanishlari bilan qo‘shimcha ravishda Enhanced Messaging Service (EMS) va Multimedia Messaging Service (MMS) kabi yangi xizmatlar kiritilgan. yuqorida tasvirlangan xavfsizlik nuqsonlari, umuman olganda, barcha xizmatlar va transport kanallariga taalluqlidir, chunki ular barcha almashinuvi ma’lumotlar va signallash ma’lumotlarini maqsad qiladi. Ammo, bunday umumiy nuqsonlarga qo‘shimcha ravishda, ba’zi GSM transport kanallari o‘ziga xos muammolar va zaifliklarga ega. SMS xabar almashinuvi uning saqlash va o‘tkazish xususiyati tufayli qo‘shimcha xavfsizlik zaifliklariga ega bo‘lib, Internet orqali amalga oshirilishi mumkin bo‘lgan soxta SMS muammosi mavjud. Foydalanuvchi roumingda bo‘lganida, SMS mazmuni turli tarmoqlar va ehtimol Internet orqali o‘tadi, bu esa uni turli zaifliklar va hujumlarga ochib beradi. Boshqa bir xavotir, agar dushman telefonni qo‘lga kiritib, avvalgi himoyalanmagan xabarlarni o‘qib chiqsa, yuzaga keladi. USSD esa sessiya yo‘nalishidagi texnologiya bo‘lib, hujumlarga nisbatan zaif, chunki xabarlar GSM asosiy tarmog‘ida shifrlanmagan va himoyalanmagan.

WAP ME ga Internetga ulanish imkonini beradi. WAP arxitekturasida MS va Web server o‘rtasida joylashgan WAP Gateway, Internet protokollari (HTTP, SSL/TLS, va UDP/TCP/IP) bilan mos WAP protokollarini (WSP/WTP, WTLS, va WDP) tarjimon sifatida ishlaydi va ba’zi implementatsiyalarda WAP bo‘shlig‘iga sabab bo‘lgan qo‘shimcha xavfsizlik nuqsonini keltirib chiqaradi. Boshqa xavotirlar Internetning xavfsizlik muammolaridan kelib chiqadi, chunki Internet – bu GSM xavfsizlik arxitekturasida asosiy tarmoq xavfsiz va boshqariladigan muhit sifatida faraz qilingan katta nazoratsiz tarmoqdir. Web serverlar shuningdek, mijoz (ME)da zararli appletlarni yuklab olish va bajarishlari mumkin, shuning uchun appletlar va boshqa yuklab olingan dasturlar xavfsizligi boshqa bir xavotir manbai hisoblanadi.

V. GSM XAVFSIZLIK NUQSONLARIGA YECHIMLAR

GSM tarmog‘ining xavfsizlik nuqsonlari tarmoqni zaiflashtiradi va foydalanuvchilarni xavf ostiga qo‘yadi. Biroq, ushbu zaifliklarni bartaraf etish va tarmoqni himoyalash uchun bir qancha yechimlar mavjud. Ushbu maqolada GSM xavfsizligini mustahkamlash uchun qo‘llanilishi mumkin bo‘lgan ba’zi amaliy yechimlar keltirilgan:

1. Shifrlashni kengaytirish va modernizatsiya qilish. GSM tarmog‘ida ma’lumotlar almashinuvi paytida xavfsizlikni ta’minlash uchun shifrlash texnologiyalarini yanada takomillashtirish zarur. A5/1, A5/2, va A5/3 kabi shifrlash algoritmlari mavjud bo‘lsa-da, yangi va kuchliroq algoritmlar, masalan, AES (Advanced Encryption Standard)ni joriy etish tavsiya etiladi. Bu o‘zgartirishlar ma’lumotlar va

qo‘ng‘iroqlarni yanada ishonchli himoya qilishga yordam beradi. Shuningdek, shifrlashni barcha kanallar va xizmatlar, jumladan SMS va USSD, uchun kengaytirish kerak.

2. SIM kartalarini mustahkamlash. SIM kartalari GSM tarmog‘ining xavfsizligini ta’minlashda muhim rol o‘ynaydi. SIM kartalari uchun maxfiy kalitlarni saqlash va autentifikatsiya jarayonlarini yanada kuchaytirish zarur. Foydalanuvchi SIM kartalarini himoya qilish uchun PIN va PUK kodlarini mustahkamlash hamda SIM kartalarini yana bir marta autentifikatsiya qilish usullarini joriy etish tavsiya etiladi. Shuningdek, SIM kartalarini yuqori darajada xavfsizligini ta’minlash uchun ko‘proq kriptografik protokollarni qo‘llash zarur.

3. IMSIning himoyalanishi. IMSIning himoyasini kuchaytirish uchun uni faqat zarur hollarda ishlatish va boshqa xavfsizlik usullarini qo‘llash zarur. Foydalanuvchi identifikatorini himoya qilish uchun vaqtincha mobil obunachi identifikatori (TMSI) kabi mexanizmlardan foydalanishni kengaytirish kerak. Bundan tashqari, IMSI raqamining tarmoqdan tashqarida xavfsiz o‘tkazilishi va uning to‘liq shifrlanishi ta’minlanishi kerak.

4. Qo‘shimcha xavfsizlik protokollarini joriy etish. GSM tarmog‘ida qo‘shimcha xavfsizlik protokollarini joriy etish tarmoqni kuchaytirish uchun muhimdir. Masalan, SSL/TLS protokollarini qo‘llash orqali tarmoqda o‘tkazilayotgan ma’lumotlarni yanada ishonchli shifrlash mumkin. WAP va SMS kabi xizmatlar uchun xavfsizlikni yaxshilash uchun shifrlashni kengaytirish va faqat autentifikatsiya qilingan foydalanuvchilarga kirish huquqini berish tavsiya etiladi. Shuningdek, Internetga kirish va yuklab olingan dasturlarni xavfsizligini ta’minlash uchun tarmoqni faqat sertifikatlangan va xavfsiz qurilmalar bilan ishlashga ruxsat berish zarur.

5. Vaqtinchalik identifikatorlar va autentifikatsiyani mustahkamlash. GSM tarmog‘ida ro‘yxatdan o‘tgan foydalanuvchilarning identifikatsiyasini yaxshilash va anonimlikni ta’minlash uchun vaqtinchalik mobil abonent identifikatori (TMSI)ni joriy etish zarur. Bu foydalanuvchining haqiqiy IMSI raqamini oshkor qilishning oldini oladi va tarmoqda ro‘yxatdan o‘tgan abonentlarni anonimli tarzda autentifikatsiya qilishga imkon beradi. TMSI va IMSI raqamlarini almashtirish orqali tarmoqni tinglashdan himoya qilish mumkin.

6. Hujumlarni aniqlash va oldini olish. Tarmoqda hujumlarni aniqlash va oldini olish uchun xavfsizlik tahlili va monitoring tizimlarini joriy etish zarur. GSM tarmog‘ida real vaqt rejimida xavfsizlik tahlilini amalga oshirish va tarmoqdagi barcha aloqalarni kuzatish yordamida dushman hujumlarini erta aniqlash mumkin. Xavfsizlikni yaxshilash uchun tarmoqdagi ma’lumotlarni doimiy ravishda tahlil qilib, xavfli faoliyatlarni aniqlash va blokirovka qilish zarur.

GSM tarmog‘ining xavfsizlik nuqsonlarini bartaraf etish uchun yuqorida keltirilgan yechimlarni amalga oshirish zarur. Bu yechimlar tarmoqning butun xavfsizlik arxitekturasini mustahkamlashga yordam beradi va foydalanuvchi ma’lumotlarini himoya qilishda samarali bo‘ladi. Shuningdek, yangi texnologiyalar va protokollarni joriy etish tarmoqni yanada ishonchli qiladi va GSM tarmog‘ida yuzaga kelishi mumkin bo‘lgan xavfsizlik tahdidlariga qarshi samarali choralar ko‘riladi.

VI. XULOSA

Ushbu maqolada GSM tarmog‘ining xavfsizligi tahlil qilinib, uning xavfsizlik muammolariga qisqacha va to‘liq sharh berilgan. Tadqiqotda GSM tarmog‘ida ko‘plab tabiiy xavfsizlik zaifliklari mavjudligi va ularning firibgarlik yoki foydalanuvchilarni aldatish uchun ishlatilishi mumkinligi aniqlangan. Shuningdek, hozirgi kunda mavjud bo‘lgan 2G va 3G tarmoqlarining xavfsizligini oshirishga qaratilgan amaliy yechimlar taqdim etilgan. Yechimlardan ba’zilari tarmoq infratuzilmasining xavfsizligini yaxshilashga mo‘ljallangan bo‘lsa, boshqalari esa endi endi xavfsizlikni ta’minlashga qaratilgan. Oxirgi foydalanuvchigacha xavfsizlik yoki ilovalar qatlamidagi xavfsizlik hozirgi 2G v 3G tizimlarida eng samarali va foydali yechim sifatida ko‘riladi.

ADABIYOTLAR

[1] Статистика интернета и соцсетей на 2024 год — цифры и тренды в мире и в России. https://www.web-canape.ru/business/statistika-interneta-i-socsetej-na-2024-v-mire-i-v-rossii/

[2] GSMA: в мире насчитали 4,3 миллиарда пользователей смартфонов. https://lenta.ru/news/2023/10/14/gsm/

[3] *M. Toorani, S.A.A. Beheshti*. Solutions to the GSM Security Weaknesses Proceedings of the Second International Conference on Next Generation Mobile Applications, Services, and Technologies (NGMAST'08). DOI: 10.1109/NGMAST.2008.88

[4] *P. Chandra*, “Bulletproof Wireless Security, GSM, UMTS, 802.11 and Ad hoc Security,” Elsevier, 2005.

[5] *S.M. Siddique, and M. Amir*, “GSM Security Issues and Challenges,” 7th IEEE

International Conference on Software Engineering, Artificial Intelligence, Networking and Parallel/Distributed Computing (SNPD'06), pp.413-418, June 2006.
[6] *V. Niemi, and K. Nyberg*, “UMTS Security,” John Wiley and Sons, 2003.
[7] *C-C Lo, and Y-J Chen*, “Secure Communication Mechanisms for GSM Networks,” IEEE Transactions on Consumer Electronics, Vol.45, No.4, pp.1074-1080, Nov. 1999.
[8] *W. Rankl, and W. Effing*, “Smart Card Handbook,” 3rd ed., John Wiley and Sons, 2003.
[9] *F.J. Gonzalez-Castano, J. Vales-Alonso, J.M. Pousada-Carballo, F.I. de Vicente, and M.J. Fernandez-Iglesias*, “Real-Time Interception Systems for the GSM Protocol,” IEEE Transactions on Vehicular Technology, Vol.51, No.5, pp. 904-914, Sept. 2002.
[10] *J.R. Rao, P. Rohatgi, H. Scherzer, and S. Tinguely*, “Partitioning Attacks: Or How to Rapidly Clone Some GSM Cards,” IEEE Symposium on Security and Privacy (S&P'02), pp.31-41, 2002.
[11] *Зуйков А. В., Михайлов Д. М., Стариковский А. В., Фроимсон М. И.* Уязвимости системы коммерческих SMS-шлюзов в инфраструктуре GSM-сетей // Перспективы развития информационных технологий. 2010. №2.

Поступила в редакцию 28.09.2024

Citation: *Mamatov M.* (2024). GSM tarmog‘ining xavfsizlik zaifliklari va ularni bartaraf etish usullari. Raqamli texnologiyalarning nazariy va amaliy masalalari xalqaro jurnali. 7(4). – B. 86-91. https://doi.org/10.62132/ijdt.v7i4.224

SECURITY VULNERABILITIES OF THE GSM NETWORK AND METHODS FOR MITIGATING THEM

Mamatov M.[1]
[1] Samarkand State Institute of Foreign Languages, Samarkand, Uzbekistan

Abstract. *The mobile communication industry has seen rapid growth in the number of users, and the globally most popular GSM network is facing a number of security vulnerabilities. While some of these issues have been addressed in higher-generation networks due to the development of modern technologies, many operators continue to use 2G and 3G systems. This paper analyzes the most critical security flaws in the GSM network and its data transmission channels, and proposes effective and innovative solutions to enhance the security of 2G and 3G systems using modern technologies.*

Keywords: *mobile communication, GSM, 2G, 3G, security, data transmission channels.*

УЯЗВИМОСТИ БЕЗОПАСНОСТИ СЕТИ GSM И СПОСОБЫ ИХ УСТРАНЕНИЯ

Маматов М.[1]
[1] Самаркандский государственный институт иностранных языков, Самарканд, Узбекистан

Аннотация. *Индустрия мобильной связи переживает быстрый рост числа пользователей, и наиболее популярная в мире сеть GSM сталкивается с рядом уязвимостей безопасности. Несмотря на то, что некоторые из этих проблем были решены в сетях более высоких поколений благодаря развитию современных технологий, многие операторы продолжают использовать системы 2G и 3G. В данной статье анализируются наиболее критичные уязвимости безопасности в сети GSM и её каналах передачи данных, а также предлагаются эффективные и инновационные решения для повышения безопасности систем 2G и 3G с использованием современных технологий.*

Ключевые слова: *мобильная связь, GSM, 2G, 3G, безопасность, каналы передачи данных.*