РАДІОТЕХНІКА ТА ТЕЛЕКОМУНІКАЦІЇ

УДК 621.396.42

DOI <https://doi.org/10.32838/2663-5941/2021.2-2/04>

Гарист А.В.

Український науково-дослідний інститут спеціальної техніки та судових експертиз
Служби безпеки України

АНАЛІЗ ЗАХИЩЕНОСТІ МЕРЕЖ СТІЛЬНИКОВИХ ОПЕРАТОРІВ ІЗ ПРОТОКОЛОМ БЕЗПЕКИ SS7

Телефонна мережа загального користування починаючи з 80-х років XX сторіччя модернізувалась із простої мережі, яка забезпечує передачу голосу з обмеженими можливостями передачі даних, до більш інтелектуального засобу з можливістю передавати інформацію з високою пропускну спроможністю та можливістю її швидкого відновлення в разі апаратних відмов. Стимулом до модернізації служило прагнення телекомунікаційних компаній ефективно керувати мережею та збільшувати її пропускну спроможність найбільш економічним чином.

У телефонних мережах, зокрема мобільних, чітко розділяються абонентський (голос або дані) і службовий трафік (наприклад, для встановлення з'єднання). Службовий трафік – це система сигналізації № 7 (Signaling System № 7, далі за текстом – SS7), яка містить певний набір протоколів, правил і повідомлень. Протокол SS7 належить до мережі передачі даних і до низки технічних протоколів або правил, які регулюють обмін даними по них. Його було розроблено в 1970-х роках для відстеження та під'єднання викликів у різних мережах операторів зв'язку, але тепер він зазвичай використовується для розрахунку білінгу стільникового зв'язку та відправлення текстових повідомлень у доповнення до маршрутизації мобільних і стаціонарних викликів між операторами й регіональними комутаційними центрами.

У статті представлено результати дослідження захищеності мереж із протоколом захисту SS7. Протокол SS7 використовується для обміну службовою інформацією між мережевими пристроями в телекомунікаційних мережах. Коли розроблявся цей стандарт, доступ до мережі SS7 мали лише оператори фіксованою зв'язку, тому безпека не була пріоритетним завданням. Сьогодні сигнальна мережа вже не є повністю ізольованою, тому зловмисник, який отримав до неї доступ, має можливість експлуатувати вади безпеки для того, щоб прослуховувати голосові виклики абонентів, читати SMS, викрадати гроші з рахунків, обходити системи тарифікації або впливати на функціонування мобільної мережі.

На початку 2000-х років було запропоновано специфікацію Sigtran, яка дала змогу передавати службову інформацію протоколу SS7 по IP-мережі і сигнальна мережа перестала бути ізольованою.

Ключові слова: система сигналізації № 7, абонент, стільникова мережа зв'язку, ідентифікатор, протокол, білінг.

Постановка проблеми. Незважаючи на появу мереж нового покоління 4G, які використовують іншу систему сигналізації Diameter, проблеми безпеки протоколу SS7 будуть залишатися актуальними ще довгий час, оскільки оператори зв'язку досі повинні забезпечувати підтримку стандартів 2G та 3G, а також взаємодію між мережами різних поколінь. Ба більше, дослідження доводять, що протокол Diameter схильний до тих же загроз, що й SS7. У статті розглянуто вразливості цього протоколу, а також опис можливих атак, надано приклади застосування цих вразливостей, щоб продемонструвати масштаби проблем безпеки сучасних мереж зв'язку.

Аналіз останніх досліджень і публікацій. Уперше вразливості SS7 були публічно продемонстровано в 2008 році. Німецький дослідник Тобіас Енгель показав техніку стеження за абонентами мобільних мереж. У 2014 році експерти Positive Technologies Дмитро Курбатов і Сергій Пузанков виступили на конференції Positive Hack Days із презентацією «Як підслухати людину на іншому кінці земної кулі» та представили детальний звіт «Вразливості мереж мобільного зв'язку на основі SS7», у якому розповідали не тільки про прослуховування, але й про багато інших можливостей хакерів у сигнальній мережі SS7, зокрема переказ грошей, перехоплення SMS-повідомлень, визна-

чення місця розташування абонента без його відома та інше.

У 2015 році фахівці SR Labs в ефірі австралійської програми «60 хвилин», перебуваючи в Німеччині, перехоплювали SMS-листування австралійського сенатора Ніка Ксенофонта і британського журналіста, а потім спостерігали за пересуваннями сенатора у відрядженні в Токіо.

Водночас, незважаючи на значну кількість наукових публікацій, присвячених проблемам вразливостей протоколу SS7, стрімкий розвиток систем зв'язку та протоколів їх захисту зумовлює потребу подальших досліджень цієї тематики.

Постановка завдання. Метою статті є аналіз захищеності сигнальних мереж SS7 у режимі реального часу та виявлення нелегітимної активності з можливістю блокування несанкціонованих повідомлень або оповіщення сторонніх засобів фільтрації та блокування трафіку. Метою аналізу є своєчасне виявлення потенційних загроз і реагування на них, не надаючи негативного впливу на функціонування мережі зв'язку.

Виклад основного матеріалу дослідження. Адресація вузлів у мобільному зв'язку під час взаємодії між операторами відбувається не за IP-адресами, а за адресами Global Title, формат яких нагадує телефонні номери. Адреси Global Title в обов'язковому порядку повинні входити в діапазон телефонних номерів, закріпленими за оператором зв'язку, а якщо на національному рівні діапазони розбиваються за регіонами, то й адреси Global Title вузлів мережі повинні відповідати регіональним діапазонам.

Для взаємодії вузлів ядра мобільного оператора використовується протокол MAP – Mobile Application Part. Протокол MAP спрямований на реалізацію функцій, які властиві саме мережі мобільного зв'язку, такі як аутентифікація і реєстрація мобільного апарату в мережі, локалізація абонента для здійснення вхідного виклику, підтримка безрозривного мовного каналу зв'язку під час пересування абонента. Кожній операції відповідають певні повідомлення протоколу MAP зі своїм набором параметрів.

Для мобільних комунікацій використовуються телефонні номери, які називаються MSISDN – Mobile Subscriber Integrated Services Digital Network Number. Цей номер надається абоненту під час укладання договору з мобільним оператором, але в надрах мережі зв'язку абоненти адресуються за ідентифікатором – IMSI (International Mobile Subscriber Identity), який прив'язується до конкретної SIM-картки. Пере-

важна більшість операцій вимагає адресації абонента саме через IMSI, отже, для проведення більшості атак, спрямованих на конкретного абонента, зломиснику насамперед потрібно дізнатися цей ідентифікатор.

Потрібно також зазначити, що в протоколах SS7 не закладено можливості аутентифікації вузлів, фільтрації повідомлень за списками доступу, динамічну маршрутизацію нових вузлів мережі.

Розгляньмо приклад опису атаки.

Наприклад, ми маємо номер +380670000000. Це MSISDN (Mobile Subscriber Integrated Services Digital Number). Він не зберігається на SIM-картці. На SIM-картці зберігається інший ідентифікатор – IMSI, який передається в мережу тільки під час реєстрації абонента. Це 15-значне число, яке має вигляд 380-11-555555555, у якому «380» – код країни, «11» – код оператора, а інші 10 цифр – внутрішній унікальний номер цієї SIM-картки (MSIN, Mobile Subscriber Identification Number). Саме IMSI використовується для ідентифікації абонента всередині стільникової мережі зв'язку, тобто для здійснення будь-яких операцій із номером.

Для здійснення атаки на протокол SS7 зломисник під'єднується до сигнальної мережі SS7 і відправляє службову команду Send Routing Info в мережевий канал, вказуючи номер телефону абонента, який атакується як параметр. Домашня абонентська мережа відправляє у відповідь таку технічну інформацію: IMSI і адресу MSC, за якою надаються послуги підписнику.

Після цього зломисник змінює адреси білінгової системи в профілі підписника на свої власні адреси псевдобілінгової системи (наприклад, повідомляє, що абонент прилетів на відпочинок і в роумінгу зареєструвався на новій білінговій системі). Як відомо, жодну перевірку така процедура не проходить. Далі атакуючий вводить оновлений профіль у базу даних VLR через повідомлення «Insert Subscriber Data».

Коли абонент, якого атакують, здійснює вихідний дзвінок, його комутатор звертається до системи зломисника замість фактичної білінгової системи. Система зломисника відправляє комутатору команду, що дозволяє перенаправити виклик третій стороні, яка контролюється зломисником.

У сторонньому місці встановлюється конференц-зв'язок між трьома підписниками, два з них є реальними (абонент А і абонент В), а третій вводиться зломисником незаконно і здатний прослуховувати й записувати розмову.

Відповідним чином ми маємо можливість отримати і SMS-повідомлення, вказавши свій MSC/VLR, увесь трафік буде направлено зловмиснику. Наприклад, так можна зібрати одно-разові SMS-паролі для двоетапної авторизації в різних сервісах. SMS вимагає від MSC/VLR підтвердження його доставки, і якщо його не відправляти, а замість цього перереєструвати абоненту на «справжній» MSC, то через кілька хвилин буде зроблено ще одну спробу доставки повідомлення, і воно надійде адресату. Тобто одне й те ж SMS буде відправлено двічі: спочатку – зловмиснику, потім – адресату.

Маючи доступ до псевдобілінгової системи, на яку вже зареєструвався абонент, можна отримати будь-яку інформацію, яка надходить або виходить з його телефону.

Усі вищенаведені дії з перехоплення повідомлень і прослуховування телефонної розмови можна виконувати за допомогою IMSI-перехоплювачів. Вони налаштовуються так, щоб мобільний телефон жертви вважав, що це єдине доступне з'єднання, оскільки віддають перевагу тій стільниковій вишці, чий сигнал найбільш сильний для того, щоб максимізувати якість сигналу й мінімізувати власне енергоспоживання.

Крім того, у мережах GSM (2G) тільки мобільний телефон повинен проходити процедуру аутентифікації, від стільникової вишки цього не потрібно, тому його легко ввести в оману, зокрема щоб від'єднати на ньому шифрування даних.

Налаштовуються IMSI-перехоплювачі так, що без посередництва IMSI-перехоплювача не можна зробити виклик.

Знаючи IMSI мобільного телефону цілі, оператор може запрограмувати IMSI-перехоплювач, щоб він зв'язувався тільки з цим телефоном, коли той перебуває в межах досяжності.

Після під'єднання оператор використовує процес картографування радіочастот, щоб з'ясувати напрямок місцеположення цілі та його напрям руху.

За правильного налагодження перехоплювача мобільний телефон цілі може надавати інформацію про режим роботи в стандарті LTE, 3G або 4G, а насправді працювати в режимі 2G із більш слабкою системою шифрування.

Деякі мобільні телефони навіть у режимі LTE виконують команди без попередньої аутентифікації, хоча стандарт LTE до цього зобов'язує. Крім того, оскільки LTE-інтерфейс розроблявся як модернізація UMTS-інтерфейсу, який є модернізованим GSM-інтерфейсом, то його структура не

бездоганна. Також, незважаючи на широке поширення мереж 3G і 4G, мережі 2G, як і раніше, забезпечують резервний доступ, якщо 3G і 4G стають недоступними.

Коли IMSI-перехоплювач захоплює IMSI із SIM-картки і IMEI з мобільного телефону, обидва ці параметри зберігаються в базі даних пристрою. Отже, зміна SIM-карток і зміна мобільного телефону не допоможуть уберегтися від прослуховування за допомогою IMSI-перехоплювача.

Стандарт мобільних пристроїв бездротової високошвидкісної передачі даних Long Term Evolution (LTE), який використовують мільярди людей, було розроблено для виправлення багатьох огріхів безпеки в попередньому стандарті, відомій як глобальна система мобільного зв'язку GSM. Взаємна аутентифікація між кінцевими користувачами і базовими станціями та використання перевірених схем шифрування були двома основними змінами. Тепер дослідники публічно виявляють слабкі місця в LTE, які дають змогу зловмисникам відправляти найближчих користувачів на шкідливі вебсайти та відстежувати сайти, які вони відвідують, аналізувати трафік абонента й маніпулювати даними, що відправляються на пристрій користувача.

Атаки можливі через хиби, які вбудовані в сам стандарт LTE. Найбільш серйозна слабкість – це форма шифрування, яка не захищає цілісності даних. Брак аутентифікації даних дає змогу зловмисникові непомітно маніпулювати IP-адресами в зашифрованому пакеті. Дослідниками розроблено три варіанти атаки на LTE. Дві атаки проводяться в пасивному режимі та дають змогу збирати метадані про трафік, наприклад ідентифікувати певні види трафіку й визначати, які сайти відвідує користувач.

Атака, якою займалася група дослідників, отримала назву aLTET. Вона змушує мобільні пристрої використовувати шкідливий сервер системи доменних імен, який перенаправляє користувача на шкідливий сервер, маскується під Hotmail шляхом заміни IP-адреси DNS-сервера в DNS-пакетах.

Для захисту від підміни DNS-пакетів рекомендується застосовувати методи захисту DNS-трафіку, такі як DNS-SEC і DNS over TLS/HTTPS.

Атака вимагає фізичної присутності поблизу від жертви й ґрунтується на ініціюванні під'єднання пристрою жертви до фіктивної базової станції, трафік з якої перенаправляється до цієї базової станції (MITM-атака, що нагадує IMSI-catcher, але дає змогу не тільки прослуховувати трафік, але й модифікувати пакети).

Дві інших хиби пов'язані з тим, як LTE показує користувачів у стільниковій мережі та дає можливість витоку конфіденційної інформації про дані, які передаються між базовими станціями й кінцевими користувачами.

Можливість маніпулювати трафіком зумовлена недоробками в механізмах шифрування, які застосовуються на каналному рівні LTE (Data Link Layer). Зокрема, дані в LTE шифруються з використанням алгоритму AES-CTR, що працює в режимі лічильника, але без застосування засобів для контролю цілісності блоків. Брак контролю цілісності дає змогу підмінити шифротекст. Зокрема, в AES-CTR шифротекст формується шляхом застосування операції XOR між ключовою послідовністю (keystream) й вихідними даними.

Якщо атакуючий знає, які дані буде передано в пакеті, він може визначити частину ключової послідовності, яка використовується для створення частини шифротексту (операція XOR дає змогу відновити вміст ключа, знаючи підсумковий шифротекст і вихідні дані), і використовувати його для підміни відомих вихідних даних на свої дані, згенерувавши для них коректний шифротекст.

Найбільш простою з огляду практичної реалізації є підміна IP-адреси DNS-сервера в DNS-пакетах, оскільки атакуючий може передбачити адресу DNS-сервера (зазвичай використовуються сервери провайдера або публічні сервери типу 8.8.8.8 або 1.1.1.1). Варто зазначити, що проблема частково зачіпає й ще не прийнятий стандарт 5G, у якому введено додатковий режим надійного шифрування даних, що передаються з контролем цілісності, але проблема в тому, що цей режим не обов'язковий і запропонований як опція.

Основними проблемами під час атак є:

- необхідно заздалегідь знати, де є ціль, і мати дублюючу базову станцію, яка працює в радіусі приблизно кілометра від місця розташування;
- наявність спеціальної програмно-обумовленої радіосистеми, на якій виконується індивідуальна реалізація специфікації LTE;
- стабільність з'єднання, фільтрування радіооперешкод і програмне забезпечення для вияв-

лення шахрайства, впровадженого операторами мережі.

У лабораторних умовах для демонстрації стабільної атаки в приміщенні використовуються спеціальні екрани, які допомагають позбутися шумів і домогтися підтримки стійкого під'єднання.

У середині 2016 року Національний інститут стандартів і технологій США (The National Institute of Standards and Technology, NIST) представив документ, згідно з яким використання SMS-повідомлень для здійснення двофакторної аутентифікації в майбутньому не буде заохочуватись. У документі міститься пряма вказівка на те, що використання SMS-повідомлень для двофакторної аутентифікації буде розглядатися як неприпустиме й небезпечне.

Висновки. Узагальнюючи вищезазначене, можна зробити висновок, що захищеність мереж SS7 досі на низькому рівні. Мережі зв'язку містять небезпечні вразливості, які дають змогу порушити доступність сервісів для абонентів. Майже в кожній мережі можна прослухати розмову абонента або прочитати вхідні SMS-повідомлення та проводити шахрайські операції.

Оператори усвідомлюють наявні ризики та вживають заходів, які спрямовані на зниження ймовірності реалізації загроз.

Сьогодні вдалося скоротити ризики витоку інформації про мережу й абонента із впровадженням системи SMS Home Routing, яка здійснює фільтрацію повідомлень. Нині із цим мережі мобільного зв'язку використовують системи фільтрації та блокування сигнального трафіку.

Проте, незважаючи на активне впровадження додаткових систем захисту, усі мережі зв'язку є схильними до вразливостей, які пов'язані як із приватними випадками некоректного налагодження обладнання, так і з архітектурними проблемами сигнальних мереж SS7, які неможливо усунути наявними засобами. Тільки комплексний підхід до розв'язання проблем безпеки, який передбачає регулярний аналіз захищеності, підтримання параметрів мережі в актуальному стані, постійний моніторинг сигнального трафіку та своєчасне виявлення нелегітимної активності, може забезпечити високий рівень захисту від злочинців.

Список літератури:

1. ОКС-7. *Вікіпедія*. URL: <https://ru.wikipedia.org/wiki/ОКС-7#:~:text=Система%20сигнализации%20№%207%2C%20или,с%20канальным%20разделением%20по%20времени>.
2. Уязвимости сетей мобильной связи на основе SS7. URL: <https://www.ptsecurity.com/upload/corporate/ru-ru/analytics/PT-SS7-security-2014-rus.pdf>.
3. Tobias Engel (2008), Location Mobile Phones using SS7-25. Chaos Communication Congress. URL: http://media.ccc.de/v/25c3-2997-en-locating_mobile_phones_using_ss7.

**Haryst A.V. ANALYSIS OF THE SECURITY OF NETWORKS
OF CELLULAR OPERATORS WITH A SECURITY PROTOCOL SS7**

Since the 1980s, the public telephone network has been upgraded from a simple network that provides voice transmission with limited data transmission capabilities to a more intelligent means that has the ability to transmit information with high bandwidth and the ability to quickly recover from hardware failures.

The incentive for modernization was the desire of telecommunications companies to effectively manage the network and increase its capacity in the most cost-effective way. This upgrade laid the foundation for new services such as ISDN, Intelligent Networking and others.

In telephone networks, including mobile ones, subscriber traffic (voice or data) and service traffic (for example, for establishing a connection) are clearly separated. Service traffic is Signaling System 7 – SS7, which contains a specific set of protocols, rules and notifications. The SS7 protocol refers to the data network and the technical protocols or rules that govern the exchange of data over them. It was developed in the 1970s to track and connect calls across various carrier networks, and is now used to calculate cellular billing and send text messages in addition to routing mobile and landline calls between carriers and regional switching centers.

This article presents the results of a study of the security of networks with the SS7 security protocol. When this standard was developed, only fixed operators had access to the SS7 network, so security was not a priority. Today, the signaling network is no longer completely isolated, so the offender who has gained access to it has the opportunity to use security flaws in order to listen to voice calls of subscribers, read SMS messages, transfer money from accounts, bypass billing systems or affect the functioning of the mobile networks.

In the early 2000s, the SIGTRAN specification was proposed, which allowed the transmission of SS7 protocol information over an IP network, and the signaling network was no longer isolated.

Key words: *Signaling System № 7, subscriber, cellular communication network, identifier, protocol, billing.*