УДК 004.056

ВРАЗЛИВОСТІ ПРОТОКОЛУ SS7 В УМОВАХ ІНТЕГРАЦІЇ З IP МЕРЕЖАМИ

І. М. Цибуленко-Сігов[1,a], Л. Ю. Гальчинський[2]

[1] Навчально-науковий Фізико-технічний інститут

Анотація

Робота присвячена дослідженню вразливостей протоколу SS7 в умовах його інтеграції з IP-мережами, аналізі найпоширеніших сценаріїв атак та розробка рекомендацій для підвищення рівня безпеки у мобільних мережах. У цій роботі описано поняття та основні вразливості, що стосуються мережі SIGTRAN. Результати проведеного дослідження можливо застосувати у реалізації мережі SS7 over IP для покращення рівня безпеки обміну інформацією через мережі 2G/3G.

Ключові слова: SS7, SIGTRAN, система сигналізації, вразливості

Вступ

Протокол SS7 став основою сучасних мобільних мереж 2G (GSM) та 3G (UMTS), він дозволяє: встановлювати та завершувати телефонні дзвінки, реалізовувати роумінг між операторами, передавати SMS, обробляти запити на визначення локації абонента, переадресовувати виклики чи ідентифікувати номери. Із часом стало зрозуміло, що старі протоколи 2G/3G, які були оптимально спроектовані для передачі голосу згодом стануть перевантаженими. На заміну прийшли протоколи LTE 4G, 5G, що можуть обробляти більші об'єми трафіку з вищою швидкістю, однак перехід на кардинально нові технології займає багато часу та коштує чималих грошей, тому протоколи, в основі яких лежить система сигналізації SS7 не втратять своєї актуальності в найближчому майбутньому. Розуміння та врахування ризиків, які з'являються зі сторони IP для мережі сигналізації дає можливість забезпечити безпеку передачі інформації в застарілих мережах, що в свою чергу дозволить безпечний та розмірений перехід до нових технологій.

1. Постановка задачі

Безпека обміну даних, зокрема через мобільні мережі є однією із найважливіших тем сучасності. Хоч наразі існує багато новітніх рішень з передачі даних через IP, комунікаційні технології 2G і 3G будуть актуальними набагато довше, ніж ми це очікуємо, а отже SS7 буде рушієм обміну даними. Ключовим питанням цієї роботи є дослідження вразливостей Системи сигналізації №7, що виникають з боку IP мереж та можливостей пом'якшення кіберризиків.

[a]bogatuur@gmail.com

2. Вразливості протоколу SIGTRAN

2.1. Огляд основних понять протоколу SIGTRAN

Традиційні архітектури 2G (Global System for Mobile Communications – GSM) та 3G (Universal Mobile Telecommunication System – UMTS) складаються з мереж доступу і базової мережі. На рис. 1 зображено взаємозв'язок між мережею доступу та базовою мережею із зовнішніми SS7 або IP-мережами. Мережа доступу, також відома як підсистема базових станцій (Base Station Subsystem – BSS) для архітектури 2G або універсальна наземна мережа радіодоступу (Universal Terrestrial Radio Access Network – UTRAN) для 3G, дає змогу користувачам (абонентам) під'єднувати свої мобільні термінали до мережі.

Мережа доступу складається з базової приймально-передавальної станції (Base Transceiver Station – BTS) і вузла B (NodeB) для 2G і 3G відповідно, які використовуються для забезпечення зв'язку між мобільною станцією (Mobile Station – MS) і мережею. Крім того, мережа доступу має контролери, які називаються Base Station Controller (BTS) для 2G і Radio Network Controller (RNC) для 3G, які відповідають за розподіл радіо ресурсів між BTS і підтримання радіозв'язку.

Основна мережа, або підсистема комутації мережі (Network Switching Subsystem – NSS), відповідає за обслуговування мережі, якість обслуговування та вихідні дзвінки. NSS поділяється на мобільний центр комутації, бази даних користувачів та елементи з'єднання. Мобільний комутаційний центр (Mobile Switching Center – MSC) контролює управління викликами, білінг та взаємозв'язок мережі із зовнішніми мережами з комутацією каналів, мережі SS7 та IP-мережами (роумінг).

Робота мережі покладається на елементи бази даних що зберігають інформацію про користувачів у

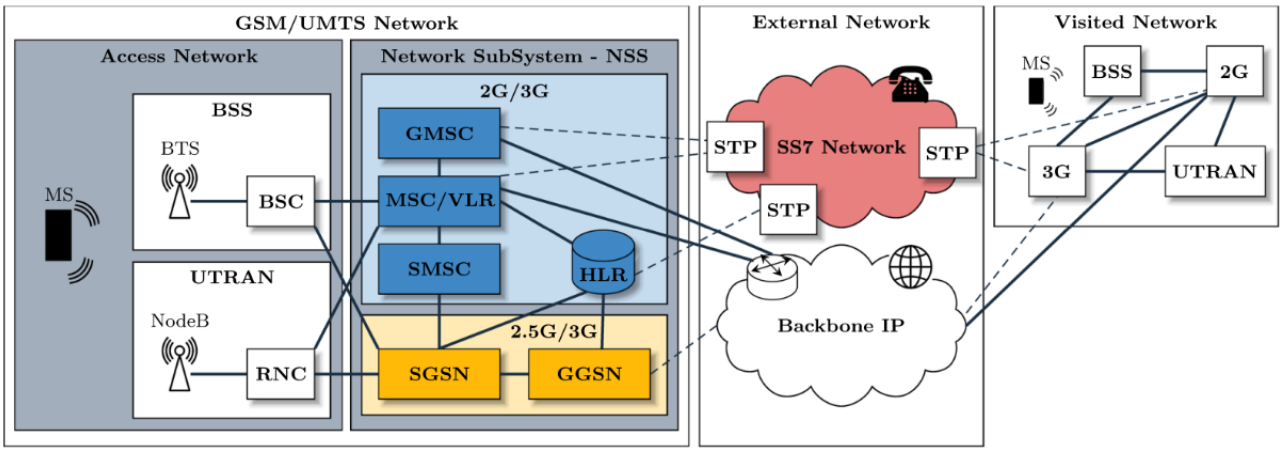

Рис. 1. Базова архітектура 2G/3G мережі

домашніх, Home Location Register (HLR), та у відвіданих мережах, Visitor Location Register (VLR). HLR зберігає постійні дані: номер телефону або міжнародний абонентський номер мобільної станції (Mobile Station International Subscriber Directory Number – MSISDN) та ідентифікатор SIM-карти (International Mobile Subscriber Identity – IMSI), який використовується для визначення місцезнаходження користувача в мережі. VLR зберігає тимчасову інформацію про абонентів у роумінгу. Оскільки GSM не підтримує передачу пакетів даних,було запроваджено, до складу NSS було запроваджено два нових елементи GPRS: обслуговуючий вузол підтримки (Serving GPRS Support Node – SGSN) та шлюзовий вузол підтримки (Gateway GPRS Support Node – GGSN), подібні до MSC/GMSC, але з підтримкою IP.

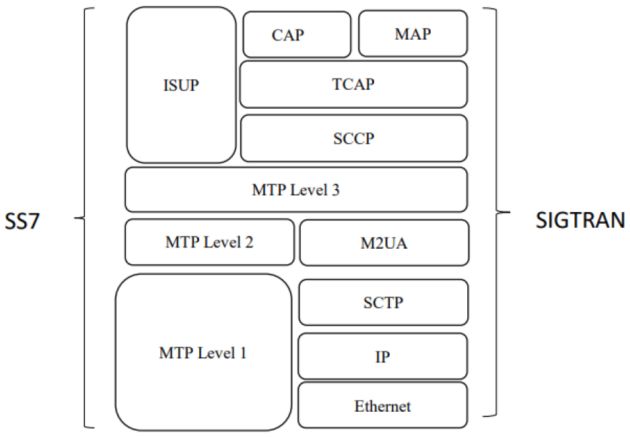

Рис. 2. Стек протоколів CCS7

2.2. Традиційні мережі 2G/3G

Signaling System 7 (SS7) – це міжнародний стандарт телекомунікаційного протоколу, який визначає, як мережеві елементи в телефонній мережі загального користування (PSTN) обмінюються інформацією та сигналами управління.

SIGTRAN – це набір протоколів, призначений для передачі протоколів сигналізації через IP, і є розширенням сімейства протоколів SS7. Він підтримує ті управління додатками і викликами, як і SS7, але використовує IP протокол для транспортування – Stream Control Transmission Protocol (SCTP).

Типове застосування SIGTRAN – сигнальні шлюзи, які дозволяють мережам передачі голосу по IP (VoIP) взаємодіяти з традиційними телефонними мережами, використовуючи комутацію каналів і SS7. Шлюз отримує сигнальні повідомлення, що надходять з мережі SS7, і пересилає їх на сторону IP за допомогою SIGTRAN.

SS7 визначає стек протоколів, подібний за функціональністю до моделі OSI. Головними властивостями SS7 є надійність і відмовостійкість, а в IP мережах - швидкість передачі даних, тому поєднання цих технологій стало головною задачею. З цією метою було створено SIGTRAN (Signaling Transport). Серед протоколів, доданих до стеку SS7, був введений протокол MAP (Mobile Application Part). MAP використовується як для зв'язку між елементами основної мережі (MSC, HLR, SGSN і т.д.), так і для міжмережного зв'язку. Протокол прикладного рівня використовує клієнт-серверний підхід, і зловмисники часто використовують його вразливості. На додаток до MAP, існує ще один прикладний протокол – CAP (CAMEL Application Protocol), який надає послуги мобільним мережам. У стеку SS7 протоколи MAP і CAP працюють поверх протоколу TCAP (Transaction Capability Application Part), який стандартизує зв'язок між базами даних мобільних мереж. SCCP (Signaling Connection Control Part) – це протокол мережевого рівня, що використовується для маршрутизації в системах SS7, який також вразливий. SS7 використовується як для передачі сигналів між різними мережами, як показано на рис. 2, так і всередині мобільної мережі [1].

2.3. Вразливості SS7

На момент розробки протоколу SS7, стільникові мережі були нечисельними і, як правило, були пов'язані з урядовими установами. Початкові мережі передбачали взаємну довіру між операторами.

Однак із стрімким розвитком телекомунікаційної сфери, на ринку почала з'являтися велика кількість нових операторів, зокрема менших компаній (MVNO – Mobile Virtual Network Operator), що мають доступ до мережі SS7. Сьогодні все ще використовуються повідомлення вразливого протоколу MAP. А оскільки дизайн SS7 не враховував проблеми безпеки, що ми маємо сьогодні, багато вразливостей все ще можуть бути використані за допомогою MAP. Наприклад, можна відстежувати місцезнаходження користувачів, перехоплювати дзвінки та SMS, надсилати фішингові повідомлення.

Проблема залишається і в 4G (Non-Standalone) через можливий перехід до 2G/3G для обробки голосових дзвінків. Голосові дзвінки, що працюють на комутації каналів, не підтримуються за замовчуванням, оскільки 4G базується на комутації пакетів. Для надання голосових послуг повністю через LTE, (Voice Over Long Term Evolution - VoLTE), необхідно розгорнути мультимедійну підсистему IP (IMS). Хоч IMS є частиною стандартів 4G та 5G, оскільки використання ядра IMS вимагає величезних інвестицій в інфраструктуру, деякі оператори не розгортають ядро IMS для підтримки дзвінків VoLTE. У цьому випадку їм доведеться перейти на застарілі мережі (2G/3G) з підтримкою голосу, так званий резервний варіант з комутацією каналів (Circuit Switched Fallback, CSFB), що використовує SS7 [2]. Крім того, для повного переходу на VoLTE всі мобільні пристрої користувачів повинні мати вбудовану підтримку VoLTE, що, ймовірно, займе певний час. Тому багато вузлів все ще залишаються гібридними, підтримуючи як протокол SS7, так і протокол Diameter, який замінює SS7 в LTE. На даний момент найбільш практичним рішенням є перехід на нижчу версію, тому провайдерам 4G все ще доводиться мати справу з системою сигналізації SS7 і притаманними їй вразливостями.

3. Атаки на мережі SS7

Атаку користувачів мобільної мережі через SS7 можна здійснити кількома способами. Всі вони включають поетапний підхід, використовуючи відомі вразливості для отримання доступу до інформації, що може бути використана для атаки на абонентів або елементи мережі.

3.1. Особливості атак типу SS7

Для стислості ми називаємо ці кроки «атакою SS7» або «атакою на мобільну мережу». Перший крок фокусується на бездротовому інтерфейсі, який використовується для передачі даних між мобільними станціями. Цей зв'язок використовує загальні Broadcast Common Control Channel (BCCH), Paging Channel (PCH) і виділені логічні канали. Лише останні включають автентифікацію, тому використання незахищених BCCH і PCH дає зловмиснику, який має доступ до мережі SS7, необхідну інформацію (TMSI, Global Title тощо) для здійснення атаки.

Зловмисник з пасивним радіообладнанням або програмно визначеним радіо (SDR) може перехоплювати всю інформацію у відкритому вигляді, що поширюється каналами BCCH і PCH. Антени SDR, що є на ринку за доступними цінами, можуть бути використані для прослуховування конфіденційної інформації з повітряного інтерфейсу. Інший подібний варіант використовує комбінацію USRP (універсальний програмний радіо периферійний пристрій) і програмного забезпечення з відкритим кодом, такого як GNURadio, для прослуховування мереж доступу.

У виділених логічнийх каналах GSM використовуються алгоритми шифрування A5/1, A5/2, A5/3 та GEA4 [3], які виявилися вразливими [4]. Взаємна автентифікація в GSM з'явиася не зразу, тому розгорнута не на всіх станціях. Коли GSM не використовує алгоритм для автентифікації обох сторін (UMTS-AKA), він припускає, що базові станції завжди є легітимними – в цій моделі довіри повідомлення від мережі до мобільних станцій не потребують автентифікації. Як наслідок, зловмисник з активною радіостанцією («симуляторами стільникового вузла» або «IMSI Catcher»), може здійснити атаку «Людина посередині» (MITM), встановивши проміжне з'єднання між користувачем і мережею.

Програмне забезпечення з відкритим вихідним кодом, що реалізує стандарти мобільного зв'язку, також може використовуватися для MITM-атак. Наприклад, SigPloit-ss7 [5], може бути встановлене на мікрокомп'ютер Raspberry Pi із модулем GSM Layer-2/3, щоб пасивно і активно діяти в мережі GSM. Таким чином, зловмисник за допомогою спеціального програмного та апаратного забезпечення може видавати себе за базову станцію і в той час приховувати частоти сусідніх BTS. Оскільки мобільний телефон приєднується до BTS, з найвищим рівнем сигналу, абоненти підключаються до зловмисних вузлів. З точки зору мережі, зловмисник маскується, видаючи себе за користувача. Після підключення до фальшивої базової станції всі повідомлення, якими обмінюються справжня базова станція та абонент, отримує зловмисник, в тому числі IMSI, IMEI, місцезнаходження тощо [6]. Ця інформація може бути використана для подальшої атаки на мережу або справжніх користувачів мобільного зв'язку.

SS7 не передбачав строгі вимоги безпеки, тому будь-яке повідомлення від MAP або іншого протоколу зі стеку SS7, призначене для ядра мобільної мережі або якоїсь сигнальної точки SS7, отримує негайну відповідь. Хоч отримати доступ до мережі SS7, щоб почати генерувати повідомлення, не так вже й легко, можна безпосередньо орендувати або придбати хаб SS7 з доступом до мобільної мережі. Такий доступ зазвичай надається MVNO або невеликим операторам великими телекомунікаційними провайдерами для забезпечення аутсорсингу та розширення послуг, таких як роумінг та SMS. Після того, як ці MVNO або малі оператори отримують доступ до концентратора, на додаток до доступу до мережі, вони можуть отримати GT (Global Title) та угоду про роумінг.

3.2. Аналіз механізмів атак типу SS7 і засоби пом'якшення їх наслідків

У документах IR.71 та IR.82, опублікованих Асоціацією GSM, висвітлюються вразливості SS7 [7], пов'язані з початковим припущенням про взаємну довіру між операторами. Варто зазначити, що цю інформацію можна отримати з відкритих джерел [8, 9]. З них можна виокремити три категорії MAP та CAP-повідомлень. Ці категорії визначають рекомендації щодо фільтрації вихідних і вхідних повідомлень на вузлах ядра мобільної мережі і транзитних вузлах (сигнальних точках мережі SS7).

- Категорія 1: Ця категорія складається з MAP-повідомлень, якими обмінюються виключно всередині мережі. Повідомлення цього типу повинні прийматися від зовнішніх мереж тільки в тому випадку, якщо це явно дозволено контрактом. Одним з таких повідомлень є ATI (AnyTimeInterrogation), яке слід приймати і обробляти тільки в тому випадку, якщо вузол-джерело є HLR мережі-джерела. Для цієї категорії рекомендується прийняти політику, яка відфільтровує ці повідомлення на межі мережі за допомогою брандмауерів.
- Категорія 2: складається з MAP-повідомлень, що надсилаються з домашньої мережі абонента до відвідуваної мережі, яка може працювати з роумінговими користувачами. Наприклад, абонент з міста А подорожує в місті Б, і база даних HLR з А запитує мережу Б, щоб перевірити місцезнаходження абонента. Щоб запобігти атакам цієї категорії, GSMA рекомендує перевіряти джерело MAP-повідомлення, щоб переконатися, що IMSI абонента, який подорожує, дійсно належить до HLR домашньої мережі.
- Категорія 3: Ця категорія складається з MAP-повідомлень від відвідуваних мереж до домашньої мережі, також внаслідок роумінгу користувачів. Це схоже на категорію 2, але процес починається, наприклад, з VLR в місті В (відвідуваної) до HLR в місті А (домашньої). У цій зворотній ситуації застосування фільтрів стає складнішим, оскільки повідомлення може бути створено будь-де. Отже, зловмисник може стверджувати, що абонент знаходиться в його власній мережі. Тоді домашня мережа повинна порівняти інформацію про останнє місцезнаходження користувача з інформацією в отриманому MAP-повідомленні. Якщо інформація не збігається, слід порахувати, чи міг абонент переміститися зі свого останнього місцезнаходження до нового, про яке було повідомлено, за час, що минув. Якщо буде зроблено висновок, що поточне місцезнаходження є необґрунтованим, повідомлення має бути відфільтроване.

Висновки

В представленій роботі було проведено дослідження механізмів атак на IP мережі і аналіз потенційних вразливостей пов'язаних з протоколом SS7. Використовуючи віртуальну машину DragonOS [10] – дистрибутив Linux, орієнтований на роботу з програмно-обумовленим радіо (SDR), та SiGploit – фреймворк для тестування безпеки систем сигналізації, було емульовано трафік зі зловмисним кодом. Показано можливості захоплення діалогу для проведення аналізу та виявлено можливості відрізняти зловмисні SS7 запити від нелегітимних.

Перелік використаних джерел

1. *Macedo L. de Carvalho*, *Campista M.* Attacks to mobile networks using SS7 vulnerabilities: a real traffic analysis. // Telecommunication Systems. — 2023. — Vol. 83. — P. 253–265. — DOI: 10.1007/s11235-023-01018-0. — URL: https://doi.org/10.1007/s11235-023-01018-0.
2. Performance of CS Fallback from LTE to UMTS / J. E. Vargas Bautista, S. Sawhney, M. Shukair, I. Singh, V. K. Govindaraju, S. Sarkar // IEEE Communications Magazine. — 2013. — Т. 51, № 9. — С. 136—143. — DOI: 10.1109/MCOM.2013.6588662.
3. On Security Research Towards Future Mobile Network Generations / D. Rupprecht, A. Dabrowski, T. Holz, E. Weippl, C. Pöpper // IEEE Communications Surveys and Tutorials. — 2018. — Т. 20, № 3. — С. 2518—2542. — DOI: 10.1109/COMST.2018.2820728.
4. Breaking the GSM A5/1 cryptography algorithm with rainbow tables and high-end FPGAS / M. Kalenderi, D. Pnevmatikatos, I. Papaefstathiou, C. Manifavas. — 2012. — DOI: 10.1109/FPL.2012.6339146.
5. *D'Alessandro R.* SiGploit a signaling security testing framework. — 2018. — URL: https://github.com/ethicalhackeragnidhra/SigPloit-ss7.
6. *Торопчин Є.*, *Гальчинський Л. Ю.* Вразливості конфігурацій мобільних мереж та методи їх пом'якшення // Collection of Scientific Papers «SCIENTIA». — 2024. — Т. 79, № 4. — С. 97—105. — URL: https://previous.scientia.report/index.php/archive/article/view/2132.
7. *Association G.* SMS SS7 Fraud Prevention Version 6.1. — 2024. — URL: https://www.gsma.com/newsroom/wp-content/uploads//IR.71-v6.1.pdf.
8. *Schaeken V.* Vulnerabilities, potential risks and recommendations. — 2019. — URL: https://www.itu.int/en/ITU-T/Workshops-and-Seminars/102019/Documents/Vulnerabilties_and_Categories.pdf.
9. *Association G.* SS7 vulnerabilities and attack exposure report. — 2018. — URL: http://gsma.com/get-involved/gsma-membership/wp-content/uploads/2018/07/SS7_Vulnerability_2017_A4.ENG_.0003.03.pdf.
10. *Cemaxecuter.* DragonOS. — 2025. — URL: https://sourceforge.net/p/dragonos-focal/wiki/Home/.