УДК 621.391.7:004.056.5
В. Новосад; О. Оробчук, Ph.D
(Тернопільський національний технічний університет імені Івана Пулюя, Україна)

АНАЛІЗ ВРАЗЛИВОСТЕЙ ПРОТОКОЛУ SS7, ЗАГРОЗИ ТА МЕТОДИ ЗАХИСТУ

UDC 621.391.7:004.056.5
V. Novosad, student; O. Orobchuk Ph.D

ANALYSIS OF SS7 PROTOCOL VULNERABILITIES, THREATS, AND PROTECTION METHODS

Протокол SS7 (Signaling System No. 7) є фундаментальною технологією для телекомунікаційних мереж другого і третього поколінь (2G та 3G), та взаємодії між різними мережами, особливо між 4G і попередніми поколіннями. Він забезпечує передачу сигналів для маршрутизації викликів, передачі SMS та підтримки роумінгу.

Однак, архітектура SS7 побудована на принципі довіри між вузлами мережі, що створює значні ризики безпеки. Вразливості цього протоколу вже неодноразово використовувалися для таких атак, як перехоплення повідомлень, визначення місцезнаходження користувачів, шахрайство у роумінгу та перенаправлення викликів.

Актуальність даної теми обумовлена тим, що попри впровадження сучасніших протоколів, таких як LTE та 5G, SS7 залишається у використанні. Його широке застосування у мобільних мережах створює загрози для конфіденційності мільйонів користувачів, фінансової стабільності операторів та національної безпеки. У роботі проведено дослідження ключових вразливостей SS7, оцінка їх впливу на телекомунікаційні мережі та розробка рекомендацій щодо їх мінімізації. У ході дослідження систематизовано основні вразливості, зокрема відсутність шифрування даних між вузлами мережі, недостатня автентифікація запитів, а також відсутність ефективної фільтрації трафіку. Серед можливих заходів захисту розглянуто впровадження SS7 Firewall, який блокує небезпечні запити, систем моніторингу для аналізу мережевого трафіку та попередження атак у реальному часі, а також впровадження автентифікації вузлів. Крім того, важливим рішенням є перехід до сучасного протоколу Diameter, що забезпечує вищий рівень безпеки завдяки вбудованому шифруванню та автентифікації.

Ці результати можуть бути використані операторами мобільного зв’язку для забезпечення комплексного підходу до захисту їхніх мереж, включаючи впровадження сучасних технологій моніторингу, шифрування даних та багаторівневої автентифікації. Завдяки цьому оператори зможуть ефективніше виявляти та запобігати атакам, знижувати ризики витоку конфіденційної інформації та мінімізувати фінансові втрати, спричинені шахрайством у роумінгу чи іншими видами атак.

Література

1. 3GPP TS 29.002. Mobile Application Part (MAP) Specification. Version 15.6.0. Sophia Antipolis: 3GPP, 2020. 250 с.
2. Engel T. SS7: Locate. Track. Manipulate. Presentation at 31st Chaos Communication Congress (31C3). 2014. 58 с.
3. GSM Association. SS7 Interconnect Security Monitoring and Firewall Guidelines. London: GSM Association, 2017. 45 с.
4. Positive Technologies. SS7 Security: Threats and Vulnerabilities. [Електронний ресурс]. – Режим доступу: https://www.ptsecurity.com/ (дата звернення: 04.12.2024). 25 с.
5. RFC 6733. Diameter Base Protocol. [Електронний ресурс]. – Режим доступу: https://datatracker.ietf.org/doc/html/rfc6733 (дата звернення: 04.12.2024). 160 с.