

**НАЦІОНАЛЬНИЙ ТЕХНІЧНИЙ УНІВЕРСИТЕТ УКРАЇНИ
«КИЇВСЬКИЙ ПОЛІТЕХНІЧНИЙ ІНСТИТУТ
імені ІГОРЯ СІКОРСЬКОГО»
НАВЧАЛЬНО-НАУКОВИЙ ФІЗИКО-ТЕХНІЧНИЙ ІНСТИТУТ
Кафедра інформаційної безпеки**

До захисту допущено
Завідувач кафедри

_____ **Дмитро ЛАНДЕ**
(підпис)
« _____ » _____ 2025 р.

Дипломна робота
на здобуття ступеня бакалавра
за освітньо-професійною програмою «Системи, технології та математичні
методи кібербезпеки»
спеціальності 125 «Кібербезпека»
на тему: Вразливості протоколу SS7 в умовах інтеграції з IP мережами

Виконав (-ла): здобувач вищої освіти **IV** курсу, групи ФБ-14
(шифр групи)

_____ **Цибуленко-Сігов Ілля Миколайович** _____
(прізвище, ім'я, по батькові) (підпис)

Керівник доцент кафедри ІБ к.т.н., доцент Гальчинський Леонід Юрійович _____
(посада, науковий ступінь, вчене звання, прізвище, ім'я, по батькові) (підпис)

Рецензент _____
(посада, науковий ступінь, вчене звання, науковий ступінь, прізвище, ім'я, по батькові) (підпис)

Засвідчую, що у цій дипломній роботі немає
запозичень з праць інших авторів без відповідних
посилань.
Здобувач вищої освіти _____
(підпис)

Київ – 2025 року

НАЦІОНАЛЬНИЙ ТЕХНІЧНИЙ УНІВЕРСИТЕТ УКРАЇНИ
«КИЇВСЬКИЙ ПОЛІТЕХНІЧНИЙ ІНСТИТУТ
імені ІГОРЯ СІКОРСЬКОГО»
НАВЧАЛЬНО-НАУКОВИЙ ФІЗИКО-ТЕХНІЧНИЙ ІНСТИТУТ
Кафедра інформаційної безпеки

Рівень вищої освіти – перший (бакалаврський)

Спеціальність – 125 «Кібербезпека»

Освітньо-професійна програма «Системи, технології та математичні методи кібербезпеки»

ЗАТВЕРДЖУЮ

Завідувач кафедри

_____ Дмитро ЛАНДЕ

(підпис)

«__» _____ 2025 р.

ЗАВДАННЯ
на дипломну роботу здобувачу вищої освіти

Цибуленко-Сігову Іллі Миколайовичу

(прізвище, ім'я, по батькові)

1. Тема роботи «Вразливості протоколу SS7 в умовах інтеграції з IP мережами»

керівник роботи доцент кафедри ІБ, к.т.н., доцент Гальчинський Л.Ю.

(прізвище, ім'я, по батькові, науковий ступінь, вчене звання)

затверджені наказом по університету від «26» травня 2025 р. No 1761-с

2. Термін подання здобувачем вищої освіти роботи «16» травня 2025 р.

3. Вихідні дані до роботи: Літературні джерела, дані про існуючі вразливості, GSMA FS.11 (SS7 Interconnect Security Monitoring and Firewall Guidelines)

4. Зміст роботи: дослідження стеків протоколів SS7 та SIGTRAN, аналіз вразливостей SS7 у гібридних мережах, симуляції атак за допомогою SiGPloit, аналіз отриманих результатів симуляції атак, категоризація виявлених атак згідно з настановами GSMA FS.11, надання рекомендацій щодо запобігання вразливостям.

5. Перелік ілюстративного матеріалу (із зазначенням плакатів, презентацій тощо): презентація.

6. Дата видачі завдання: 07.11.2024

7. Календарний план

№ з/п	Назва етапів виконання дипломної роботи	Термін виконання етапів дипломної роботи	Примітка
1	Формулювання завдання та тематики дипломної роботи	14.10.2024 - 07.11.2024	Виконано
2	Пошук та опрацювання літературних джерел	08.11.2024 - 02.03.2025	Виконано
3	Огляд процесу обміну повідомленнями в 2G/3G мережах	03.03.2025 - 23.03.2025	Виконано
4	Ознайомлення зі стеком протоколів SS7 та SIGTRAN	24.03.2025 - 31.03.2025	Виконано
5	Ознайомлення з методами симуляції мережі SIGTRAN та генерування в ній трафіку	01.04.2025 - 14.04.2025	Виконано
6	Проходження переддипломної практики	14.04.2025 - 16.05.2025	Виконано
7	Формування рекомендацій щодо пом'якшення ризиків у мобільних мережах	19.05.2025 - 23.05.2025	Виконано
8	Оформлення дипломної роботи відповідно до методичних вказівок	26.05.2025 - 09.06.2025	Виконано
9	Передзахист дипломної роботи	16.06.2025	
10	Захист дипломної роботи	23.06.2025	

Здобувач вищої освіти

(підпис)

Керівник роботи

(підпис)

Ілля ЦИБУЛЕНКО-СІГОВ
(Власне ім'я, ПРІЗВИЩЕ)

Леонід ГАЛЬЧИНСЬКИЙ
(Власне ім'я, ПРІЗВИЩЕ)

РЕФЕРАТ

Обсяг роботи 104 сторінки, 33 ілюстрації, 7 таблиць, 6 додатків, 27 джерел літератури.

Об'єкт дослідження: процеси передачі сигнальних повідомлень SS7 через IP-мережі за допомогою протоколів SIGTRAN.

Предмет дослідження: вразливості сигнальних мереж SS7/SIGTRAN та методи їх усунення.

Мета дослідження: Зменшення ризиків компрометації конфіденційності та цілісності даних абонентів у конвергентних SS7/IP мережах шляхом виявлення, демонстрації та розробки рекомендацій щодо протидії актуальним атакам.

Методи дослідження: Аналіз літературних джерел, симуляція мережі SS7 та генерування трафіку зі зловмисним вмістом, розробка рекомендацій.

Отримані результати: Визначено типи атак. Для кожного типу атак на протокол SS7 розроблено рекомендації щодо пом'якшення існуючих ризиків.

Результати роботи були представлені на XXIII Всеукраїнській науково-практичній конференції студентів, аспірантів та молодих вчених.

Ключові слова: SS7, SIGTRAN, система сигналізації, вразливості, мережі

ABSTRACT

This work contains 104 pages, 33 illustrations, 7 tables, 6 appendices, 27 references.

Object of research: security of SS7-over-IP (SIGTRAN) networks.

Subject of research: the process of messaging in 2G and 3G networks.

Purpose of the study: Reducing the risks of compromising subscriber data confidentiality and integrity in convergent SS7/IP networks by identifying, demonstrating, and developing recommendations for countering relevant attacks.

Research methods: Literature analysis, simulation of the SS7 network and generation of traffic with malicious content, development of recommendations.

Results: The types of attacks are determined. For each type of attack on the SS7 protocol, recommendations have been developed to mitigate existing risks.

The results of the work were presented at the XXIII All-Ukrainian Scientific and Practical Conference of Students, Postgraduates and Young Scientists.

Keywords: SS7, SIGTRAN, signaling system, vulnerabilities, networks

ЗМІСТ

ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ, СИМВОЛІВ, ОДИНИЦЬ, СКОРОЧЕНЬ І ТЕРМІНІВ	7
ВСТУП	10
1 ПРОТОКОЛ SS7	15
1.1 Історія	15
1.2 Основні поняття SS7	16
1.3 SS7 в GSM	29
1.4 SIGTRAN	34
1.5 Інтегрована Мережева Архітектура SIGTRAN	43
Висновки до розділу 1	47
2 ВРАЗЛИВОСТІ SS7	49
2.1 Вразливості SS7 у гібридних мережах	49
2.2 Симуляція SS7	50
2.3 SiGPloit Реалізація Симуляції Мережі SS7/SIGTRAN	52
2.4 SiGPloit Реалізація Симуляції Мережі SS7/SIGTRAN	56
Висновки до розділу 2	61
3 СИМУЛЯЦІЯ АТАК SS7	62
3.1 Network enumeration	62
3.2 IMSI Catch	66
3.3 Any Time Interrogation	69
3.4 Provide Subscriber Info	72
3.5 MITM (Update Location)	75
3.6 SMS Spoofing	79
Висновки до розділу 3	82
4 РЕКОМЕНДАЦІЇ	84
4.1 Категорії атак GSMA FS.11	85
4.2 Рекомендації	86
ВИСНОВКИ	93
ПЕРЕЛІК ДЖЕРЕЛ ПОСИЛАНЬ	96
ДОДАТОК А	98
ДОДАТОК Б	99
ДОДАТОК В	100
ДОДАТОК Г	101
ДОДАТОК Д	102
ДОДАТОК Е	103

ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ, СИМВОЛІВ, ОДИНИЦЬ, СКОРОЧЕНЬ І ТЕРМІНІВ

3G (англ. 3rd Generation) – третє покоління технології мобільного зв'язку

2G (англ. 2nd Generation) – друге покоління технології мобільного зв'язку

BSC (англ. Base Station Controller) – контролер базової станції

BSSAP (англ. Base Station Subsystem Application Part) – Прикладна частина підсистеми базової станції

BTS (англ. Base Transceiver Station) – базова приймально-передавальна станція

CAS (англ. Channel Associated Signaling) – система каналної сигналізації

CLEC (англ. Competitive Local Exchange Carriers) – Конкурентні Місцеві Оператори Зв'язку

CRC (англ. Cyclic redundancy check) – циклічний надлишковий код

FISU (англ. Fill In Signal Units) – одиниці сигналу заповнення

GMSC (англ. Gateway Mobile Switching Server) – шлюзовий мобільний комутаційний центр

GSM (англ. Global System for Mobile Communications) – глобальна система мобільного зв'язку

HLR (англ. Home Location Register) – реєстр домашнього розташування

IETF (англ. Internet Engineering Task Force) – відкрите міжнародне співтовариство проектувальників, учених, мережевих операторів і провайдерів

IMSI (англ. International Mobile Subscriber Identity) – міжнародний ідентифікатор користувача мобільного зв'язку

IP (англ. Internet protocol) – інтернет протокол

ISDN (англ. Integrated Services Digital Network) – Цифрова Мережа з Інтегрованими Послугами

ISUP (англ. ISDN User Part) – протокол, що замінив TUP

ITU (англ. International Telecommunication Union) – міжнародна спілка електрозв'язку

LAP-D (англ. Link Access Protocol for the ISDN “D” channel) – протокол доступу до каналу ISDN «D»

Linkset - набір каналів

LSSU (англ. Link Status Signal Units) – одиниці сигналу стану з’єднання

MAP (англ. Mobile Application Part) – Мобільна прикладна частина

MSC (англ. Mobile Switching Centre) – мобільний комутаційний центр

MSU (англ. Message Signal Units) – одиниці сигналу повідомлення

MTP (англ. Message Transfer Part) – рівень передачі повідомлень в SS7

MTP1 (англ. MTP Level 1) – фізичний рівень SS7

MTP2 (англ. MTP Level 2) – канальний рівень SS7

MTP3 (англ. MTP Level 3) – мережевий рівень SS7

Multihoming – властивість мережевого протоколу або системи мати кілька незалежних підключень до мережі

NGN (англ. Next generation network) – мережа наступного покоління

OSI (англ. Open Systems Interconnection) – модель Взаємодії Відкритих Систем

PSTN (англ. Public switched telephone network) – телефонна мережа загального користування

SCCP (англ. Signaling Connection Control Part) – протокол мережевого рівня, що відповідає за маршрутизацію в SS7 над MTP

SCP (англ. Service Control Point) – точка управління послугами

SCTP (англ. Stream Control Transmission Protocol) – протокол передачі з керуванням потоком

SG (англ. Signaling Gateway) – Сигнальний шлюз

SIGTRAN (англ. Signaling Transportation) – група телекомунікаційних протоколів, розширення SS7

SMS (англ. Short Message Service) – служба коротких повідомлень

SP (англ. Signaling Point) – сигнальна точка

SPC (англ. Signaling Point Code) – код точки сигналізації

SS7 (англ. Signaling System No. 7) – система сигналізації N7

SSP (англ. Service Switching Point) – точка комутації послуг

STP (англ. Service Transfer Point) – точка передачі сигналів

SU (англ. Signal Unit) – сигнальна одиниця

TCAP (англ. Transaction Capabilities Application Part) – Прикладна частина транзакційних можливостей

TCB (англ. Transport Control Block) – блок керування транспортуванням

TCP (англ. Transmission Control Protocol) – протокол управління передачею

TDM (англ. Time Division Multiplexing) – мультиплексування з поділом за часом, часове ущільнення

TUP (англ. Telephone User Part) – протокол для встановлення та завершення голосових дзвінків SS7.

UDP (англ. User Datagram Protocol) – Протокол датаграм користувача

UMTS (англ. Universal Mobile Telecommunications System) – універсальна мобільна телекомунікаційна система

VLR (англ. Visitors Location Register) – реєстр віддаленого розташування

ВСТУП

Актуальність роботи:

У сучасному світі відбувається стрімкий розвиток телекомунікацій та інформаційних технологій, мобільні мережі стали наріжним каменем сучасної інфраструктури, забезпечуючи зв'язок багатьох мільйонів користувачів по всьому світу. Протокол SS7 (Signaling System No. 7), є основою стільникових мереж, розроблений у 1970-х роках, та впроваджений як міжнародний стандарт Міжнародною спілкою електрозв'язку (ITU). Стандарт визначає процедури і протокол, за допомогою яких мережеві елементи телефонної мережі загального користування (PSTN) обмінюються інформацією через мережу цифрової сигналізації для здійснення налаштування, маршрутизації та контролю бездротових (стільникових) і дротових викликів.

Традиційні мережі SS7 побудовані з дотриманням високих вимог до надійності та продуктивності. Вони мають високий ступінь резервування, що зменшує час простою мережі сигналізації, передаючи трафік по резервних каналах у випадку відмови основного. Незважаючи на це, мережі SS7 не настільки масштабовані, як IP-мережі, через що їх розширення стає дорогим і складним процесом. Однак попит на сигнальні мережі SS7 стрімко зростає завдяки масовій популярності мобільних послуг зв'язку та експоненційному збільшенню кількості користувачів мобільних телефонів.

Зростання попиту на послуги, такі як Media over IP (MoIP), спонукає операторів зв'язку до переходу на новітні мережі, що краще підтримують передачу пакетів даних. У цьому контексті IP вважається найперспективнішим мережевим протоколом, оскільки він забезпечує покращене використання ресурсів та знижує витрати на експлуатацію, обслуговування та інфраструктуру мережі.

Перехід від традиційних мереж SS7 до IP-базованих Next Generation Networks (NGN) не відбувається миттєво — співіснування цих технологій очікується протягом тривалого часу, можливо навіть десятиліть. Основний виклик полягає в інтеграції цих двох типів мереж, що робить актуальним використання архітектур, які поєднують класичні мережі SS7 з IP-мережами, застосовуючи останні для транспортування сигнальних повідомлень SS7.

З метою вирішення цієї проблеми група Signaling Transportation (SIGTRAN) робочої групи Internet Engineering Task Force (IETF) розробила новий набір сигнальних протоколів, що дозволяють передавати повідомлення SS7 через IP-мережі [1]. SIGTRAN використовує протокол Stream Control Transmission Protocol (SCTP), який забезпечує багатоканальність та multihoming, що створює необхідний рівень надійності та відмовостійкості, подібний до традиційних мереж SS7.

Незважаючи на високу надійність та продуктивність, традиційні мережі SS7 мають суттєві вразливості в питаннях безпеки. Це зумовлено тим, що протокол був розроблений у часи, коли кіберзагрози не мали такого масштабу та складності, як сьогодні.

Від початку SS7 використовував підхід “walled garden” (із англ. - огорожений сад), тобто оператори безумовно взаємно довіряють один одному — мережа SS7 вважалась як довірена закрита мережа. Зазвичай мережі SS7 дуже безпечні, оскільки вони є власністю компанії, а обладнання зберігається в приміщеннях, що надійно охороняються, з обмеженим фізичним доступом для співробітників.

Однак сьогодні мережеві провайдери можуть відкривати свої мережі SS7 для третіх сторін в якості комерційних пропозицій, що може призвести до появи вразливостей. Атаки на SS7 можуть мати серйозні наслідки і, в залежності від їх характеру, дозволять отримати доступ до місцезнаходження користувача та деталей дзвінків/SMS.

Крім того, перехід до IP-мереж не лише відкриває нові можливості, але й піддає сигнальні повідомлення SS7 кіберзагрозам, які можуть надходити зі сторони пакетних мереж, націлені на конкретний вузол сигналізації SIGTRAN в мережі з комутацією каналів. Передача колись безпечних сигнальних повідомлень SS7 на основі TDM через загальнодоступні IP-мережі у вигляді пакетів з корисним навантаженням відкриває ці повідомлення для кіберзагроз, які можуть бути легко запущені з боку IP-мереж, зокрема Інтернету. Витік даних, фішингові атаки, шпигунське програмне забезпечення, злом криптографічного захисту, перехоплення IMSI користувача за допомогою фальшивої базової станції [2] та багато інших атак можуть призвести до перехоплення як мережевих, так і абонентських даних, обмежити абонентський доступ, викликавши перевантаження, та/або поставити під загрозу безпеку всієї мобільної мережі.

Мета дослідження: зменшення ризиків компрометації конфіденційності та цілісності даних абонентів у конвергентних SS7/IP мережах шляхом виявлення, демонстрації та розробки рекомендацій щодо протидії актуальним атакам.

Завдання дослідження:

1. Проаналізувати архітектурні особливості та механізми функціонування протоколів SS7 та SIGTRAN для ідентифікації теоретичних передумов вразливостей.
2. Розгорнути симуляційне середовище та експериментально продемонструвати ланцюжок атак, починаючи від розвідки мережі і закінчуючи перехопленням даних абонента.
3. Класифікувати реалізовані атаки згідно з настановами GSMA FS.11 та розробити практичні рекомендації щодо запобігання виявленим загрозам.

Об'єкт дослідження: Процеси передачі сигнальних повідомлень SS7 через IP-мережі за допомогою протоколів SIGTRAN.

Предмет дослідження: Вразливості сигнальних мереж SS7/SIGTRAN та методи їх усунення.

Методи дослідження: У роботі застосовувалися методи системного аналізу, аналіз літературних джерел, експериментальне тестування в симульованому середовищі, аналіз мережевого трафіку (з використанням Wireshark), а також аналіз галузевих стандартів та розробка рекомендацій.

Наукова новизна одержаних результатів:

Систематизовано та експериментально підтверджено комплексний набір актуальних вразливостей SS7/SIGTRAN мереж, що охоплюють як етапи розвідки мережі, так і безпосередні атаки на конфіденційність абонентів та цілісність їхніх комунікацій.

Здійснено детальну класифікацію реалізованих атак у відповідності до категорій загроз, визначених провідним галузевим стандартом GSMA FS.11, що підкреслює їхню відповідність реальним загрозам та підвищує наукову цінність дослідження.

Надано узагальнені рекомендації щодо запобігання виявленим вразливостям, які ґрунтуються на практичних результатах експериментів та розширеному аналізі стандартів безпеки, що дозволяє адаптувати їх до сучасних умов конвергентних мереж.

Практичне значення одержаних результатів:

Результати дослідження надають операторам мобільного зв'язку та провайдерам телекомунікаційних послуг чітке розуміння актуальних загроз безпеці їхніх SS7/SIGTRAN інфраструктур, що базується на практичних демонстраціях атак.

Сформульовані рекомендації можуть бути безпосередньо використані для посилення захисту сигнальних мереж, зокрема, для налаштування SS7/SIGTRAN міжмережевих екранів, впровадження систем виявлення вторгнень та оптимізації правил фільтрації трафіку.

Матеріали дипломної роботи можуть служити практичним посібником для фахівців з мережевої безпеки, які працюють з SS7/SIGTRAN, а також бути включені до навчальних програм для підготовки майбутніх експертів у галузі телекомунікаційної безпеки.

Дослідження сприяє підвищенню загальної обізнаності щодо важливості безпеки сигнальних мереж, стимулюючи розробку та впровадження нових, більш стійких захисних рішень.

Апробація результатів роботи: Результати дослідження були представлені на XXIII Всеукраїнської науково-практичної конференції студентів, аспірантів та молодих вчених «Теоретичні і прикладні проблеми фізики, математики та інформатики» (14 - 17.05.2025 р., м. Київ, Україна), та доповнено рекомендації в подальшій роботі.

1 ПРОТОКОЛ SS7

1.1 Історія

У ранніх телекомунікаційних мережах в різних частинах світу існувало багато різних систем сигналізації зі своїми стандартами. Це створювало проблеми під час дзвінків між мережами з різними типами сигналізації. Потрібно було запровадити стандарт для узгодження комунікації між мережами.

Перед ITU було поставлено завдання знайти загальний стандарт, за допомогою якого всі системи сигналізації могли б працювати разом. В якості загального стандарту було рекомендовано систему каналної сигналізації CAS, в якій керуючі сигнальні повідомлення для синхронізації і вирівнювання кадрів передаються тими ж каналами, що і трафік (голос і дані). В системах CAS сигнальні повідомлення надсилаються тільки тоді, коли передається трафік. Це створює вузькі місця в телекомунікаційних мережах, а також марно витрачає пропускну здатність. Як наслідок, цей тип сигналізації краще підходить для мереж з низькою пропускну здатністю.

У 1970-х роках ITU, як стандарт для сигналізації в PSTN, була розроблена більш надійна та відмовостійка система з високим ступенем резервування – протокол Common Channel Signaling System No. 7 (SS7). Його основна мета – забезпечення обміну службовими повідомленнями між елементами телекомунікаційної мережі поза каналом безпосереднього обміну трафіком.

На рисунку нижче (Рисунок 1.1) показано різницю між сигнальними системами CAS та SS7.

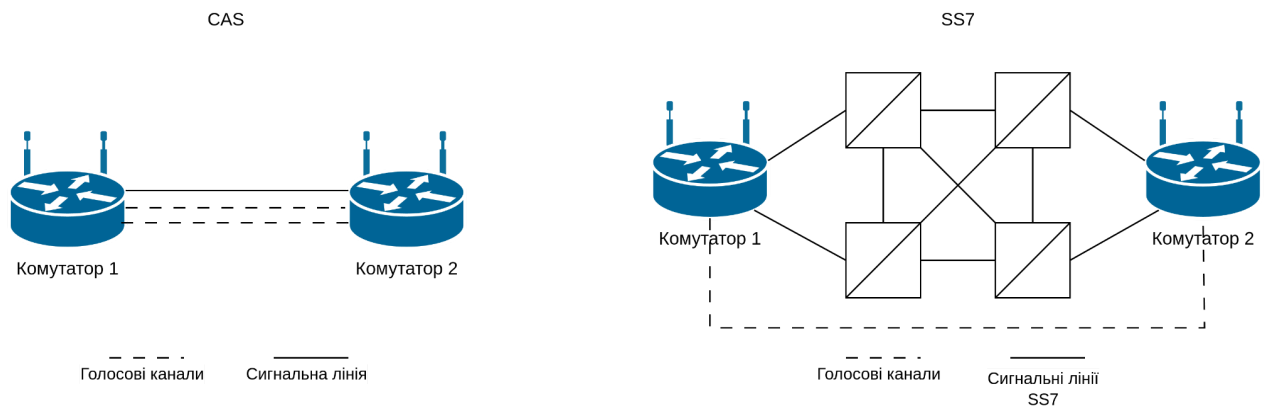


Рисунок 1.1 – Структури каналів у системах CAS та SS7

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, використовувати додаткові сервіси, такі як переадресація викликів чи ідентифікація номера.

1.2 Основні поняття SS7

1.2.1 Архітектура SS7

Архітектура SS7 складається з трьох основних типів вузлів, відомих як Точки Сигналізації (SP) в залежності від їх функціональних можливостей. До них відносяться точка комутації послуг (SSP), точка передачі сигналів (STP) і точка управління послугами (SCP). Кожна точка в мережі ідентифікується унікальним 14-бітним цілим числом, відомим як код точки сигналізації (SPC), що дозволяє маршрутизацію повідомлення між SP.

Точки з'єднуються між собою сигнальними лініями, пропускна здатність яких зазвичай становить 56 або 64 кбіт/с [3]. Для забезпечення більшої пропускної здатності та надлишковості сигнальної мережі, між будь-якими

двома SP може використовуватись до 16 каналів. Комбінація всіх каналів між будь-якими двома SP називається набором каналів (linkset).

Точки комутації сигналів (SSPs) – це телефонні комутатори, які перетворюють набраний номер у повідомлення сигналізації SS7. Вони налаштовують, управляють і завершують голосові виклики, використовуючи протоколи ISUP і TCAP. Основне завдання — визначати маршрути виклику за допомогою таблиць.

Точки передачі сигналів (STPs) – діють як маршрутизатори в мережі SS7. Вони передають повідомлення між різними точками сигналізації. Якщо SSP не знає адреси отримувача, STPs забезпечують її визначення. Вони також вимірюють трафік і можуть конвертувати протоколи.

Точки управління (SCPs) – забезпечують доступ до застосунків через примітиви. Примітив - це інтерфейс, який забезпечує доступ з одного рівня протоколу на інший рівень. Зокрема використовуються для доступу до баз даних через протокол TCAP.

Усі SP з'єднані лініями сигналізації. Лінії сигналізації SS7 характеризуються відповідно до їх використання в мережі сигналізації. Практично всі канали ідентичні, оскільки є двонаправленими каналами передачі даних зі швидкістю 56 кбіт/с або 64 кбіт/с, які підтримують однакові протоколи нижніх рівнів. Відмінність між каналами полягає лише в їх використанні у мережі сигналізації.

Нижче на рисунках (Рисунок 1.2, Рисунок 1.3) наведено приклад мережі SS7 та які канали застосовуються між SP.



Рисунок 1.2 – Умовні позначення SP

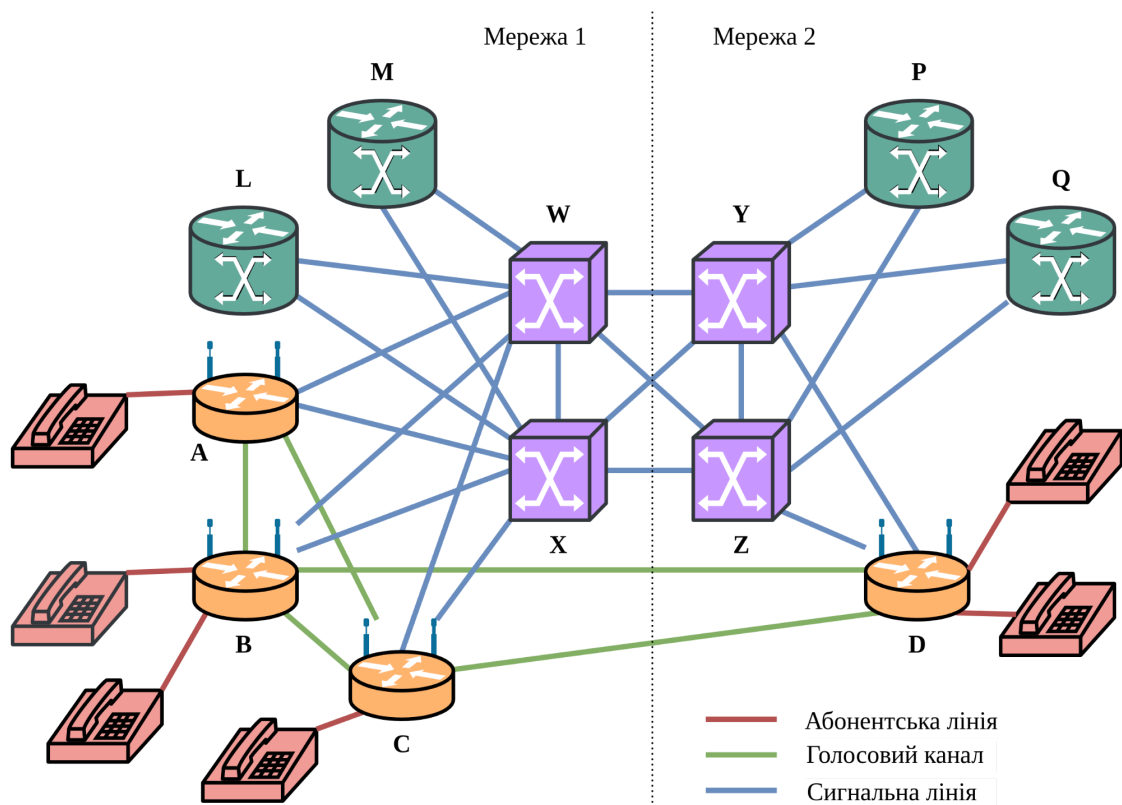


Рисунок 1.3 – Приклад мережі SS7 [4]

Зверніть увагу на такі моменти:

- STP W та X виконують однакові функції і є резервними. Разом вони називаються парою STPs. Аналогічно, STP Y та Z утворюють таку ж пару.
- Кожен SSP має два з'єднання (або linkset) – по одному до кожного з STP пари. Уся сигналізація SS7 надсилається через ці з'єднання. Оскільки STP в парі є резервними, повідомлення, надіслані через будь-яке з'єднання (до будь-якого STP), обробляються однаково.
- STP в парі обов'язково з'єднані.
- Дві пари STP з'єднуються чотирма лінками, утворюючи linkset, що називається квадом (quad).
- SCP зазвичай (але не завжди) розгортаються парами. Як і у випадку з STP, SCP в парі функціонують однаково. Пари SCP також називаються парою SCP. Зверніть увагу, що вони не з'єднані напряму.

- Такі архітектури сигналізації, які забезпечують непрямі шляхи сигналізації між елементами мережі, називаються квазі асоційованою сигналізацією.

Усі SP з'єднані лініями сигналізації. Лінії сигналізації SS7 характеризуються відповідно до їх використання в мережі сигналізації. Практично всі канали ідентичні, оскільки є двонаправленими каналами передачі даних зі швидкістю 56 кбіт/с або 64 кбіт/с, які підтримують однакові протоколи нижніх рівнів. Відмінність між каналами полягає лише в їх використанні у мережі сигналізації.

Тип А – лінії доступу (англ. A-Access). Використовуються для з'єднання SSP з STP або STP з SCP

Канал «А» з'єднує кінцеву точку сигналізації (наприклад, SCP або SSP) з STP. По каналу А передаються тільки повідомлення, що походять від кінцевого пункту сигналізації або призначені для нього.

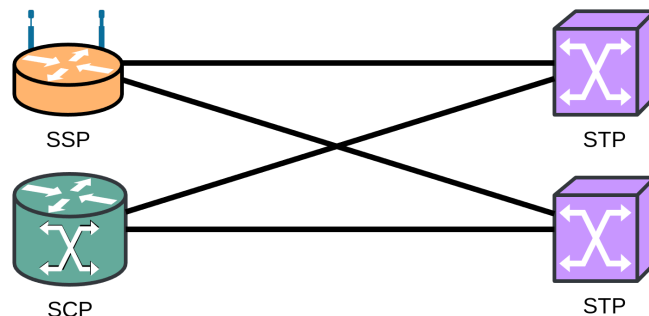


Рисунок 1.4 – Лінії «А»

Тип В – мостові з'єднання (англ. B-Bridge). Використовуються для з'єднання парних STP з іншими парними STP).

Канал «В» з'єднує STP з іншим STP. Як правило, четвірка каналів типу «В» з'єднує однорангові STP (наприклад, STP однієї мережі з STP іншої мережі).

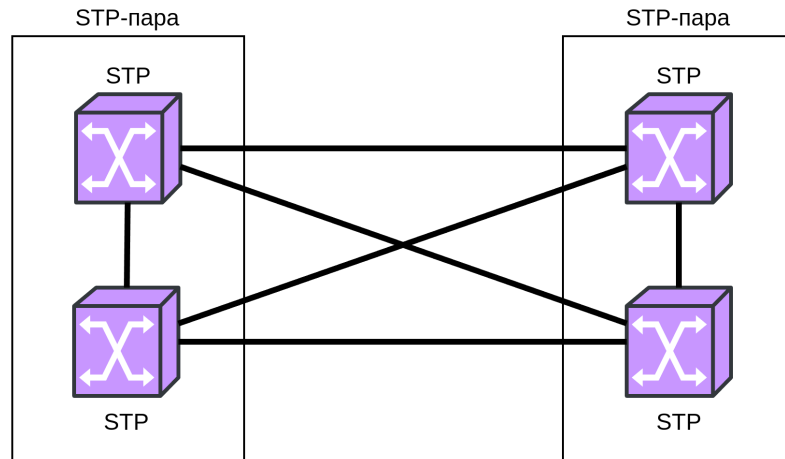


Рисунок 1.5 – Лінії «В»

Тип С – перехресні з'єднання (англ. C-Cross) Використовуються для з'єднання парних STP.

Канал «С» з'єднує STP, що виконують ідентичні функції, у спарену пару. З'єднання типу «С» використовується тільки тоді, коли STP не має іншого маршруту до пункту призначення через несправність з'єднання (збої в роботі з'єднання). SCP також можуть бути розгорнуті попарно для підвищення надійності, однак, на відміну від STP, спарені SCP не з'єднані між собою сигнальними лініями.

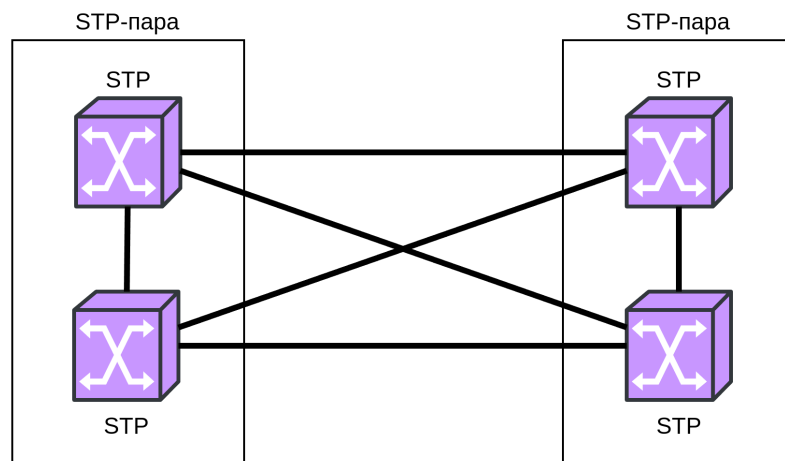


Рисунок 1.6 – Лінії «С»

Тип D – діагональні канали (англ. D-Diagonal). Використовуються для з'єднання парних STP на одному рівні ієрархії з парними STP на іншому рівні ієрархії.

Канал «D» з'єднує вторинну (локальну або регіональну) пару STP з первинною (наприклад, міжмережевий шлюз) парою STP у чотириланковій конфігурації. Вторинні STP в одній мережі з'єднуються за допомогою чотирьох каналів D. Різниця між каналами «B» і «D» є досить умовною, тому, такі зв'язки можуть називатися B/D зв'язками.

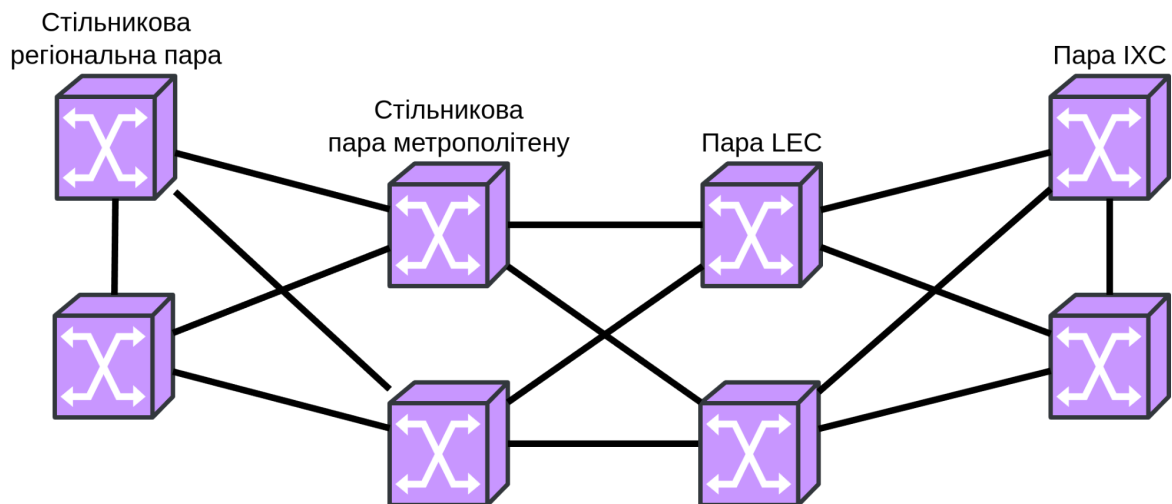


Рисунок 1.7 – Лінії «D»

Тип E – розширюючі канали (англ. E-Extended). З'єднують точки доступу до альтернативних або віддалених STP для підвищення відмовостійкості та розподілу навантаження.

Канал «E» з'єднує точку доступу з альтернативною точкою доступу STP. Лінії E забезпечують альтернативний шлях передачі сигналу, якщо домашня точка доступу SSP не може бути досягнута через лінію A. Зазвичай канали E створюються лише тоді, коли вищий рівень надійності буде вартий додаткових витрат.

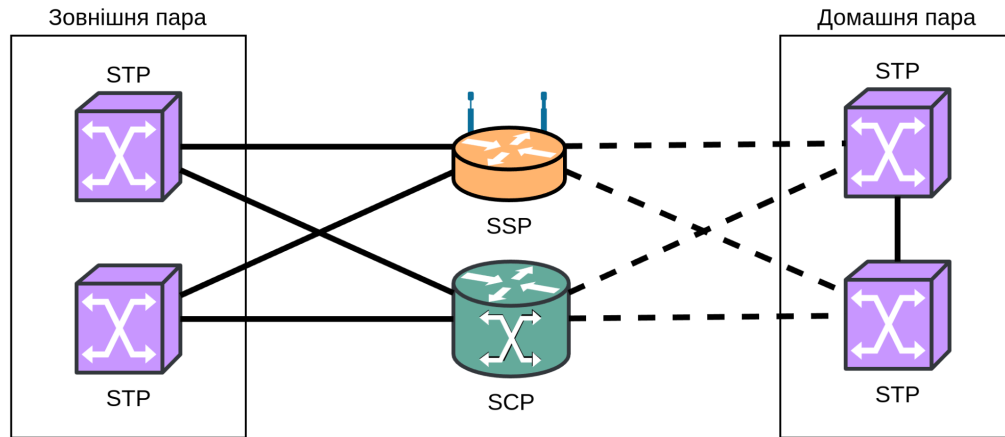


Рисунок 1.8 – Лінії «Е»

Тип F - повністю асоційовані з'єднання (англ. Fully associated).

Використовується для з'єднання SSP, коли між ними проходить значний об'єм трафіку.

Канал «F» з'єднує дві кінцеві точки сигналізації (тобто, SSP і SCP).

Зазвичай такі лінії не використовуються в мережах з STP. У мережах без STP, F канали безпосередньо з'єднують точки сигналізації.

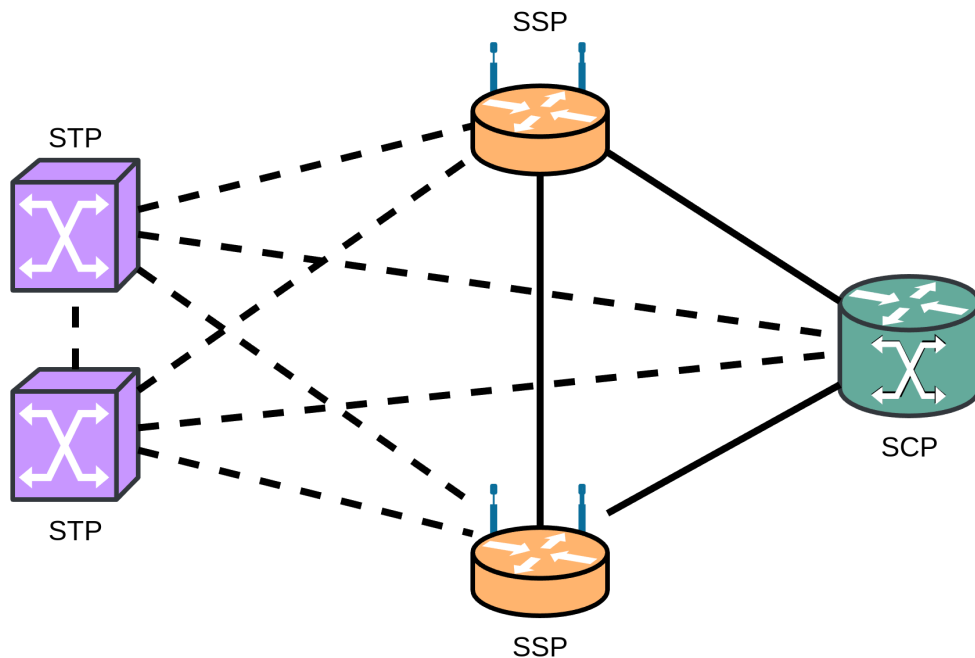


Рисунок 1.9 – Лінії «F»

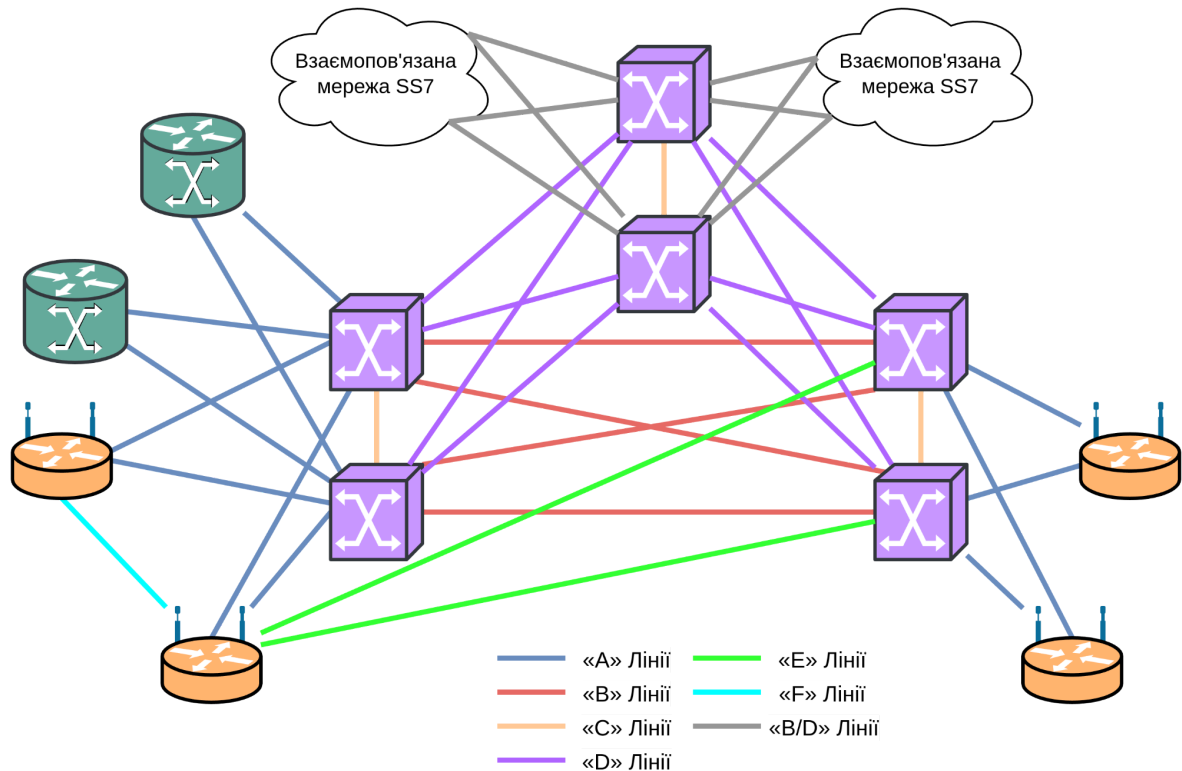


Рисунок 1.10 – Приклад використання ліній різних типів

Повідомлення (сигнал), що передається через мережу SS7, міститься в пакетах даних, які називаються сигнальними одиницями (SU). Існує три основні типи сигнальних одиниць. До них відносяться: сигнали заповнення (FISU), сигнали стану з'єднання (LSSU) та сигнали повідомлення (MSU).

FISU надсилаються, коли сигнальна лінія простоє. Це рекомендується для того, щоб інформація про помилки каналу була доступною навіть коли не передається інформація вищих рівнів. Таким чином, забезпечується швидке реагування на проблеми в мережі SS7 для мінімізації перебоїв постачання сервісу.

LSSU використовуються на сигнальному рівні каналу для переведення його у потрібний стан. Як і FISU, LSSU надсилаються безперервно між SP.

MSU несуть фактичну інформацію верхнього рівня, яка містить прапори керування, що вказують на протокол, який передається, наприклад, ISDN User Part (ISUP), коди точок (SPC) відправлення та призначення, а також поле змінної довжини – безпосередньо вміст повідомлення.

1.2.2 Стек протоколів SS7

Апаратні та програмні функції стеку протоколу SS7 поділяються на рівні, які можна порівняти з моделлю Взаємодії Відкритих Систем (OSI) для сумісності між різними системами, виготовленими різними виробниками. На рисунку 12 показані різні компоненти, які складають стек протоколу SS7.

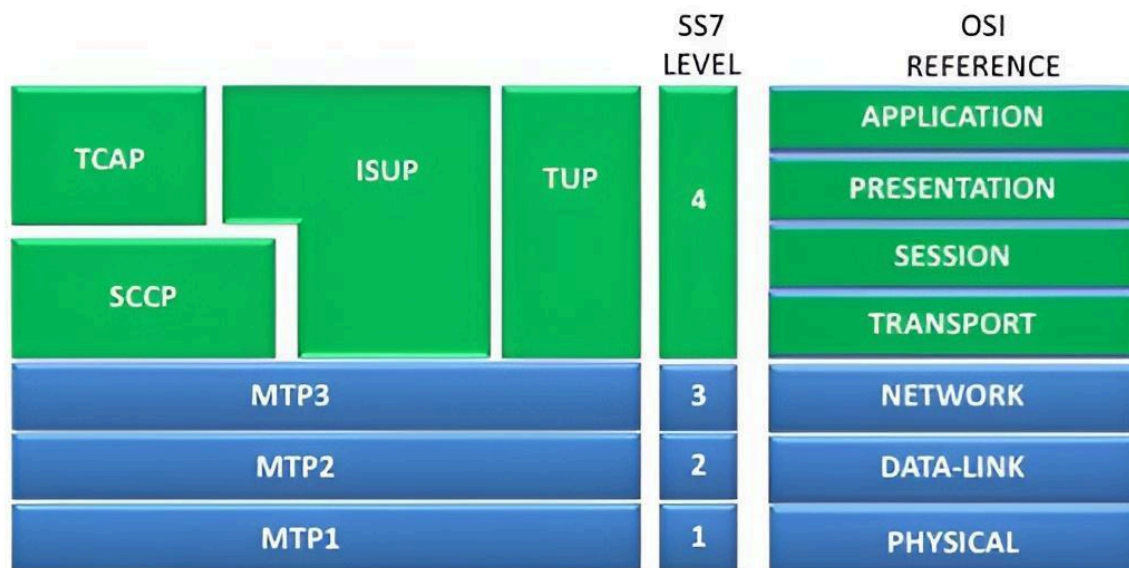


Рисунок 1.11 – Стек протоколів SS7, PSTN [5]

У стеку протоколів SS7 верхні рівні (4-7), що за функціоналом відповідають транспортному, сеансовому, представлення та прикладному, об'єднані в один.

Message Transfer Part (MTP)

MTP – це рівень протоколу SS7, що забезпечує передачу повідомлень між вузлами мережі. Він відповідає за встановлення з'єднання між фізичними мережевими вузлами, контроль помилок, коригування помилок та визначення порядку повідомлень. MTP також виконує маршрутизацію, фільтрацію та розподіл повідомлень у межах одного вузла. Його функціонал поділяється на три рівні. [5]

MTP Level 1 (Фізичний рівень)

MTP1 визначає фізичні, електричні та функціональні характеристики сигнального каналу. До підтримуваних інтерфейсів належать:

- E-1 (2048 кбіт/с, 32 канали по 64 кбіт/с),
- DS-1 (1544 кбіт/с, 24 канали по 64 кбіт/с),
- V.35 (64 кбіт/с),
- DS-0 (64 кбіт/с) і DS-0A (56 кбіт/с). [\[5\]](#)

MTP Level 2 (Канальний рівень)

MTP2 визначає механізми контролю та корекції помилок під час передачі повідомлень через сигнальні канали, виконуючи функції, аналогічні канальному рівню моделі OSI. Він забезпечує коректну доставку повідомлень між вузлами, регулює швидкість передачі, щоб уникнути перевантаження. Крім того використовує циклічний надлишковий код (CRC) для виявлення помилок і повторної відправки пошкоджених повідомлень. MTP2 визначає тип отриманого SU за індикатором довжини повідомлення. [\[4\]](#)

MTP Level 3 (Мережевий рівень)

MTP3 виконує функції маршрутизації, розподілу та контролю сигналізаційного трафіку в межах мережі. Його робота базується на послугах MTP2, що гарантує надійність передачі. MTP3 визначає оптимальний шлях для передачі сигналізації між вузлами, ідентифікує повідомлення та спрямовує їх до відповідних SP. Якщо певний вузол або канал виходить з ладу, третій рівень перенаправляє трафік альтернативними маршрутами, регулює потік повідомлень у разі надмірного навантаження на мережу, щоб уникнути збоїв. [\[5\]](#)

Четвертий рівень функціонально відповідає транспортному, сеансовому, представлення та прикладному рівням моделі OSI. Він включає наступні 4 протоколи:

Signaling Connection Control Part (SCCP) забезпечує дві ключові функції, яких не вистачає в MTP.

Перша – це можливість адресації додатків усередині сигнального вузла. На відміну від MTP, який може тільки приймати та передавати повідомлення для вузла в цілому, SCCP дозволяє взаємодіяти безпосередньо з конкретними програмними застосунками (підсистемами) у межах цього вузла.

У той час як мережеві керуючі повідомлення MTP та базові сигнали встановлення виклику адресуються всьому вузлу, інші типи повідомлень використовуються окремими підсистемами в межах вузла. До таких підсистем належать, наприклад, обробка викликів на номери 800, обробка карток передплати, передові інтелектуальні мережі (AIN), а також спеціальні локальні сигнальні сервіси (CLASS), такі як повторний набір номера або повернення виклику. SCCP дозволяє чітко адресувати ці підсистеми, забезпечуючи коректну маршрутизацію повідомлень. [5]

Telephone User Part (TUP) – застарілий протокол, який використовувався у аналогових телефонних системах для встановлення та завершення голосових дзвінків. Він працює виключно з аналоговими каналами зв'язку. Сьогодні TUP майже повністю замінений ISDN User Part (ISUP), однак все ще зустрічається в деяких країнах, таких як Китай та Бразилія. [5]

ISDN User Part (ISUP) визначає набір повідомлень і протоколів, які використовуються для встановлення, управління та завершення голосових і дата-викликів у телефонній мережі загального користування (PSTN). Крім того, ISUP відповідає за керування транковими лініями, на яких базуються ці з'єднання.

Попри свою назву, ISUP використовується як для ISDN-з'єднань, так і для звичайних телефонних викликів у не-ISDN мережах. У північноамериканській версії протоколу SS7 повідомлення ISUP передаються виключно через MTP, що забезпечує їх маршрутизацію між необхідними вузлами мережі. Проте, якщо

виклик відбувається в межах одного комутаційного вузла, ISUP-сигналізація не використовується. [5]

Transaction Capabilities Application Part (TCAP) визначає повідомлення та протокол, що використовуються для обміну інформацією між застосунками в різних вузлах мережі. TCAP зазвичай застосовується для обслуговування баз даних, таких як обробка карток для дзвінків, номери 800, а також для послуг інтелектуальних мереж (AIN). Крім того, він використовується для послуг міжкомутаційних з'єднань, зокрема для повторного набору номера та повернення дзвінків.

Оскільки повідомлення TCAP повинні бути доставлені до конкретних застосунків у вузлах, до яких вони адресовані, для їх транспортування використовується SCCP. [4]

1.2.3 Доступність SS7

Сигнальна мережа SS7 є фундаментом телекомунікаційної інфраструктури, з самого початку розроблялась із фокусом на високу продуктивність та надійність. Її архітектура включає вбудовані механізми виявлення та корекції помилок, а також забезпечує послідовну доставку сигнальних одиниць.

Основні вимоги до надійності та продуктивності SS7 описані в рекомендаціях ITU-T Q.706 [6] та Q.709 [7], і реалізуються через функціональність Message Transfer Part (MTP), яка забезпечує обслуговування протоколів верхнього рівня.

Ключові вимоги до надійності та продуктивності SS7:

- Ймовірність невиявленої помилки в сигнальній одиниці повідомлення (Message Signal Unit, MSU) не повинна перевищувати 1 на 10^{10} .

- Втрата повідомлень через збій у МТР повинна бути не частіше ніж 1 на 10^7 повідомлень.
- Доступність сигнального з'єднання між двома кінцевими точками сигналізації (SEP) повинна становити не менше 99.998%, що відповідає максимальному простою в 10 хвилин на рік.
- Порухення послідовності доставки повідомлень (включаючи дублювання) повинно відбуватись не частіше, ніж 1 на 10^{10} повідомлень.
- Час передачі повідомлень через STP (Signal Transfer Point) в нормальних умовах не повинен перевищувати 100 мс, також неявно зазначено що затримки в чергах не повинні займати більшу частину загального часу доставки.

Механізми досягнення вимог:

Вимога 1 реалізується за рахунок якісного фізичного середовища передачі, функції CRC на рівні МТР2 та мінімізації внутрішніх помилок реалізації системи.

Вимога 2 забезпечується використанням резервних сигнальних ліній і процедури перемикавання (change-over), яка дозволяє без втрат перенаправити трафік з несправного каналу на альтернативний – за умови, що закінчення сигнального з'єднання на обох вузлах ще працює і підтримується альтернативний шлях.

Для виконання вимоги 3, МТР використовує набір процедур для підтримки надмірності. Наприклад, виявлення збоїв на лініях 64 кбіт/с відбувається протягом 128 мс за допомогою монітора помилок МТР2. У разі доступності альтернативного маршруту, МТР3 автоматично ініціює процедуру перемикавання.

Для вимоги 4, МТР3 застосовує явний або таймерний контроль послідовності під час маршрутизації трафіку через альтернативні канали або при поверненні до основної лінії.

Хоча час передачі через STP є здебільшого питанням реалізації, а не протоколу, MTP включає механізми обмеження черг вихідних повідомлень, що дозволяє контролювати загальні затримки сигналізації (вимога 5). Зокрема, монітор помилок MTP2 оперативно виявляє несправні лінії, та виводить з експлуатації, якщо рівень помилок перевищує 4×10^3 . У разі виникнення перевантаження каналів, система керування трафіком MTP інформує джерела про необхідність зменшення навантаження. Якщо перевантаження стає хронічним (наприклад, через численні відмови ліній), може бути активовано умовне перенаправлення для оптимізації трафіку. [8]

1.3 SS7 в GSM

1.3.1 Сигналізація в 2G та 3G мережах

У мобільних мережах 3G сигналізація SS7 використовується між основними елементами мережі. До них відносяться контролер базової станції (BSC), реєстр домашнього розташування (HLR), мобільний комутаційний центр (MSC), а також між MSC та іншими мобільними мережами і телефонною мережею загального користування (PSTN) через шлюзовий мобільний комутаційний центр (GMSC).

Інші протоколи сигналізації, що використовуються в мережах 3G, окрім SS7, включають протокол доступу до каналу ISDN «D» (LAP-D), який використовується між BSC і базовою приймально-передавальною станцією (BTS) [9]. Структура повідомлень LAP-D схожа на SS7, але він не здатен працювати в режимі мережі, тому використовується тільки для з'єднань «точка-точка». Інший протокол, який також використовується в мережах 3G, -

LAP-D modified - використовується для передачі сигналів між мобільною станцією та BTS.

Оригінальні рівні протоколу SS7, описані в підрозділі 1.2.2 на сторінці 22, здебільшого стосуються PSTN. У стільникових мережах 2G і 3G сигналізація є складнішою. На відміну від PSTN, мобільні мережі 2G і 3G мають додаткові вимоги до сигналізації через відмінності в мережевій архітектурі, що потребує великої кількості сигналізації, не пов'язаної з викликами.

Абонент у PSTN є статичним, на відміну від мобільного абонента в мережах 2G і 3G. Мобільність абонента вимагає безперервного відстеження мобільної станції, що створює необхідність процедури оновлення місцезнаходження. Відстеження мобільної станції мережею для оновлення її поточного місцезнаходження є прикладом сигналізації, не пов'язаної з викликом, оскільки сигналізація відбувається за відсутності виклику. Управління цією вимогою вимагає додаткових наборів стандартних сигнальних повідомлень. У системах 2G і 3G додатковими рівнями протоколу сигнальних повідомлень є

Прикладна частина транзакційних можливостей (TCAP)

Прикладна частина транзакційних можливостей (TCAP) підтримує обмін даними, не пов'язаними з каналами зв'язку, між застосунками в мережі SS7, використовуючи послугу SCCP без підключення. Це полегшує підключення до зовнішньої бази даних. Запити і відповіді, що надсилаються між SSP і SCP, передаються в TCAP-повідомленнях. Деякі додатки, які використовують TCAP, включають Операційну, технічну та адміністративну частину (OMAP), яка використовує сервіси для зв'язку та функцій управління через мережу через віддалений термінал. Також у мобільних мережах GSM мобільна прикладна частина (MAP) використовує TCAP для обміну інформацією про абонентів стільникового зв'язку між різними мережами для підтримки автентифікації користувачів, ідентифікації обладнання та роумінгу [9].

Мобільна прикладна частина (MAP)

MAP - це протокол прикладного рівня SS7, який використовується в мережах GSM для доступу до реєстру домашнього місцезнаходження, реєстру місцезнаходження відвідувачів, центру мобільної комутації, реєстру ідентифікації обладнання, центру автентифікації, центру служби коротких повідомлень і вузла підтримки GPRS для надання таких послуг, як роумінг, обмін текстовими повідомленнями (SMS) та автентифікація абонента. MAP транспортується та інкапсулюється за допомогою протоколів SS7 MTP, SCCP та TCAP.

Прикладна частина підсистеми базової станції (BSSAP)

BSSAP використовується для сигнального зв'язку між MSC та BSC, а також між MSC і мобільною станцією. Він передає запити на управління викликом для початкового встановлення з'єднання та зміни атрибутів з'єднання між BSC та MSC. Він також обробляє завершення зв'язку між зв'язаними MSC та BSC.

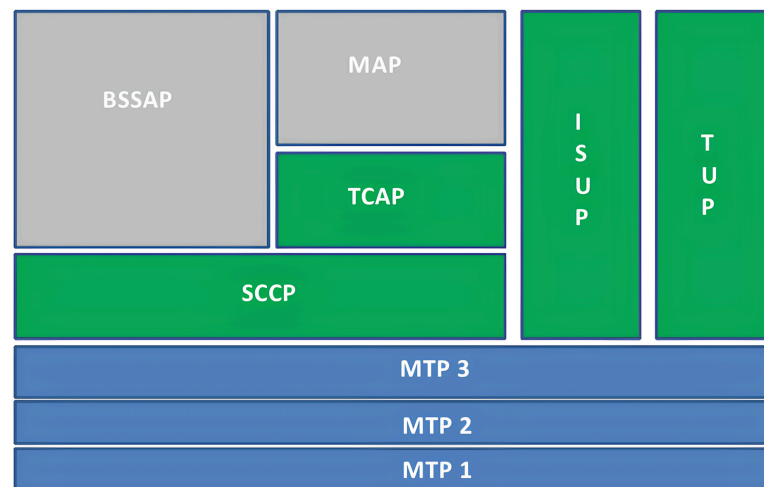


Рисунок 1.12 – Стек протоколів мережі GSM [9]

1.3.2 Протокольні рівні в елементах мережі 3G

Вимоги SS7 до окремих елементів мережі 3G відрізняються. Не всі елементи мережі мають всі протоколи в стеку SS7.

Мобільний комутаційний центр (MSC)

MSC є елементом мережі 3G, який відповідає за управління викликами, тому для виконання цієї функції необхідні протоколи TUP та ISUP. Також MSC разом з VLR відповідає за оновлення місцезнаходження і зв'язок з BSC і HLR. Для виконання цих завдань необхідні BSSAP і MAP. BSSAP знаходиться на вершині SCCP, а TCAP забезпечує обслуговування MAP.

МТР є фундаментом, на якому побудований SS7, і тому він повинен бути в кожному елементі мережі, включаючи MSC, який здатний обробляти сигнали SS7. Таким чином, MSC має весь стек протоколів SS7.

Контролер базової станції (BSC)

При використанні сигнальних повідомлень SS7, BSC взаємодіє з MSC тільки для управління всіма діями виклику, такими як встановлення з'єднання і хендовери, і тому для виконання таких функцій йому потрібен протокол BSSAP. BSSAP знаходиться поверх SCCP, який, в свою чергу, базується на рівнях МТР.

Home Location Register (HLR)

На відміну від MSC, який вимагає TUP/ISUP для управління викликами на мобільній станції та BSC, HLR має справу лише із запитом до бази даних щодо статусу користувачів мережі з метою автентифікації. Для цього він використовує протокол MAP. MAP базується на TCAP, який обслуговується SCCP, що лежить на рівнях МТР.

На рисунку нижче (Рисунок 1.13) показано стеки протоколів SS7 у різних елементах мережі та зв'язок сигнального зв'язку між цими елементами мережі.

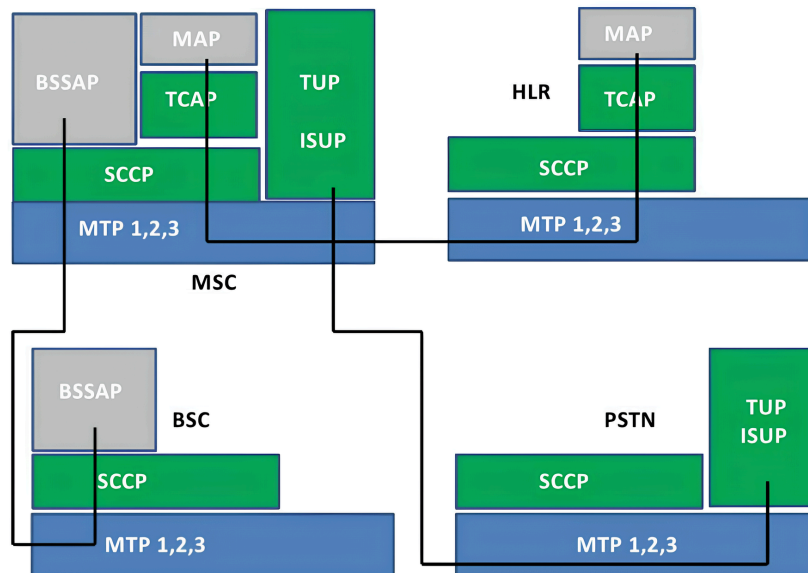


Рисунок 1.13 – Протоколи SS7 у різних елементах мережі [9]

1.3.3 Адресація, міжнародна маршрутизація

Повідомлення між застосунками у мережі SS7 обмежені розміром від 200 до 250 байт, залежно від розміру заголовків повідомлень. Деякі останні версії SS7 можуть підтримувати більші повідомлення завдяки сегментації повідомлень на будь-якому з'єднанні, але це нелегко реалізувати. Навіть якщо відомо, що пункт призначення підтримує цю можливість, сегменти можуть бути втрачені, якщо на шляху вони зустрінуться з STP, який її не підтримує. І, враховуючи кількість варіантів маршрутизації в SS7, визначити список потенційних проміжних STP дуже складно.

Фундаментальною адресою в SS7 є система точкових кодів, за якою точці сигналізації присвоюється унікальний номер. Точкові коди присвоюються кожною мережею окремо і значно відрізняються за розміром, від 14 біт до 24 біт. Звідси, маршрутизація за кодами пунктів може використовуватися лише в межах однієї національної мережі, і це обмеження ускладнює сигналізацію для всіх інших країн.

Другий тип адреси в SS7 відомий як «глобальний заголовок». Глобальний заголовок може бути перекладений або на проміжний пункт, або на пункт призначення. У випадку міжнародної сигналізації глобальний заголовок спочатку переводиться в код точки міжнародного шлюзу, який виконує трансляцію протоколу, а потім переводить глобальний заголовок в код точки в національній мережі призначення, або використовує маршрутизацію глобального заголовка для пересилання повідомлення до STP, який виконує цю функцію.

Хоча міжнародна маршрутизація з використанням SS7 здійснюється з використанням глобальних назв, це не означає, що глобальні назви повністю сумісні між країнами. Кодування глобальних назв є національним питанням, і це робить міжнародні шлюзи спеціалізованими і складними пристроями.

Основною проблемою глобальних назв є управлінський тягар, який вони накладають на STP. Кожен STP повинен мати набір таблиць маршрутизації для кожного типу глобальних назв, вони повинні бути налаштовані відповідно до положення STP в мережі і повинні часто оновлюватися. Помилки в таблицях глобальних заголовків можуть призвести до втрати повідомлень або навіть до відмови мережі. [5]

1.4 SIGTRAN

Використання протоколів Signaling Transport (SIGTRAN) - це перший крок до об'єднання мереж SS7 з IP-мережами. Сучасні телекомунікаційні компанії рухаються до повністю IP-мереж, але такий перехід не відбувається за одну ніч. За прогнозами Ericsson до кінця 2030 року в залежності від регіону від 32% до 3% мобільних станцій матимуть максимально доступну технологію 3G, і лише у Північній Америці та Східній Європі очікується що всі мобільні станції

матимуть підтримку 4G або 5G. [10] Головне завдання зараз - дати можливість цим системам співіснувати і покращити послуги, які вони надають.

У технології SIGTRAN, також відомий як SS7 через Інтернет-протокол (SS7oIP), різні вузли традиційної мережі SS7 на основі TDM сигналізуються повідомленнями протоколу SS7, які передаються через Інтернет-протокол з метою транспортування між віддаленими точками комутації сигналу (SSP) або між SSP і програмним комутатором для трафіку, пов'язаного з передачею голосу через IP (VoIP).

1.4.1 Транспортування SS7 через IP

Маршрутизація телефонних дзвінків на великі відстані через IP-мережу є більш економічно вигідною, ніж аналогічна маршрутизація за допомогою більш традиційних методів – комутації каналів на основі TMD.

З'являлося багато гнучких стандартів для IP-протоколу, однак серед нового покоління жоден не забезпечував усі можливості сигналізації SS7. Альтернатив системі сигналізації не знайшлося, тому виникла потреба в інтеграції SS7 в архітектуру програмного комутування. Для роботи над цим питанням була створена робоча група IETF, яка і розробила SIGTRAN.

Ці стандарти дозволяють мережам нового покоління на базі IP взаємодіяти з існуючими мережами SS7 і обмінюватися інформацією без втрати функціональних можливостей. SIGTRAN розкладає стек SS7 і дозволяє різним рівням спілкуватися за допомогою транспортного рівня IP. Замість використання MTP як транспортного протоколу, SIGTRAN передає інформацію окремо кожному рівню інфраструктури IP.

Для доставки повідомлень через IP в Інтернеті було визначено два транспортні протоколи: TCP та UDP, але вони ставлять певні обмеження для сигналізації в реальному часі, що роблять їх непридатними для цього завдання.

Протокол UDP був спеціально розроблений для забезпечення режиму передачі пакетів у комп'ютерних мережах, що з'єднані між собою. Цей протокол передбачає, що протокол IP використовується як базовий протокол. Він забезпечує передачу повідомлень від одних програм до інших. Протокол орієнтований на транзакції, і доставка та захист від дублювання не гарантуються. UDP є протоколом без підключення і не використовує повідомлення підтвердження (ACK) для забезпечення надійної та упорядкованої передачі. UDP є найбільш корисним у ситуаціях, коли потрібні високі швидкості передачі, але він не відповідає іншим умовам продуктивності сигнальних повідомлень SS7 [11].

TCP – це байто-орієнтований транспортний протокол, що забезпечує потік байтів і гарантує їхню впорядковану доставку. Це є критично важливим, зокрема, при передачі великих обсягів даних, як-от в електронній пошті або при передачі файлів. Проте, саме сувора послідовність доставки робить його непридатним для сигнальних повідомлень.

TCP дуже чутливий до затримок, що виникають внаслідок втрати пакетів, і це призводить до повторних передач. Під час очікування підтвердження втраченого пакету, решта пакетів затримується, через блокування черги (head-of-line blocking). Це зазвичай призводить до непотрібних затримок інших пакетів, тому TCP не підходить для застосунків реального часу, таких як Voice over IP (VoIP).

При встановленні TCP-з'єднання Хост 1 надсилає повідомлення SYN до Хоста 2, на яке той відповідає SYN-ACK. Потім Хост 2 чекає відповідного ACK від Хоста 1, що є останнім кроком у тристоронньому рукошляванні при встановленні TCP-з'єднання.

Однак ця процедура може бути вразливою до атак типу відмова в обслуговуванні (DoS), відомих як SYN-атаки. Вони реалізуються надсиланням SYN-повідомлень до Хоста 2. Ці повідомлення використовують ресурси пам'яті, що згодом може призвести до збою Хоста 2, і легітимні користувачі не зможуть отримати доступ до сервісу. Такий сценарій є неприпустимим у мережі SS7, де телефонні послуги мати надзвичайно високу доступність [12].

Основними характеристиками транспортного рівня мережевої сигналізації є: впорядкована та надійна передача повідомлень, резервування на випадок відмови каналу, низький рівень втрат і затримок, а також безпека від атак типу "відмова в обслуговуванні" (DoS).

Протоколи UDP і TCP не можуть задовольнити всі ці вимоги. Саме тому SIGTRAN (Signaling Transport working group) розробив новий транспортний протокол — Stream Control Transmission Protocol (SCTP). SCTP вдосконалює попередні TCP та UDP, забезпечуючи надійну передачу інформації таким чином, що відповідає вимогам систем SS7.

1.4.2 Стек протоколів SIGTRAN

Як згадувалося в попередньому підрозділі 1.4.1 на сторінці 34, сигнальні повідомлення SS7 мають дуже суворі вимоги щодо втрат і затримок. TCP не відповідає цим вимогам і не є придатним вибором, оскільки затримки є надто великими, а UDP не забезпечує достатньої надійності. Тому для подолання недоліків у надійності та продуктивності між двома традиційними методами IP-транспортування був розроблений набір протоколів SIGTRAN.

Набір протоколів SIGTRAN включає транспортний протокол SCTP, а також кілька протоколів рівня адаптації користувача (UA), які необхідні для транспортування повідомлень SS7 через IP (див. Рисунок 1.14).

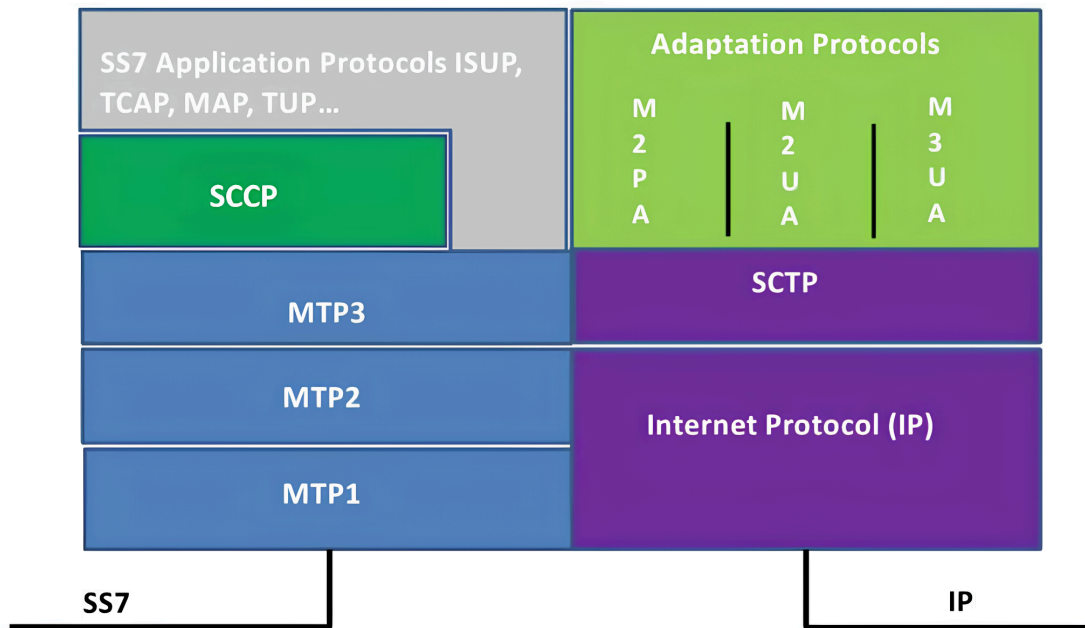


Рисунок 1.14 – Стек протоколів SIGTRAN [5]

Архітектура SIGTRAN складається з двох основних рівнів:

- **Передача загальної сигналізації (Common signaling transport):** Цей рівень забезпечує безпомилкову та впорядковану доставку повідомлень прикладного рівня. Він включає базовий IP-мережевий рівень та протокол SCTP.
- **Рівні адаптації користувача (User Adaptation layers):** Ці рівні підтримують специфічні примітиви, необхідні для конкретних сигнальних застосунків. До них належать, наприклад, M2PA, M2UA, M3UA та SUA.

Протокол передачі з керуванням потоком (SCTP) був розроблений насамперед для транспортування телефонних повідомлень SS7 через IP-мережі з метою відтворення функцій надійності та продуктивності SS7. SCTP є протоколом передачі дейтаграм на рівні застосунків, який працює поверх ненадійних рішень для дейтаграм, таких як UDP або TCP.

Протокол SCTP еквівалентний TCP, оскільки він пропонує як механізми керування потоком, так і керування перевантаженням. Однак він має дві основні функції, які підвищують його надійність та продуктивність, роблячи його більш

придатним для транспортування сигналізації SS7. Цими функціями є багатовузловість (multi-homing) та багатопоточність (multistreaming) [5].

Багатовузловість (Multi-Homing)

Як і стандартна сигналізація SS7, функція багатовузловості забезпечує надмірність в IP-передачі сигнальних повідомлень за допомогою SIGTRAN. Функція багатовузловості SCTP дозволяє кожному мережевому вузлу мати кілька IP-адрес, де кожна пара IP-адрес між двома вузлами називається шляхом.

Кожен шлях між двома фізично з'єднаними мережевими вузлами пов'язаний з повідомленнями "серцебиття" (heartbeat messages), які вказують на активний або неактивний режим. Кожен вузол вибирає основний шлях, і якщо на цьому шляху виникає збій, дані повторно надсилаються через альтернативний шлях (якщо доступний). Після певної кількості повторних передач основний шлях вважається неактивним, і вибирається новий шлях. Якщо він активний, то він стає новим основним шляхом.[13]

Функція багатовузловості дозволяє мережі перенаправляти дані на інші IP-адреси, що робить її більш стійкою до відмов фізичних каналів. У класичній мережі SS7 завжди існує щонайменше два фізично різні шляхи для передачі даних. Оскільки SIGTRAN має забезпечувати IP-рішення з усіма якостями мережі SS7, функція багатовузловості може бути використана для забезпечення такого ж рівня надмірності, як і в сигнальних мережах SS7.

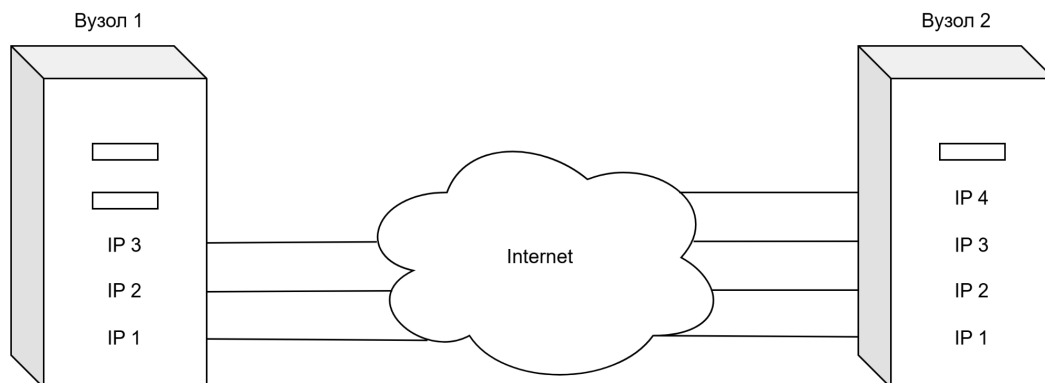


Рисунок 1.15 – Багатовузловість SCTP [13]

Багатопотоковість (Multi-Streaming)

Функція багатопотоковість протоколу SCTP допомагає зменшити затримки при встановленні з'єднань, а також зменшує перевантаження мережі при використанні транспортного стеку протоколів SIGTRAN для транспортування сигнальних повідомлень SS7. Багатопотоковість SCTP — це відправлення пакетів даних у кількох, одночасних та незалежних потоках, так що у випадку втрати даних в одному потоці, доставка не буде порушена для інших потоків. Ці потоки можливі без відкриття окремих шляхів між двома вузлами. Багатопоточність використовується для уникнення блокування черги (head-of-line blocking), що є поширеним явищем у звичайному TCP (див. Рисунок 1.16).

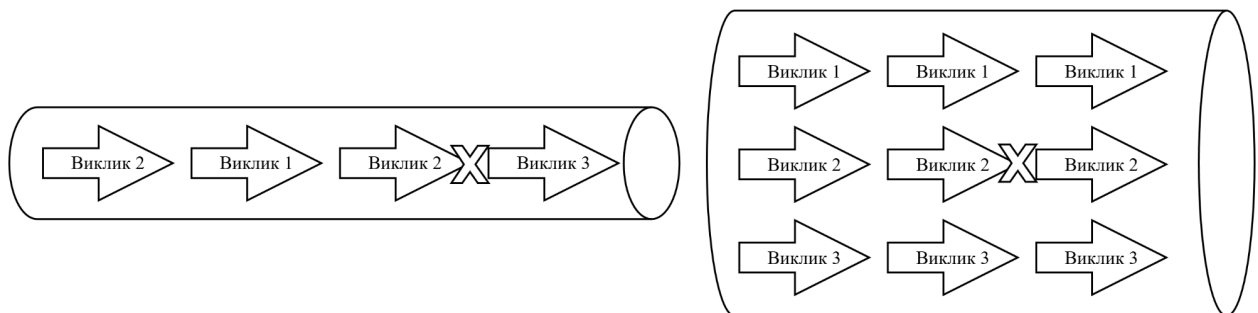


Рисунок 1.16 – Багатопотоковість SCTP [13]

При звичайній поточковій передачі даних TCP, коли сигнальний пакет для виклику втрачається, все з'єднання блокується, очікуючи на повторну передачу, що призводить до блокування голови черги. Затримка на відновлення втрачених даних може становити кілька мілісекунд або навіть секунд. Така затримка сигналізації є неприйнятною при здійсненні телефонного дзвінка за допомогою сигналізації SS7. У поточковій передачі SCTP (Рисунок 1.15) асоціація між двома вузлами може мати кілька потоків, кожен з яких призначений для певного ресурсу або застосунку. Втрата повідомлення, що стосується виклику 2, впливає лише на цей потік даних. Виклики 1 і 3 обслуговуються у звичайному режимі.

Створення кількох потоків за допомогою TCP також можливе, але вимагає відкриття кількох TCP-з'єднань, де кожне діє як потік. Кожне з'єднання вводить

Блок керування транспортуванням (TCB) на стороні сервера, який містить всю важливу інформацію про з'єднання. Ці TCB споживають пам'ять, і їх може бути забагато для функціонування зайнятої сигнальної точки з різними клієнтами, тому множинні TCP-з'єднання не підходять. Також використання лише однієї асоціації SCTP з потоками замість кількох TCP-з'єднань допомагає скоротити час встановлення виклику. [5]

Таким чином, SIGTRAN є кращим протоколом для транспортування повідомлень SS7 через IP завдяки функціям багатоузловості (multi-homing), багатопотоковості (multi-streaming) та багатьом іншим вдосконаленням транспортного рівня SCTP.

Таблиця 1.1 – Основні відмінності між функціями трьох протоколів IP-транспортування: TCP, UDP та SCTP. (✓ = так, ✗ = ні, Н/З = не застосовується)

Функція/Послуга	SCTP	TCP	UDP
Дозволяє напівзакриті з'єднання	✗	✓	Н/З
Пакетування PDU застосунку	✓	✓	✗
Фрагментація PDU застосунку	✓	✓	✗
Контроль перевантаження	✓	✓	✗
Підтримка ECN (Explicit Congestion Notification)	✓	✓	✗
Контроль потоку	✓	✓	✗
Повнодуплексний	✓	✓	✗
Багатовузловість (Multi-homing)	✓	✗	✗
Багатопотоковість (Multi-streaming)	✓	✗	✗
Впорядкована доставка даних	✓	✓	✗
Виявлення MTU шляху	✓	✓	✗
Збереження меж повідомлень	✓	✗	✓
Захист від SYN-флуд-атак	✓	✗	Н/З
Перевірка доступності	✓	✓	✗
Надійна передача даних	✓	✓	✗
Невпорядкована доставка даних	✓	✗	✓

Протоколи Рівня Адаптації Користувача (User Adaptation Layer) у SIGTRAN

Протоколи рівня адаптації користувача підтримують специфічні примітиви, необхідні для конкретного сигнального застосунку. Основними протоколами рівня адаптації користувача, які широко використовуються в SIGTRAN, є протокол MTP2 Peer-to-Peer Adaptation Layer (M2PA), протокол MTP2 User Adaptation Layer (M2UA) та протокол MTP3 User Adaptation Layer (M3UA). Рівні адаптації користувача названі відповідно до послуги, яку вони замінюють, а не за користувачем цієї послуги. Наприклад, M2UA адаптує SCTP для надання послуг MTP2, а не для надання послуги MTP2. [5]

Протокол Адаптаційного Рівня MTP2 Peer-to-Peer (M2PA)

Протокол M2PA забезпечує режим роботи peer-to-peer для передачі сигнальних повідомлень SS7 через IP-мережу. Він замінює канал MTP2 під MTP3. Користувачем M2PA є MTP3 на обох кінцях з'єднання. M2PA надає можливість для однорангових рівнів MTP3 в SG (Signaling Gateways) спілкуватися безпосередньо. Цей протокол використовується для з'єднань "SG до SG" і найкраще підходить для об'єднання двох островців мережі SS7.

M2PA головним чином відповідає за [5]:

- Активацію/деактивацію каналу у відповідь на запити від MTP3.
- Підтримку інформації про стан каналу.
- Підтримку порядкових номерів та буферів повторної передачі для отримання MTP3.
- Підтримку стану відмови локального та віддаленого процесора.

Протокол Адаптаційного Рівня Користувача MTP2 (M2UA)

M2UA — це протокол для передачі повідомлень SS7 MTP3 через IP-мережу, що використовується між шлюзом сигналізації (SG) та контролером медіашлюзу (MGC) у VoIP-мережах. M2UA надає інтерфейс між MTP3 та SCTP, що дозволяє застосункам MTP3 прозоро працювати поверх базової транспортної послуги SCTP та IP замість MTP2. Цей інтерфейс забезпечує прозору зв'язність між традиційними комутованими за каналом сигнальними

точками SS7 та елементами сигналізації нового покоління з підтримкою IP, такими як Softswitch або контролер медіашлюзу. [5]

Протокол Адаптації Користувача MTP3 (M3UA)

Протокол MTP3 User Adaptation (M3UA) був розроблений IETF для транспортування будь-якої сигналізації користувача SS7 MTP3 (наприклад, ISUP, SCCP та MAP) через IP, використовуючи протокол SCTP. M3UA також може працювати в різних архітектурах: SG-to-peer, peer-to-peer. [5]

M3UA надає послугу MTP3 між SG та сервером застосунків, підтримує користувачів MTP3: ISUP та SCCP. M3UA замінює сигнальний канал SS7, набір сигнальних каналів, комбінований набір каналів та сигнальні маршрути. M3UA розроблений для того, щоб дозволити застарілим вузлам SS7 TDM спілкуватися з вузлами SIGTRAN з підтримкою IP. [5]

1.5 Інтегрована Мережева Архітектура SIGTRAN

M2UA — це протокол для передачі повідомлень SS7 MTP3 через IP-мережу, що використовується між шлюзом сигналізації (SG) та контролером медіашлюзу (MGC) у VoIP-мережах. M2UA надає інтерфейс між MTP3 та SCTP, що дозволяє застосункам MTP3 прозоро працювати поверх базової транспортної послуги SCTP та IP замість MTP2. Цей інтерфейс забезпечує прозору зв'язність між традиційними комутованими за каналом сигнальними точками SS7 та елементами сигналізації нового покоління з підтримкою IP, такими як Softswitch або контролер медіашлюзу. [5]

З розвитком мобільних комунікацій кінцевим користувачам мобільних пристроїв пропонуються широкосмугові мультимедійні можливості. Пов'язані мультимедійні потоки вимагають, щоб мережі були більш гнучкими у наданні пропускної здатності за запитом, ніж сучасні мережі, які базуються на TDM. Таким чином, технологія транспортування, повинна розвиватися у сторону стільникових та пакетних технологій.

SS7 хоч і вважається застарілою системою, мережеві компоненти на базі сигналізації, які включають MSC, SSP, STP, та SGs, продовжують займати левову частку телекомунікаційного ринку. Темпи зростання абонентів на ринках, стабільний ріст SMS-повідомлень, послуги, розширені VoIP, та взаємодію між застарілими мережами TDM на базі SS7 та мережами нового покоління стимулювали ріст сигналізації SS7 за межі простого "контролю викликів" до надання розширених послуг для TDM та IP-доменів.

Рушійною силою взаємодії між мережами SS7 на базі TDM та новими IP-мережами IP Multimedia Subsystem (IMS) з використанням технології перетворення протоколів SIGTRAN є Шлюзи сигналізації (SGs). Вони транспортують сигналізацію додатків між мережею SS7 та IP-мережею, слугуючи з'єднанням застарілих мереж на базі TDM з пакетними мережами нового покоління. SGs реалізують стек протоколів SS7 та пов'язані з SS7-over-IP підкомпоненти SIGTRAN. У поєднанні з програмними комутаторами (softswitches), медіа-шлюзами, серверами додатків та медіа-серверами, SGs забезпечують функціональність контролю викликів та можливості обробки послуг традиційних комутаторів PSTN. [5]

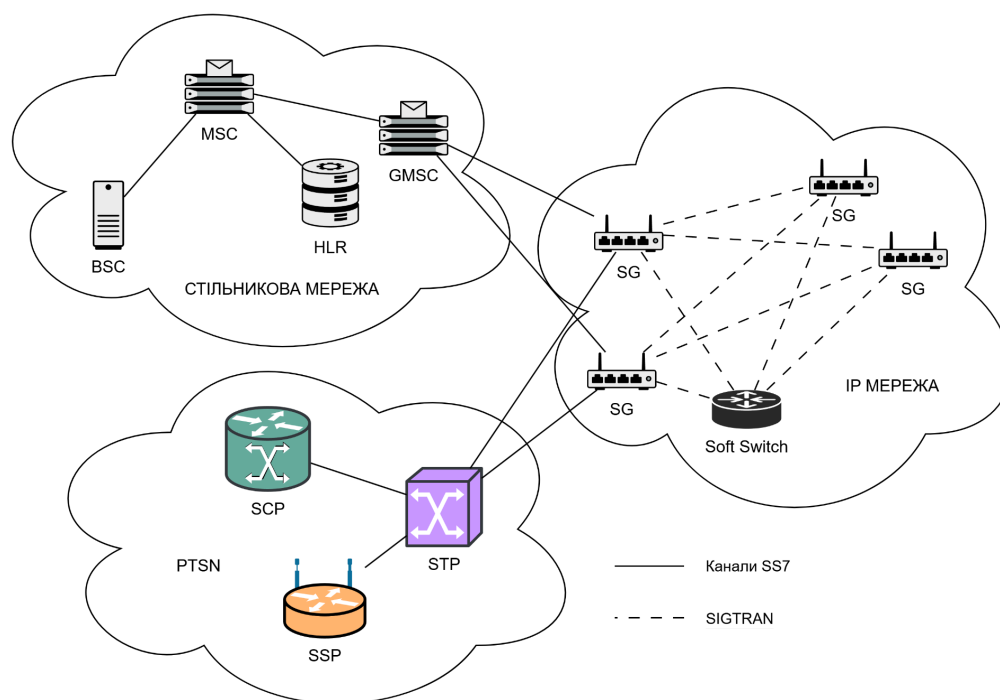


Рисунок 1.17 – Міжмережеві зв'язки сигналізації через SGs

1.5.1 Симуляція SIGTRAN

Існує багато комерційних реалізацій стеку SIGTRAN. Багато великих гравців беруть участь у сервісі Plugtest Європейського інституту стандартів телекомунікацій (ETSI). Сервіс Plugtest ETSI — це професійний підрозділ Європейського інституту стандартів телекомунікацій (ETSI), який спеціалізується на організації заходів з тестування взаємодії для компаній, організацій та органів стандартизації (ETSI, IETF, ITU тощо) [15]. Ці тести проводяться у сферах телекомунікацій, Інтернету, мовлення та мультимедіа. Деякі з основних гравців включають, зокрема: Adax, Cisco Systems, Ericsson, Hewlett-Packard, Siemens, Intellinet, Performance Technologies та Ulticom.

Наступні підрозділи коротко пояснюють деякі з популярних реалізацій SIGTRAN:

Реалізація Siemens/Університету Ессена

Ця реалізація [16] була розроблена Siemens, Університетом Ессена та Університетом прикладних наук, Німеччина. Це лише реалізація SCTP. Вона працює на Linux 2.4 та 2.6, FreeBSD 4.8, Solaris 8, Mac OS 10 та Windows (з деякими обмеженнями). Крім того, вона підтримує як IPv4, так і IPv6 та включає інструмент тестування SCTP. За допомогою інструменту тестування можна перевірити правильність встановлення та спробувати тестові сценарії.

Реалізація Berkeley Software Distribution (BSD) з проектом KAME

Проект KAME [17] — це спільні зусилля шести японських компаній зі створення єдиного надійного набору програмного забезпечення, що особливо орієнтований на IPv6/IPsec. Він працює на FreeBSD 4.0, OpenBSD 2.7, NetBSD 1.5, BSD/OS 4.2 та новіших версіях цих систем. Проект мав на меті надання безкоштовних еталонних реалізацій стеку IPv6 та IPsec (як для IPv4, так і для IPv6) для варіантів BSD та забезпечує розширені мережеві можливості, такі як розширене чергування пакетів, мобільність тощо.

Реалізація SCTP для ядра Linux (LKSCTP)

Проект LKSCTP [18] був започаткований одним з винахідників SCTP – Рендаллом Стюартом – у співпраці з Motorola. Ця реалізація підтримує SCTP, а також надає інструменти тестування з численними тестовими випадками. Вона може працювати як на IPv4, так і на IPv6. Для встановлення пакета необхідна версія ядра Linux 2.5.36 або пізніша, і вона повинна бути налаштована з увімкненою підтримкою мережесхемних опцій "SCTP Configuration".

Реалізація Open SS7

Проект OpenSS7 [19] розпочався у 1996 році, але спочатку був лише стеком SS7. Функції SIGTRAN були введені у 2001 році та включають протокол SCTP та протоколи адаптації користувача M2UA, M3UA та SUA. Також доступна реалізація TCP для порівнянь між двома транспортними протоколами (SCTP проти TCP). До стеку OpenSS7 SIGTRAN, також включені частини мобільного зв'язку, такі як реєстр домашнього розташування (HLR) з можливостями GPRS. OpenSS7 був розроблений для ядра Linux. Наразі він вимагає ядра 2.4.10+ та компілятора C (gcc), здатного компілювати ядро Linux.

Реалізація Dialogic SS7/SIGTRAN

Реалізація Dialogic SS7/SIGTRAN — це пропрієтарний комплект розробки SS7 від Dialogic Corporation, яка є всесвітнім постачальником телекомунікаційного обладнання, що обслуговує як ринки підприємств, так і постачальників послуг. Широкий асортимент продукції Dialogic включає медіа-шлюзи, медіа-сервери, шлюзи сигналізації та медіа-плати, і охоплює як традиційну технологію TDM, так і VoIP/SIP [20]. Наразі проект виключно комерційний і не передбачає ніякого безкоштовного доступу до продукту.

Реалізація SiGPloit

SiGploit — це фреймворк для тестування безпеки сигналізації, розроблений спеціально для фахівців та дослідників у галузі телеком-безпеки. Його мета — тестувати на проникнення та експлуатувати вразливості в сигнальних протоколах, що використовуються мобільними операторами, незалежно від покоління мережі. [21]

Висновки до розділу 1

Спираючись на результати досліджень, описаних у розділі 1 можна зробити кілька важливих висновків. Злиття сигналізаційних систем на базі SS7 з IP-сигналізацією, попри прогноз 2015 року, що це є "революцією" [5], виявилось довготривалим та складним процесом, який все ще триває. Ця інтеграція продовжує приносити значні переваги як операторам мобільних мереж, так і абонентам, особливо через постійний попит на послуги, орієнтовані на дані, такі як SMS та конвергентні комунікації. Оператори й надалі скорочують витрати на транспорт SS7, замінюючи дорогі виділені сигнальні лінії конкурентоспроможним IP-з'єднанням.

Хоча SS7 і вважається застарілою технологією, вона залишається невід'ємною частиною глобальної телекомунікаційної інфраструктури. Мережеві компоненти на базі SS7 (MSC, SSP, STP, HLR) досі займають значну частку ринку. Цей протокол глибоко вбудований у PSTN та мережі 2G/3G і продовжує використовуватися для забезпечення основних функцій, таких як встановлення голосових дзвінків (особливо через Circuit-Switched Fallback у 4G) та доставка SMS-повідомлень, а також для міжмережевої взаємодії та роумінгу. Світовий ринок SS7 у 2023 році оцінювався в 546,6 млн доларів США з прогнозованим зростанням до 610,4 млн доларів США до 2030 року, що свідчить про його збережену, хоч і повільну, актуальність.

Протокольний комплекс SIGTRAN продовжує відігравати критичну роль у забезпеченні сумісності та з'єднання між застарілими мережами SS7 та сучасними IP-орієнтованими мережами (включаючи 4G та неавтономні 5G-мережі). SCTP, як основний транспортний протокол SIGTRAN, досі є ключовим для забезпечення необхідної надійності та продуктивності, порівнянної з мережами SS7, завдяки своїм функціям багатовузловості (multi-homing) та багатопоточності (multi-streaming), які допомагають уникати блокування черги та забезпечують надмірність. Хоча робоча група SIGTRAN

завершила свою роботу в 2009 році, її специфікації є добре визначеними та широко впровадженими, і очікується подальший розвиток та вдосконалення протоколів SIGTRAN для задоволення потреб телекомунікаційних послуг наступного покоління.

Однак, як і прогнозувалося, безпекові виклики, що виникають через взаємодію традиційних SS7 та IP-мереж, стали значною проблемою. Дизайн SS7, що ґрунтується на довірі з 1980-х років, робить його вразливим у сучасній взаємопов'язаній мережі. Існують добре задокументовані вразливості, що дозволяють відстежувати місцезнаходження абонентів, перехоплювати голосові дані та SMS (включаючи обхід двофакторної аутентифікації) та здійснювати DoS-атаки. Ці вразливості є постійною загрозою, і їхнє усунення вимагає значних зусиль, включаючи впровадження спеціалізованих брандмауерів сигналізації (SS7 firewalls), які забезпечують конвергентний захист для SS7, Diameter та HTTP/2. Регуляторні органи, такі як FCC, активно вимагають посилення безпеки навколо SS7 та Diameter.

2 ВРАЗЛИВОСТІ SS7

2.1 Вразливості SS7 у гібридних мережах

Це дослідження спрямоване на те, чи може IP-мережа стати джерелом потенційних кіберзагроз для 3G TDM-орієнтованої мережі SS7 через їхню взаємодію. Крім того, буде стисло висвітлено мотиви цих кібератак та запропоновано способи їхнього запобігання.

Мережа SS7 спочатку була задумана як закрита система, що забезпечувало їй вищий рівень захисту від зовнішніх загроз. Однак, у міру того, як телекомунікаційні мережі почали інтегруватися у єдину глобальну систему, зумовлену взаємозв'язком різних технологій, а також потребою операторів використовувати економічно вигідніші можливості IP-з'єднання, кіберзагрози для колись закритої мережі SS7 значно посилюються. Тепер кібератаки, спрямовані на конкретний вузол мережі SS7, можуть бути легко ініційовані з підключеної до неї IP-мережі за допомогою транспортного протокового комплексу SIGTRAN.

Зловмисники можуть атакувати мережу SS7 через транспортний механізм SIGTRAN з багатьох причин, серед яких, але не обмежуючись: перехоплення номерів, викликів та компрометацію загальної конфіденційності спілкування абонентів. Хакери також здатні впроваджувати шкідливі пакети у національні та глобальні мережі SS7, щоб отримати контроль над процесами обробки викликів та звітністю, а також здобути конфіденційні дані, такі як номери кредитних карток чи неопублічні телефонні номери. Крім того, несанкціоновані особи можуть читати, змінювати, вставляти або видаляти сигнальні повідомлення SS7. Злом також може призвести до відмови в обслуговуванні для всіх користувачів мережі, порушуючи роботу як звичайних, так і екстрених викликів. Захоплення шлюзів через кібератаки може спричинити перенаправлення трафіку викликів [22].

Дерегуляція телекомунікаційної галузі у 1996 році та лібералізація економіки призвели до появи численних нових гравців, відомих як Конкурентні Місцеві Оператори Зв'язку (CLEC). Це спричинило збільшення кількості інтерфейсних точок доступу до SS7, тим самим створюючи нові потенційні вектори для атак [23]. Також, взаємоз'єднання опорних мереж SS7 з IP-мережами може породити нові загрози для сигнальних мереж SS7.

З огляду на взаємозв'язок між мережею SS7 та IP-мережею, це дослідження було спрямоване на:

- а) Визначення вразливостей мережі SS7, які можуть виникнути внаслідок її інтеграції з IP-мережею через використання SIGTRAN Media Gateway як конвертера протоколів.
- б) Запропонування факторів, що пом'якшують вплив виявлених вразливостей мереж SS7, які є наслідком взаємодії SS7/IP.

2.2 Симуляція SS7

Це дослідження проводилося з використанням експериментального підходу, деталі якого пояснені в наступних підрозділах цього звіту. Однак, цей розділ надає загальний огляд застосованого методу. У контексті вивчення вразливостей SS7 до кібератак, особливу увагу було приділено Технології Транспорту Сигналізації (SIGTRAN), також відомій як SS7oIP.

У системі SS7oIP сигнальні повідомлення протоколу SS7, призначені для різних вузлів Мобільної Бездротової Мережі, інкапсулюються в Інтернет-Протокол для транспортування. Це дозволяє передавати дані між віддаленими Точками Комутації Сигналізації (SSP) або між SSP та програмним комутатором (Softswitch) для трафіку VoIP. Загальна схема експериментальної мережі візуалізована на Рисунку 2.1.

Зауважте, що фокусом експерименту була Пакетна Мережа.

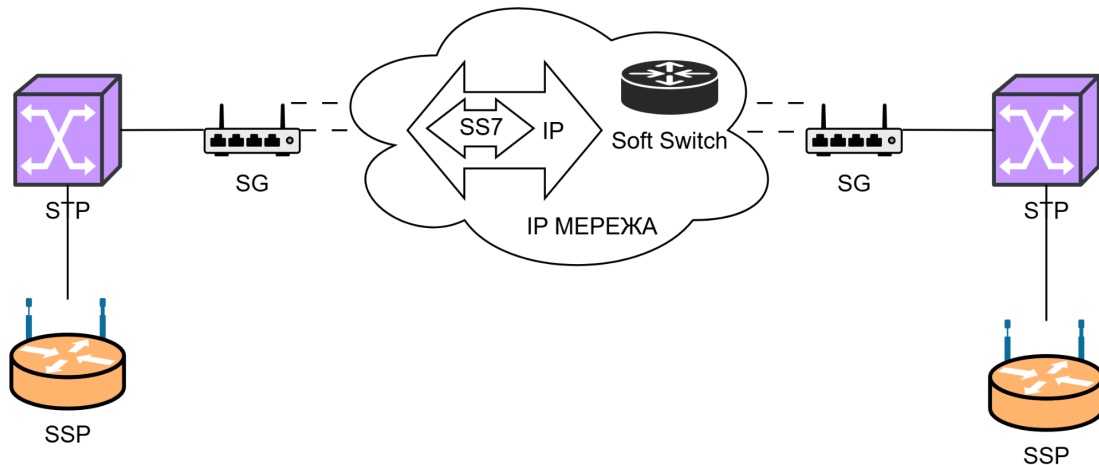


Рисунок 2.1 – Експериментальна мережа SS7 over IP (SIGTRAN)

Як показано на Рисунку 2.1, сигнальні повідомлення SS7 від віддалених SSP конвертуються у IP-трафік SIGTRAN на SG. У цьому конкретному випадку всі повідомлення SS7 розглядаються як корисне навантаження і розміщуються у октетах даних після перших двадцяти байтів IP-пакета. IP повторно збирає пакетні дейтаграми назад у сегменти на приймаючій стороні, і кожній дейтаграмі присвоюється IP-адреса вихідного та цільового вузла. Кожен маршрутизатор у IP-мережі (пристрій рівня 3), який отримує дейтаграму, приймає рішення щодо маршрутизації на основі цільової IP-адреси пакета. Отриманий пакетизований SS7-трафік потім транспортується через IP-мережу до свого призначення, будь то інший віддалений SSP або Softswitch.

Тепер зломисник, використовуючи будь-який комп'ютер з мережевим доступом, підключений у режимі логування (режим мережевого інтерфейсу, в якому мережева карта записує інформацію про кожен пакет, який вона бачить) до тієї ж IP-мережі, що транспортує пакетизовані повідомлення SS7, зможе "прослуховувати" мережу та захоплювати весь цікавий пакетизований SS7-трафік. Цей комп'ютер буде обладнаний програмним забезпеченням для аналізу IP-пакетів, таким як Wireshark, і зможе захоплювати будь-які пакети, що проходять через мережу, включаючи інформацію про IP-адреси джерела та призначення. Як тільки ця критична інформація буде розкрита, зломисник,

використовуючи програмне забезпечення для маніпуляції мережею та пакетами, зможе дестабілізувати або повністю розірвати мережеві з'єднання між цільовими IP-вузлами.

Під час розробки дослідницького проекту передбачалося, що буде отримано дозвіл на доступ до реальної мережі SIGTRAN для проведення необхідних тестів на вразливість безпеки. Згідно з початковим планом, тестування вимагало б простого підключення комп'ютера з IP інтерфейсом безпосередньо до мережі та моніторингу мережевої активності між різними мережевими вузлами. Однак, під час дослідження було виявлено, що отримати дозвіл до справжнього обладнання чесним шляхом є неможливим.

Враховуючи часові обмеження, було вирішено продовжити роботу з симуляцією мережі SIGTRAN, використовуючи один із вільно доступних інструментів реалізації SIGTRAN з Інтернету. Це альтернативний спосіб, який може досягти подібних результатів, як і тестування в реальному середовищі.

2.3 SiGPloit Реалізація Симуляції Мережі SS7/SIGTRAN

Експериментування та тестування, проведені в цьому дослідженні для встановлення вразливостей сигнальних повідомлень SS7 до кібератак, ґрунтувалися на використанні фреймворку SiGPloit.

SiGPloit – це спеціалізований фреймворк для тестування безпеки сигналізації, розроблений для фахівців та дослідників у галузі телеком-безпеки. Він є інструментом з відкритим вихідним кодом, доступним на GitHub [21], який дозволяє пентестувати та експлуатувати вразливості в сигнальних протоколах, що використовуються мобільними операторами. SiGPloit підтримує різні протоколи, включаючи SS7, GTP (3G), Diameter (4G) та SIP, що робить його універсальним інструментом для аналізу сучасних та застарілих телекомунікаційних інфраструктур. Його гнучкість дозволяє симулювати атаки та тестувати відповіді мережі в контрольованому середовищі.

SiGPloit, будучи інструментом з відкритим вихідним кодом, є дуже цінним для дослідників та фахівців з безпеки SS7/SIGTRAN. Він дозволяє тестувати різні сценарії атак, відтворювати відомі вразливості та оцінювати ефективність захисних механізмів. Його активна спільнота розробників та користувачів також сприяє обміну ідеями, кращими практиками та актуальною інформацією про нові загрози в телекомунікаційній сигналізації.

Для цілей розробки та тестування, SiGPloit надає функціонал, що дозволяє проводити симуляційні тести без необхідності отримання комерційних ліцензій, що є ідеальним для дослідницьких проектів.

2.3.1 Використані пристрої та програмне забезпечення

Для отримання кращого розуміння та аналізу кіберзагроз для сигнальних повідомлень SS7 під час їх транспортування через IP-мережу, критична оцінка базувалася на серії систематичних тестів безпеки IP-мережі з використанням фреймворку SiGPloit, який є відкритим та вільно доступним програмним забезпеченням.

Для проведення тестів було використано таке обладнання:

ПК під керуванням операційної системи DragonOS – дистрибутиву лінукс розробленого спеціально для роботи з Software Defined Radio (SDR) та безпроводними комунікаціями.

SiGPloit: Основний фреймворк для генерації та експлуатації SS7-атак. Віддалені вузли (набір змінюється в залежності від сценарію атаки), що обмінюються повідомленнями симульовано віртуально за допомогою даного програмного забезпечення.

Wireshark: Програмне забезпечення для аналізу мережевого трафіку (мережевий сніфер) для захоплення та детального аналізу SS7/SIGTRAN пакетів.

2.3.2 Використані пристрої та програмне забезпечення

На Рисунку 2.2 нижче показано мережеве з'єднання між різними компонентами мережі, використаними в дослідженні. Роль кожного компонента коротко пояснюється в наступних підрозділах.



Рисунок 2.2 – Експериментальна симульована мережа SIGTRAN

У залежності від типу розглядуваної атаки, вузли можуть служити різними елементами мережі SIGTRAN (HLR, SG). Програмне забезпечення SiGPloit розгортає необхідні рівні стеку, що описуються у розділі 1.3.2, та присвоює симульованому вузлу IP адресу. Вузол А використовується як вихідний шлюз сигналізації, Вузол Б – шлюз сигналізації призначення.

У ролі хакерського вузла, в залежності від експерименту, може виступати Вузол А. На хакерському вузлі було встановлено тестовий програмний пакет Wireshark. Як буде пояснено в наступних розділах, Wireshark – це безкоштовний аналізатор пакетів з відкритим вихідним кодом, який захоплює пакети в реальному часі та відображає їх у зручному для читання форматі.

Мережевий хаб – це фізичне з'єднання, яке об'єднує кілька комп'ютерів або інших мережевих пристроїв для формування єдиного сегмента мережі, де всі

підключені пристрої можуть спілкуватися один з одним. На відміну від мережевого комутатора чи маршрутизатора, хаб не має таблиць маршрутизації або інтелекту щодо того, куди надсилати інформацію, тому хаб просто транслює всі мережеві дані через кожне з'єднання. В цьому експерименті в ролі хаба виступав хост-комп'ютер з операційною системою DragonOS, на якому було розгорнуте програмне забезпечення SiGPloit.

Wireshark – це безкоштовний багатоплатформний інструмент для перехоплення та аналізу пакетів з відкритим вихідним кодом, який використовується для усунення несправностей у мережі, розробки програмного забезпечення та протоколів зв'язку, а також для навчання. Він дозволяє досліджувати дані з живої мережі або з файлу захоплення на диску [24].

Як сніфер пакетів, Wireshark сам по собі є пасивним, оскільки він лише спостерігає за повідомленнями, що надсилаються та отримуються додатками та протоколами, які працюють на мережевому комп'ютері, але ніколи сам не надсилає пакети. Аналогічно, отримані пакети ніколи не адресуються явно сніферу пакетів. Замість цього, сніфер пакетів отримує копію пакетів, які надсилаються/отримуються з/від додатків та протоколів, що виконуються на комп'ютері.

Іншою функцією Wireshark є можливість аналізу пакетів, яка відображає вміст усіх полів у повідомленні протоколу. Для цього Wireshark розуміє структуру всіх повідомлень, обмінюваних протоколами.

У цьому дослідженні Wireshark використовувався як програмне забезпечення для перехоплення мережевого трафіку з метою розкриття конфіденційної інформації.

2.4 SiGPloit Реалізація Симуляції Мережі SS7/SIGTRAN

Для досягнення мети цього дослідження, необхідно було точно оцінити вразливості мережі SIGTRAN до загроз, які зробили б колись закриту сигнальну мережу SS7 відкритою для атак.

Це дослідження ґрунтувалося на припущенні, що хакер вже отримав доступ до внутрішньої пакетно-комутованої мережі оператора. Такий доступ міг бути досягнутий різними способами, наприклад, за допомогою недоброчесних співробітників, а також через віддалені атаки, що використовують скомпрометовані елементи мережі, такі як IP-SS7 SG (шлюзи сигналізації).

Однак слід зазначити, що тести в цій симуляції проводилися в ідеальних та контрольованих лабораторних умовах. Як наслідок, отримані результати можуть дещо відрізнятися від тих, що можуть бути отримані в умовах реальної мережі.

Тести, які були проведені на симульованій системі SIGTRAN для встановлення вразливостей IP-мереж до кібератак, виконувалися у наступному порядку:

Nmap scan for sctp

Перелік мережі (Network Enumeration) – це активна загроза безпеці, під час якої зловмисник активно запитує мережу для збору інформації про її структуру, пристрої та відкриті служби. На відміну від пасивного перехоплення, перелік включає надсилання пакетів до мережі для отримання відповідей, тим самим розкриваючи критичні мережеві деталі. Ці загрози спрямовані на нижчі рівні мережевої інфраструктури.

У цьому тесті, використовуючи Wireshark та Nmap як програмне забезпечення для переліку, експеримент мав на меті розкрити життєво важливу мережеву інформацію, таку як IP-адреси віддалених мережевих інтерфейсів вузлів SIGTRAN та ідентифікацію відкритих портів. Будь-яке знання цієї

інформації може бути використано зловмисним зловмисником для атаки на безпеку мережевих елементів.

Цей експеримент допоможе довести, що безпека компонентів сигнальної мережі SIGTRAN компрометується через IP-мережу, отже, сигнальні повідомлення SS7 стають вразливими до кібератак.

IMSI Catch

Атака "IMSI Catch" є складною та активною загрозою безпеці, яка експлуатує сигнальну мережу SS7 для перехоплення Міжнародного Ідентифікатора Мобільного Абонента (IMSI) цільового абонента. Ця атака демонструє критичну вразливість у мережах SIGTRAN, дозволяючи зловмиснику видавати себе за легітимні мережеві елементи (наприклад, SMS-центр) для вилучення конфіденційної інформації про абонента. Така атака підкреслює, як раніше розкриті мережеві деталі можуть бути використані для глибших проникнень.

У цьому тесті експеримент мав на меті продемонструвати, як зловмисник, маскуючись під легітимний SMSC, може ініціювати запит sendIMSI до Реєстру Домашнього Розташування (HLR) цільового абонента через мережу SS7. Цей процес, що полегшується за допомогою Перетворення Глобальних Заголовків (GTT), дозволяє зловмиснику отримати IMSI абонента, який є унікальним ідентифікатором абонента в мобільній мережі. Тест використовував Wireshark для захоплення та аналізу мережевого трафіку, тим самим розкриваючи успішне перехоплення цієї конфіденційної інформації.

Результати цього експерименту надають переконливі докази того, що мережі SIGTRAN є вразливими до вдосконалених кібератак, які можуть скомпрометувати анонімність абонента та уможливити подальшу зловмисну діяльність, підтверджуючи твердження, що IP-мережі не є адекватно захищеними для транспортування чутливих сигнальних повідомлень SS7.

Any Time Interrogation

Атака "Any Time Interrogation" (ATI) є активною загрозою безпеці, яка експлуатує вразливості в сигнальній мережі SS7 для отримання несанкціонованого доступу до конфіденційної інформації абонентів. Ця атака використовує попередньо отримані дані мережевої розвідки (такі як IP-адреси та відкриті порти) для прямого запиту до Домашніх Реєстрів Місцезнаходження (HLR) або інших мережевих елементів з метою отримання конфіденційних даних про цільового абонента. Подібні атаки демонструють критичні недоліки безпеки IP-мереж під час транспортування сигнальних повідомлень SS7.

У цьому тесті, використовуючи SiGPloit як інструмент атаки та Wireshark для аналізу трафіку, експеримент мав на меті продемонструвати, як зломисник, ідентифікувавши цільовий HLR, може успішно отримати конфіденційну інформацію про абонента, включаючи його Міжнародний Ідентифікатор Мобільного Обладнання (IMEI) та дані про місцезнаходження. Це підкреслює серйозні ризики для конфіденційності та безпеки, пов'язані з розкриттям сигнальних повідомлень SS7 у IP-мережах.

Результати цього експерименту надають додаткові докази того, що IP-мережі не є достатньо безпечними для транспортування сигнальних повідомлень SS7, що робить їх вразливими до складних кібератак, які можуть скомпрометувати конфіденційність та приватність абонентів.

Provide Subscriber Info

Атака "Provide Subscriber Info" (PSI) є вдосконаленою активною загрозою безпеці, яка використовує раніше отриману мережеву інформацію для прямого запиту до обслуговуючого Центру Комутації Мобільної Зв'язку/Реєстру Відвідувачів (MSC/VLR) абонента з метою отримання точних деталей його місцезнаходження. Цей експеримент є продовженням попередніх атак переліку (enumeration) та "IMSI Catch", демонструючи, як зломисник може масштабувати доступ до критичних мережевих даних та використовувати їх для

цілеспрямованого спостереження. Така атака підкреслює притаманні вразливості мереж SIGTRAN.

Цей експеримент мав на меті продемонструвати, як зловмисник, видаючи себе за Реєстр Домашнього Розташування (HLR) та використовуючи раніше отримані адресу MSC/VLR та Міжнародний Ідентифікатор Мобільного Абонента (IMSI) цільового абонента, може успішно ініціювати запит MAP-Provide-Subscriber-Info (PSI) Request. Це дозволяє зловмиснику отримати конфіденційну інформацію про місцезнаходження, включаючи Ідентифікатор Комірки (Cell ID), Мобільний Код Країни (MCC), Мобільний Код Мережі (MNC) та Код Зони Місцезнаходження (LAC). Атака використовувала Wireshark для захоплення та аналізу мережевого трафіку, тим самим ілюструючи успішне вилучення цих чутливих даних.

Результати цього експерименту надають подальші конкретні докази того, що мережі SIGTRAN є вразливими до складних кібератак, що дозволяють несанкціоноване отримання конфіденційної інформації про місцезнаходження абонента. Це підкреслює критичну потребу в посилених заходах безпеки в IP-мережах, які передають сигнальні повідомлення SS7, для захисту конфіденційності абонентів.

Update Location

Атака "Update Location" (UL) є критичною загрозою типу "людина посередині" (MITM) у мережах SS7, що безпосередньо компрометує зв'язок та конфіденційність абонента. Ця атака демонструє, як зловмисник, видаючи себе за Центр Комутації Мобільної Зв'язку/Реєстр Відвідувачів (MSC/VLR), може перенаправляти вхідні дзвінки та SMS-повідомлення, призначені для цільового абонента. Передумова полягає в тому, що зловмисник використовує свій доступ до мережевого хаба для перехоплення та маніпулювання процедурами оновлення місцезнаходження в інфраструктурі сигналізації SS7.

У цьому тесті експеримент мав на меті продемонструвати здійсненність атаки "Update Location", в якій зловмисник, видаючи себе за легітимний

MSC/VLR, надсилає запит MAP-Update-Location Request безпосередньо до Реєстру Домашнього Розташування (HLR) цільового абонента. Після успішного завершення процедур оновлення місцезнаходження, симульований MSC/VLR зломисника приймає на себе роль обслуговуючого вузла абонента. Це дозволяє зломиснику перехоплювати вхідні SMS-повідомлення та дзвінки, призначені для абонента, які потім або відкидаються, або, як продемонстровано в цьому експерименті, потенційно перенаправляються до легітимного одержувача для збереження прихованості.

Результати цього експерименту, зафіксовані за допомогою Wireshark, ілюструють критичні кроки атаки: успішну імітацію MSC/VLR, ініціацію та підтвердження процедури Update Location, перенаправлення даних абонента, а також перехоплення та подальше пересилання SMS-повідомлення. Це беззаперечно доводить, що IP-мережі, які транспортують сигнальні повідомлення SS7, вразливі до складних MITM-атак, що призводить до порушення легітимного зв'язку та потенційної компрометації конфіденційної інформації.

SMS Spoofing

SMS Spoofing є критичною загрозою безпеці в мережах SS7, яка дозволяє зломиснику надсилати SMS-повідомлення з підробленим ідентифікатором відправника. Ця атака часто використовується для фішингових кампаній, дозволяючи зломисникам видавати себе за легітимні організації (наприклад, банки, платформи соціальних мереж) та обманом змушувати одержувачів розкривати конфіденційну інформацію. Вона підкреслює значну вразливість у сигнальній інфраструктурі SS7-IP, яку можна використовувати для шахрайських дій.

Цей експеримент мав на меті продемонструвати здійсненність атаки "SMS Spoofing". Зломисник створив та доставив SMS-повідомлення, де поле TP-Originating-Address було змінено для відображення оманливого відправника (наприклад, "Facebook"), тоді як текст SMS містив оманливе повідомлення

(наприклад, "Будь ласка, підтвердьте свій пароль на <http://facebuk.com>"). У тесті використовувався Wireshark для захоплення та аналізу мережевого трафіку, тим самим ілюструючи успішну доставку та зміст підробленого SMS.

Результати цього експерименту, зафіксовані за допомогою Wireshark, беззаперечно доводять, що мережі SS7 вразливі до SMS Spoofing. Ця вразливість дозволяє здійснювати зловмисні фішингові спроби, що безпосередньо впливає на безпеку абонентів та підкреслює нагальну потребу в надійних заходах безпеки в IP-мережах, які передають сигнальні повідомлення SS7.

Висновки до розділу 2

Цей розділ слугує фундаментальним введенням до проблематики кібератак на сигнальні повідомлення SS7, коли вони передаються через IP-мережі. Він підкреслює критичну потребу в цьому дослідженні, представляючи загальний опис проблеми, визначені цілі, обрану методологію та деталі конфігурації обладнання, задіяного в експерименті для її розв'язання.

Існуючі наукові роботи з цієї теми свідчать про значні зусилля, покладені у вивчення транспортної технології SIGTRAN. Проте більшість з них зосереджувалася переважно на продуктивності та надійності її базового транспортного протоколу SCTP. Відтак, цей розділ підтверджує нагальну потребу у посиленні дослідницької уваги та поглиблених розслідуваннях безпекового аспекту технології SIGTRAN, оскільки взаємодія між мережами SS7 та IP є життєво важливою в сучасних телекомунікаціях.

3 СИМУЛЯЦІЯ АТАК SS7

Експеримент – це тест або дослідження, що проводиться з метою перевірки, спростування або встановлення достовірності гіпотези. Експерименти, проведені в цьому дослідженні, мали на меті надати докази на користь чи проти того, що IP-мережі роблять сигнальні повідомлення SS7 відкритими та вразливими до кібератак. Ці експерименти виконувалися з використанням інструменту симуляції мережі SiGPloit. Тому цей розділ детально описує налаштування та конфігурацію системи для цієї симульованої мережі.

Експеримент симулював IP-мережу, що використовується для передачі трафіку між двома мережам SS7 за допомогою протоколів SIGTRAN. Таким чином, два однорангові SIGTRAN-сервери (вузли) були розгорнуті на кожному кінці мереж SS7/IP. Подібно до того, як точки сигналізації ідентифікуються кодами точок у мережах SS7, вузли SIGTRAN ідентифікуються IP-адресами.

IP-адреси, сигнальні протоколи та SMS-повідомлення, якими обмінювалися між двома SIGTRAN-вузлами, збиралися симульованим хакерським вузлом, підключеним до IP-мережі. Використовуючи цю інформацію, зловмисник зміг здійснити кібератаки на сигнальні повідомлення SS7.

3.1 Network enumeration

Це тестування було спрямовано на висвітлення недоліків безпеки IP-мереж під час транспортування сигнальних повідомлень SS7. Це відбувалося через розкриття певної приватної та конфіденційної мережевої інформації, яка мала бути відома лише вузькому колу провідних мережевих адміністраторів та менеджерів операторів мобільного зв'язку (MNO). За допомогою мережевого

"перерахування" (enumeration) експеримент мав на меті продемонструвати, що критично важлива мережева інформація може легко опинитися в публічному доступі за допомогою вільно доступних інструментів для мережевого "прослуховування" з інтернету, таких як Wireshark та Nmap [25].

Конфіденційною мережевою інформацією, яка була цільовою в цьому тесті, були IP-адреси та відкриті порти хост-вузлів.

Результати цього тесту матимуть велике значення для надання доказів щодо того, чи є IP-мережі достатньо безпечними для транспортування сигнальних повідомлень SS7, або ж IP-мережі роблять сигнальні повідомлення SS7 вразливими до кібератак, розкриваючи критично важливу інформацію про конфігурацію мережі вузлів SIGTRAN, яка може бути використана для здійснення подальших атак на мережі SS7.

Експериментальну мережу наведено на Рисунку 3.1.

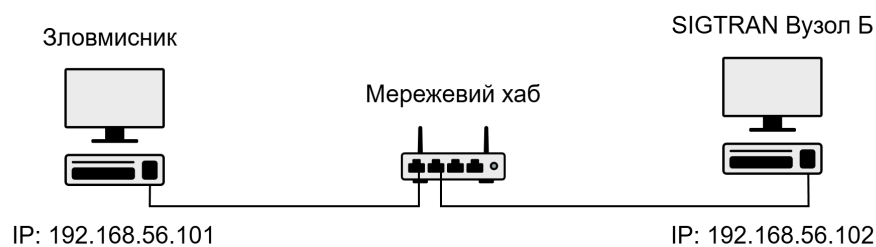


Рисунок 3.1 – Експериментальна мережа Network enumeration

Процедура тестування:

Два вузли SIGTRAN, позначені як Зловмисник та Вузол Б, були налаштовані зі статичними IP-адресами 192.168.56.101 та 192.168.56.102 відповідно.

Зловмисник представляв хакера, який отримав доступ до того ж пулу TCP/IP-мережі, що й Вузол Б, який транспортував сигнальні повідомлення SS7

через IP-мережу. Зловмисник був підключений у режимі прослуховування, що дозволяло йому бачити весь мережевий трафік.

Використовуючи програмне забезпечення Nmap Зловмисник надсилав SCTP INIT пакети на різні порти елементів мережі.

Використовуючи програмне забезпечення для перехоплення мережевого трафіку Wireshark, встановлене на своєму комп'ютері, зловмисник "прослуховував" мережу, щоб відстежувати активність між мережевими компонентами. Таким чином, він отримав критично важливу мережеву інформацію, включаючи IP-адресу та відкритий порт вузла мережі.

Було здійснено живе захоплення мережевої активності за допомогою Wireshark та проведено його аналіз.

3.1.1 Отримані результати

Результати цього експерименту, які були вилучені зі знімка екрана Wireshark (Додаток А), показані в Таблиці 3.1 нижче.

Таблиця 3.1 – Витягнуті результати тесту Network Enumeration Wireshark

No.	Time	Source	Destination	Protocol	Length	Info
3	0.0355742	192.168.56.101	192.168.56.102	SCTP	66	INIT
4	0.0356378	192.168.56.102	192.168.56.101	SCTP	298	INIT_ACK
5	0.0356624	192.168.56.101	192.168.56.102	SCTP	50	ABORT
6	0.0356713	192.168.56.101	192.168.56.102	SCTP	66	INIT
7	0.0356742	192.168.56.102	192.168.56.101	SCTP	50	ABORT

Результати, представлені в Таблиці 3.1, чітко відображають наступну інформацію:

- 1) Будь-який пакет даних, що надсилався між вихідним і цільовим вузлами, ідентифікувався за такими полями:
 - а) № – номер пакета, переданого з початку захоплення трафіку.

- b) Час – час "у секундах", коли пакет був відправлений з початку захоплення.
 - c) Джерело – IP-адреса вихідного вузла для пакета.
 - d) Призначення – IP-адреса цільового вузла для пакета.
 - e) Протокол – цифрове правило для обміну даними між двома пристроями.
 - f) Довжина – довжина кадру пакета в байтах.
 - g) Інформація – тип надісланої інформації.
- 2) Було виявлено дві хост-IP-адреси, що спілкувалися. Однією IP-адресою хоста була 192.168.56.101, а іншою – 192.168.56.102.
 - 3) Хост 192.168.56.101 (Зловмисник) надсилав пакети INIT, призначені для ініціювання спілкування між SIGTRAN хостами, до віддаленого вузла.
 - 4) Використовуваним сигнальним протоколом для обміну повідомленнями між двома хостами був Stream Control Transmission Protocol (SCTP), який є базовим надійним транспортним протоколом для мереж SIGTRAN, що функціонує над IP-рівнем.

Отримані в результаті цього експерименту IP-адреси відповідають фактичній інформації про конфігурацію IP-мережі, отриманій з командного рядка адміністратора обох SIGTRAN-хостів.

Порівнявши інформацію про IP-адреси, захоплену на знімку екрана Wireshark з результатів тестування, з фактичними даними конфігурації мережі для двох хост-вузлів SIGTRAN, цей експеримент успішно продемонстрував, що SS7 дійсно вразливий до кібератак, оскільки конфіденційна інформація про мережеві конфігурації, така як IP-адреси, може бути легко розкрита шляхом перехоплення трафіку в IP-мережі. А використовуючи сканування Nmap можна отримати точний порт, на якому працює sctp сервер.

3.2 IMSI Catch

Цей експеримент був спрямований на демонстрування, вразливості SIGTRAN мережі, що розкриває критично важливу мережеву інформацію, за допомогою якої можливо здійснити серію атак, спрямованих на отримання конфіденційної інформації про жертву. Експериментальну мережу наведено на Рисунку 3.2.

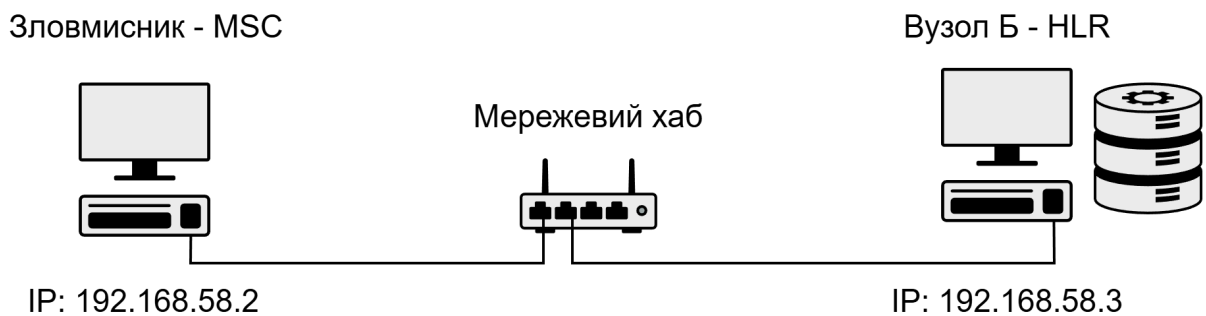


Рисунок 3.2 – Експериментальна мережа IMSI Catch

Процедура тестування:

Зловмисник видає себе за центр SMS-повідомлень (SMSC), який бажає доставити SMS-повідомлення абоненту. Щоб доставити SMS, фальшивий SMSC потребує адреси MSC/VLR, який наразі обслуговує цільового абонента.

Фальшивий SMSC створює запит sendIMSI і включає MSISDN (Мобільний міжнародний абонентський номер) цільового абонента. Потім він адресує повідомлення Шлюзовій Точці Передачі Сигналізації в домашній мережі цільового абонента. Оскільки зловмисник не знає адреси відповідного HLR (Реєстр домашнього розташування), він встановлює Global Title Translations (GTT) і використовує MSISDN як адресу абонента, що викликається (SCCP called party address). Адреса зловмисника буде розміщена в полі адреси сторони, що викликає (SCCP calling party address).

Шлюзовий STP виконує GTT, щоб знайти код точки (Point Code) та підсистему (Subsystem Number) HLR. Потім повідомлення маршрутизується до HLR. HLR запитує свою базу даних, використовуючи MSISDN як ключ. Результати запиту розміщуються у відповіді returnResultLast sendIMSI і надсилаються назад до Шлюзового STP для маршрутизації до початкового відправника запиту sendIMSI.

3.2.1 Отримані результати

Результати цього експерименту, які були вилучені зі знімка екрана Wireshark (Додаток Б), показані в Таблиці 3.2 нижче.

Таблиця 3.2 – Витягнуті результати тесту IMSI Catch

No.	Time	Source	Destination	Protocol	Length	Info
1	0.00000	192.168.58.2	192.168.58.3	SCTP	82	INIT
2	0.00001	192.168.58.3	192.168.58.2	SCTP	306	INIT_ACK
3	0.00002	192.168.58.2	192.168.58.3	SCTP	278	COOKIE_ECHO
4	0.00005	192.168.58.3	192.168.58.2	SCTP	50	COOKIE_ACK
5	0.00659	192.168.58.2	192.168.58.3	M3UA	78	ASPUP
6	0.00661	192.168.58.3	192.168.58.2	SCTP	62	SACK (Ack=0, Arwnd=106480)
7	0.00800	192.168.58.2	192.168.58.3	M3UA	78	ASPUP_ACK
8	0.00802	192.168.58.3	192.168.58.2	SCTP	62	SACK (Ack=0, Arwnd=106480)
9	0.00917	192.168.58.2	192.168.58.3	M3UA	86	ASPAC
10	0.01037	192.168.58.3	192.168.58.2	M3UA	102	SACK (Ack=1, Arwnd=106496) ASPAC_ACK
11	0.21429	192.168.58.2	192.168.58.3	SCTP	62	SACK (Ack=1, Arwnd=106496)
12	9.59159	1	2	GSM MAP	186	invoke sendIMSI
13	9.70205	2	1	GSM MAP	222	SACK (Ack=2, Arwnd=106496) returnResultLast sendIMSI
14	9.90631	192.168.58.2	192.168.58.3	SCTP	62	SACK (Ack=2, Arwnd=106496)
15	10.0454	192.168.58.2	192.168.58.3	SCTP	54	SHUTDOWN
16	10.0454	192.168.58.3	192.168.58.2	SCTP	50	SHUTDOWN_ACK
17	10.0454	192.168.58.2	192.168.58.3	SCTP	50	SHUTDOWN_COMPLETE

Результати, представлені в Таблиці 3.2, показують наступне:

У пакеті № 12 Зловмисник зі свого фальшивого MSC надсилає запит sendIMSI, використовуючи MSISDN як адресу абонента та GT свого симульованого вузла як адресу відправника (Рисунок 3.3). Цей запит адресується до HLR, що обслуговує абонента.

```

▼ Signalling Connection Control Part
  Message Type: Unitdata (0x09)
  .... 0001 = Class: 0x1
  0000 .... = Message handling: No special options (0x0)
  Pointer to first Mandatory Variable parameter: 3
  Pointer to second Mandatory Variable parameter: 14
  Pointer to third Mandatory Variable parameter: 25
  > Called Party address (11 bytes)
  ▼ Calling Party address (11 bytes)
    > Address Indicator
      SubSystem Number: VLR (Visitor Location Register) (7)
      [Linked to TCAP, TCAP SSN linked to GSM_MAP]
    ▼ Global Title 0x4 (9 bytes)
      Translation Type: 0x00 (0)
      0001 .... = Numbering Plan: ISDN/telephony (0x1)
      .... 0010 = Encoding Scheme: BCD, even number of digits (0x2)
      .000 0100 = Nature of Address Indicator: International number (0x04)
    > Calling Party Digits: 441234567890
  > Transaction Capabilities Application Part
  ▼ GSM Mobile Application
    ▼ Component: invoke (1)
      ▼ invoke
        invokeID: 0
        ▼ opCode: localValue (0)
          localValue: sendIMSI (58)
        > msisdn: 9102512222222

```

Рисунок 3.3 – Запит sendIMSI

Пакет № 13 – відповідь HLR що містить запитувану інформацію. Атакуючий отримує IMSI абонента та GT обслуговуючої HLR вузла абонента (Рисунок 3.4).

```

▼ Signalling Connection Control Part
  Message Type: Unitdata (0x09)
  .... 0001 = Class: 0x1
  0000 .... = Message handling: No special options (0x0)
  Pointer to first Mandatory Variable parameter: 3
  Pointer to second Mandatory Variable parameter: 16
  Pointer to third Mandatory Variable parameter: 27
  > Called Party address (13 bytes)
  ▼ Calling Party address (11 bytes)
    > Address Indicator
      SubSystem Number: HLR (Home Location Register) (6)
      [Linked to TCAP, TCAP SSN linked to GSM_MAP]
    ▼ Global Title 0x4 (9 bytes)
      Translation Type: 0x00 (0)
      0001 .... = Numbering Plan: ISDN/telephony (0x1)
      .... 0010 = Encoding Scheme: BCD, even number of digits (0x2)
      .000 0100 = Nature of Address Indicator: International number (0x04)
    > Calling Party Digits: 201500000000
  > Transaction Capabilities Application Part
  ▼ GSM Mobile Application
    ▼ Component: returnResultLast (2)
      ▼ returnResultLast
        invokeID: 0
        ▼ resultretres
          ▼ opCode: localValue (0)
            localValue: sendIMSI (58)
            IMSI: 609156789123456

```

Рисунок 3.4 – Відповідь sendIMSI

3.3 Any Time Interrogation

Цей експеримент був продовженням попереднього експерименту і мав на меті продемонструвати, як зловмисник може використати критично важливу мережеву інформацію, отриману за допомогою "перерахунку" мережі, на свою користь та здійснити атаку, спрямовану на отримання конфіденційної інформації про жертву.

Результати цього експерименту допоможуть продемонструвати, що IP-мережі є вразливими до кібератак. Це дослідження надало додаткові докази на користь того, що IP-мережі в цілому не є достатньо безпечними для транспортування сигнальних повідомлень SS7.

Експериментальну мережу наведено на Рисунку 3.5.

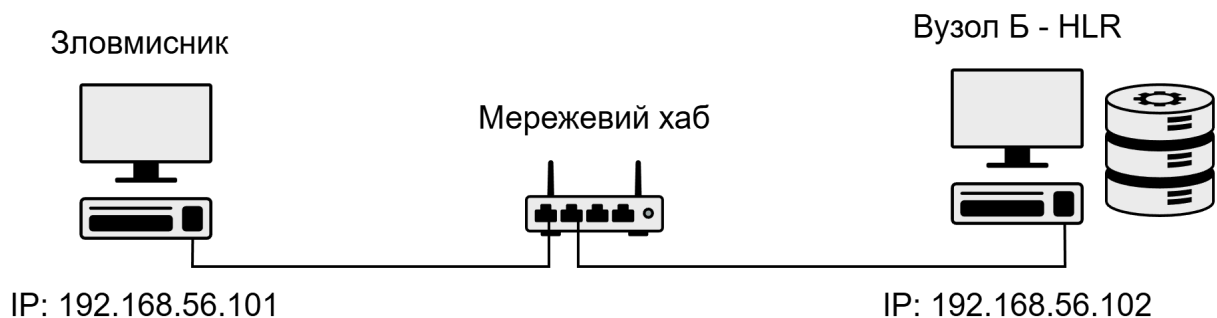


Рисунок 3.5 – Експериментальна мережа Any Time Interrogation

Процедура тестування:

Два вузли SIGTRAN, позначені як Зловмисник та Вузол Б, були налаштовані зі статичними IP-адресами 192.168.56.101 та 192.168.56.102 відповідно.

Зловмисник представляв хакера, який отримав доступ до того ж пулу TCP/IP-мережі, що й Вузол Б, який транспортував сигнальні повідомлення SS7

через IP-мережу. Зловмисник був підключений у режимі прослуховування, що дозволяло йому бачити весь трафік.

Використовуючи програмне забезпечення SiGPloit Зловмисник надіслав запит anyTimeInterrogation до Вузла Б, що в даному експерименті слугує як домашня HLR абонента жертви.

Використовуючи програмне забезпечення для перехоплення мережевого трафіку Wireshark, встановлене на своєму комп'ютері, зловмисник "прослуховував" мережу. Таким чином, він отримав критично важливу інформацію про абонента, включаючи IMEI та місцезнаходження.

3.3.1 Отримані результати

Результати цього експерименту, які були вилучені зі знімка екрана Wireshark (Додаток В), показані в Таблиці 3.3 нижче.

Таблиця 3.3 – Витягнуті результати тесту Any Time Interrogation

No.	Time	Source	Destination	Protocol	Length	Info
6	175.964	192.168.56.101	192.168.56.102	SCTP	82	INIT
7	175.964	192.168.56.102	192.168.56.101	SCTP	306	INIT_ACK
8	175.964	192.168.56.101	192.168.56.102	SCTP	278	COOKIE_ECHO
9	175.964	192.168.56.102	192.168.56.101	SCTP	50	COOKIE_ACK
10	175.985	192.168.56.101	192.168.56.102	M3UA	78	ASPUP
11	175.985	192.168.56.102	192.168.56.101	SCTP	62	SACK (Ack=0, Arwnd=106480)
12	175.987	192.168.56.101	192.168.56.102	M3UA	78	ASPUP_ACK
13	175.987	192.168.56.102	192.168.56.101	SCTP	62	SACK (Ack=0, Arwnd=106480)
14	175.990	192.168.56.101	192.168.56.102	M3UA	86	ASPAC
15	175.992	192.168.56.102	192.168.56.101	M3UA	102	SACK (Ack=1, Arwnd=106496) ASPAC_ACK
16	176.193	192.168.56.101	192.168.56.102	SCTP	62	SACK (Ack=1, Arwnd=106496)
17	185.657	1	2	GSM MAP	210	invoke anyTimeInterrogation
18	185.773	2	1	GSM MAP	294	SACK (Ack=2, Arwnd=106496) returnResultLast anyTimeInterrogation

Кінець таблиці 3.3

19	185.977	192.168.56.101	192.168.56.102	SCTP	62	SACK (Ack=2, Arwnd=106496)
20	196.174	192.168.56.102	192.168.56.101	SCTP	54	SHUTDOWN
21	196.174	192.168.56.101	192.168.56.102	SCTP	50	SHUTDOWN_ACK
22	196.174	192.168.56.102	192.168.56.101	SCTP	50	SHUTDOWN_COMPLETE

Результати, представлені в Таблиці 3.3, чітко відображають наступну інформацію:

- Отримавши IP адресу та SCTP порт віддаленої HLR зломисник розпочав атаку.
- Пакети № 6-9 це аналог хендшейку TCP, але для SCTP. Вони свідчать про успішне встановлення зв'язку між атакуючим та HLR. Пакети № 10-16 представляють комунікацію між віддаленими вузлами M3UA, що рівень адаптації готовий до прийому трафіку або повідомлень про технічне обслуговування.
- Пакетом № 17 атакуючий надсилає запит anyTimeInterrogation до HLR, вказуючи MSISDN (номер телефону) жертви. MSISDN та запитувану інформацію (requestedInfo) показано на Рисунку 3.6.

17	185.657...	1	2	GSM MAP	210 invoke anyTimeInterrogation
<					
▼	GSM Mobile Application				
▼	Component: invoke (1)				
▼	invoke				
	invokeID: 0				
>	opCode: localValue (0)				
▼	subscriberIdentity: msisdn (1)				
▼	msisdn: 916995697567f5				
	1... = Extension: No Extension				
	.001 = Nature of number: International Number (0x1)				
	 0001 = Number plan: ISDN/Telephony Numbering (Rec ITU-T E.164) (0x1)				
▼	E.164 number (MSISDN): 96599657765				
	Country Code: Kuwait (State of) (965)				
▼	requestedInfo				
	locationInformation				
	subscriberState				
	currentLocation				
	requestedDomain: cs-Domain (0)				
	imei				

Рисунок 3.6 – Запит anyTimeInterrogation

- У відповідь на запит атакуючий безперешкодно отримав конфіденційну інформацію про абонента, а саме: останнє місцезнаходження та IMEI (див. Рисунок 3.7).

```
18|185.773... 2          1          GSM MAP  294 SACK (Ack=2, Arwnd=106496) returnResultLast anyTimeInterrogation

> subscriberState: assumedIdle (0)
v locationInformationGPRS
  v geographicalInformation: 1027fba11728d202
    0001 .... = Location estimate: Ellipsoid point with uncertainty Circle (1)
    0... .... = Sign of latitude: North (0)
    .010 0111 1111 1011 1010 0001 = Degrees of latitude: 2620321 (28,11300 degrees)
    0001 0111 0010 1000 1101 0010 = Degrees of longitude: 1517778 (32,56798 degrees)
    .000 0010 = Uncertainty code: 2 (2,1 m)
    [Location OSM URI: https://www.openstreetmap.org/?mlat=28,11300&mlon=32,56798&zoom=12]
  v sgsn-Number: 910251555555f5
    1... .... = Extension: No Extension
    .001 .... = Nature of number: International Number (0x1)
    .... 0001 = Number plan: ISDN/Telephony Numbering (Rec ITU-T E.164) (0x1)
  v E.164 number (MSISDN): 20155555555
    Country Code: Egypt (Arab Republic of) (20)
  currentLocationRetrieved
  ageOfLocationInformation: 30
> imei: 53029900711684
```

Рисунок 3.7 – Відповідь anyTimeInterrogation

Цей експеримент успішно продемонстрував, що маючи доступ до SS7 хабу та знаючи лише номер абонента можна визначити його точне місцезнаходження. Що знову показує вразливість SS7 до кібератак зі IP-мережі.

3.4 Provide Subscriber Info

Цей експеримент є схожим на попередній Any Time Interrogation. Він так само має на меті продемонструвати, як зловмисник може використати критично важливу мережеву інформацію, отриману за допомогою "перерахунку" мережі та IMSI Catch, на свою користь та здійснити атаку, спрямовану на отримання місцезнаходження жертви.

Експериментальну мережу наведено на Рисунку 3.8.

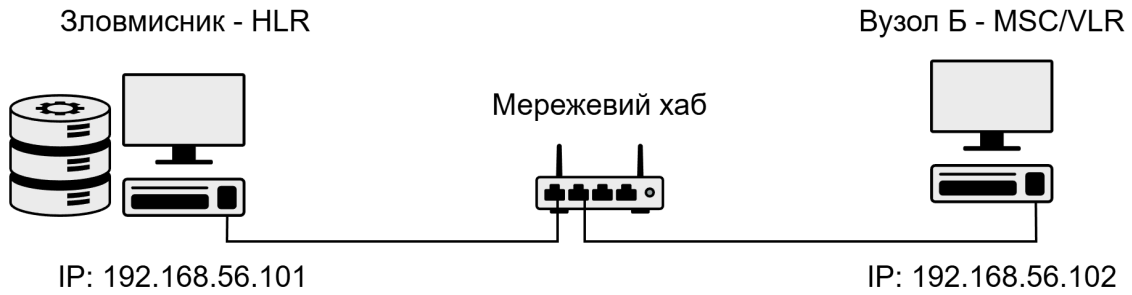


Рисунок 3.8 – Експериментальна мережа Provide Subscriber Info

Процедура тестування:

Зловмисник представляв хакера, який видавав себе за HLR. Зловмисник був підключений у режимі прослуховування.

Атакуючий надсилав повідомлення MAP-Provide-Subscriber-Info (PSI) Request безпосередньо до MSC/VLR, що обслуговує абонента. Це можливо завдяки тому, що в попередній загрозі (IMSI Catch) зловмисник отримав адресу MSC/VLR та IMSI абонента.

3.4.1 Отримані результати

Результати цього експерименту, які були вилучені зі знімка екрана Wireshark (Додаток Г), показані в Таблиці 3.4 нижче.

Таблиця 3.4 – Витягнуті результати тесту Provide Subscriber Info Wireshark

No.	Time	Source	Destination	Protocol	Length	Info
1	0.00000	192.168.56.101	192.168.56.102	SCTP	82	INIT
2	0.00001	192.168.56.102	192.168.56.101	SCTP	306	INIT_ACK
3	0.00002	192.168.56.101	192.168.56.102	SCTP	278	COOKIE_ECHO
4	0.00005	192.168.56.102	192.168.56.101	SCTP	50	COOKIE_ACK
5	0.00510	192.168.56.101	192.168.56.102	M3UA	78	ASPUP
6	0.00512	192.168.56.102	192.168.56.101	SCTP	62	SACK (Ack=0, Arwnd=106480)
7	0.00637	192.168.56.101	192.168.56.102	M3UA	78	ASPUP_ACK
8	0.00639	192.168.56.102	192.168.56.101	SCTP	62	SACK (Ack=0, Arwnd=106480)

9	0.00752	192.168.56.101	192.168.56.102	M3UA	86	ASPAC
---	---------	----------------	----------------	------	----	-------

Кінець таблиці 3.4

10	0.00868	192.168.56.102	192.168.56.101	M3UA	102	SACK (Ack=1, Arwnd=106496) ASPAC_ACK
11	0.21119	192.168.56.101	192.168.56.102	SCTP	62	SACK (Ack=1, Arwnd=106496)
12	16.1616	1	2	GSM MAP	202	invoke provideSubscriberInfo
13	16.2091	2	1	GSM MAP	302	SACK (Ack=2, Arwnd=106496) returnResultLast provideSubscriberInfo
14	16.4112	192.168.56.101	192.168.56.102	SCTP	62	SACK (Ack=2, Arwnd=106496)
15	26.5572	192.168.56.102	192.168.56.101	SCTP	54	SHUTDOWN
16	26.5573	192.168.56.101	192.168.56.102	SCTP	50	SHUTDOWN_ACK
17	26.5573	192.168.56.102	192.168.56.101	SCTP	50	SHUTDOWN COMPLETE

Із Таблиці 3.4 можна виокремити таку інформацію:

- Пакетом № 12 зловмисник сформує повідомлення MAP-PSI (Req.) та відправляє його до Шлюзової Точки Передачі Сигналізації (Gateway STP), адресуючи його Обслуговуючому MSC/VLR (адреса якого отримана в рамках експерименту 3.2). IMSI абонента (отримане в рамках експерименту 3.2) буде включено в це повідомлення (Рисунок 3.9).

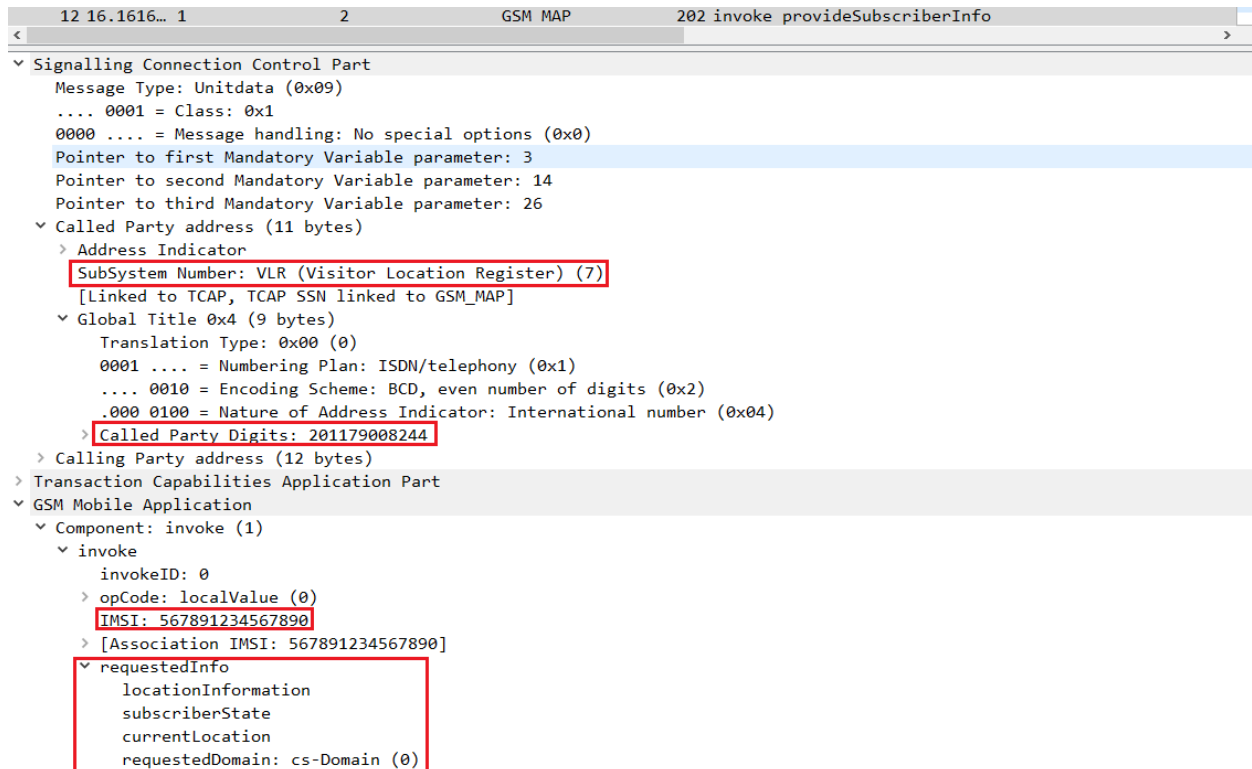


Рисунок 3.9 – Запит provideSubscriberInfo

- Після того, як MSC/VLR оновив інформацію про місцезнаходження абонента, він сформував та надіслав повідомлення MAP-PSI (Resp.) Пакетом № 13, що містить запитану інформацію про місцезнаходження (Рисунок 3.10), до "Фальшивого HLR".

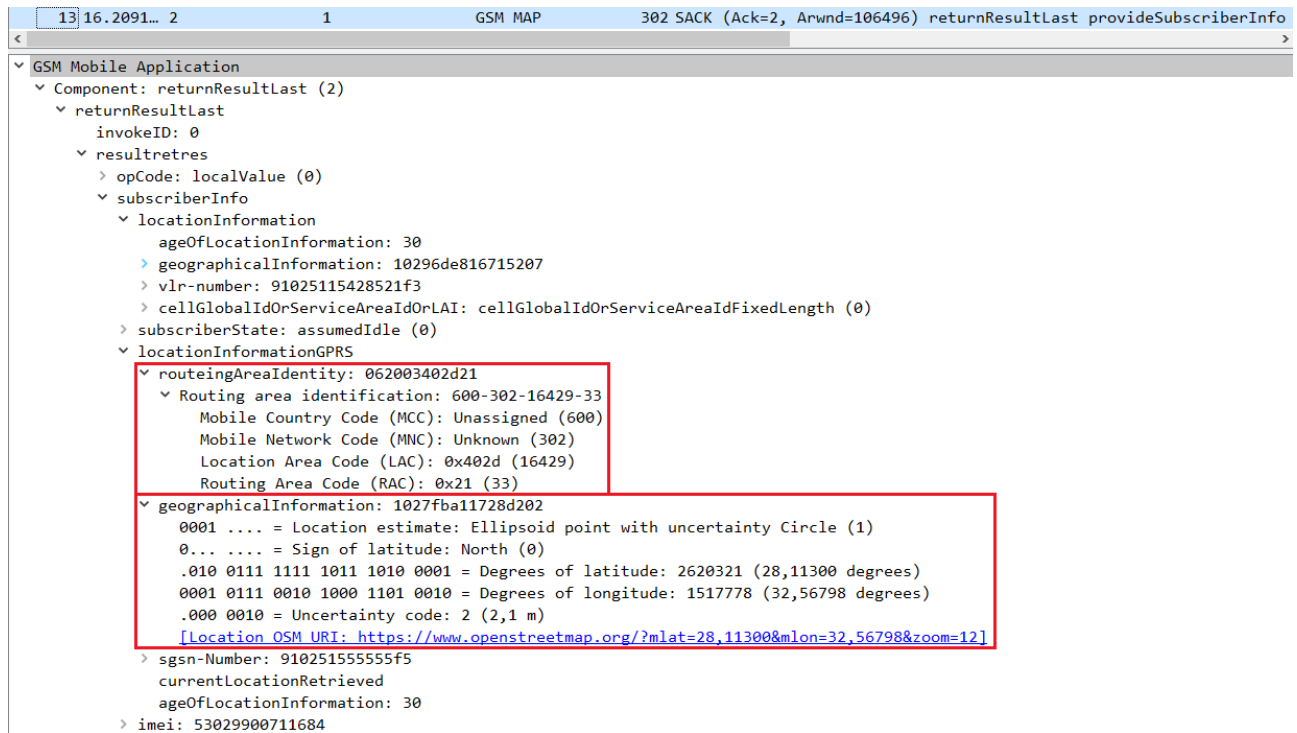


Рисунок 3.10 – Відповідь provideSubscriberInfo

В результаті атаки зловмисник отримує таку інформацію щодо місцезнаходження цільового абонента: Ідентифікатор комірки (Cell Id), Мобільний код країни (MCC), Мобільний код мережі (MNC), Код зони місцезнаходження (LAC). Це знову доводить можливість отримання конфіденційної інформації через використання SIGTRAN.

3.5 MITM (Update Location)

Передумова цієї атаки полягає в тому, що зловмисник видаватиме себе за MSC/VLR і надсилатиме повідомлення MAP-Update-Location- (UL) Request безпосередньо до HLR абонента. Після завершення процедур оновлення місцезнаходження, зловмисник отримуватиме повідомлення та дзвінки, що надходять абоненту. Такий стан триватиме доки абонент не переміститься до іншого MSC/VLR, не перезавантажить телефон або не здійснить вихідний дзвінок.

Експериментальну мережу наведено на Рисунку 3.11.

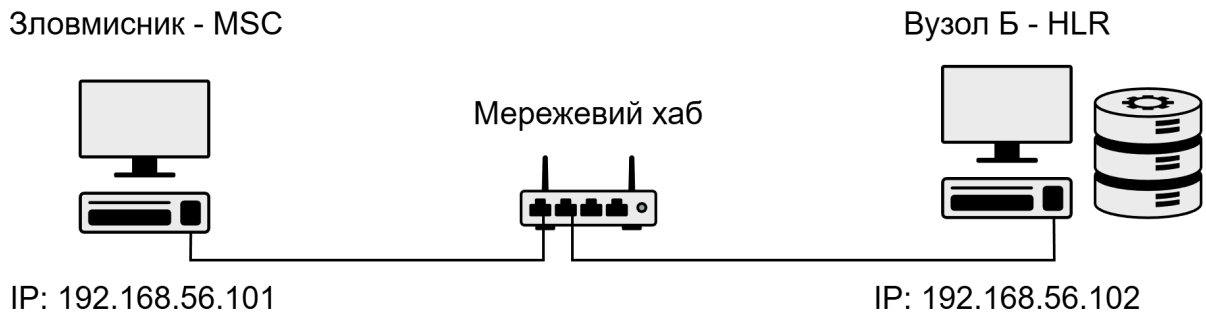


Рисунок 3.11 – Експериментальна мережа Update Location

Процедура тестування:

Зловмисник представляв хакера, який видаватиме себе за MSC/VLR що має зв'язок із HLR абонента через мережевий хаб. Зловмисник був підключений до хаба у режимі прослуховування, що дозволяло йому бачити весь трафік.

Використовуючи програмне забезпечення SiGPloit Зловмисник надіслав запит Update Location до Вузла Б, що в даному експерименті слугує як домашня HLR абонента жертви.

Як і в попередніх експериментах, за допомогою Wireshark, після завершення процедур оновлення місцезнаходження, зловмисник захопив SMS-повідомлення абонента та направив його до справжнього отримувача.

Звичайна процедура доставки SMS-повідомлень не була захоплена wireshark, адже вона відбувається в іншій мережі та не проходить через хаб, до якого має доступ зловмисник.

3.5.1 Отримані результати

Результати цього експерименту, які були вилучені зі знімка екрана Wireshark (Додаток Д), показані в Таблиці 3.5 нижче.

Таблиця 3.5 – Витягнуті результати тесту MITM (Update Location)

No.	Time	Source	Destination	Protocol	Length	Info
1	0.00000	192.168.56.101	192.168.56.102	SCTP	82	INIT
2	0.00001	192.168.56.102	192.168.56.101	SCTP	306	INIT_ACK
3	0.00002	192.168.56.101	192.168.56.102	SCTP	278	COOKIE_ECHO
4	0.00005	192.168.56.102	192.168.56.101	SCTP	50	COOKIE_ACK
5	0.00373	192.168.56.101	192.168.56.102	M3UA	78	ASPUP
6	0.00374	192.168.56.102	192.168.56.101	SCTP	62	SACK (Ack=0, Arwnd=106480)
7	0.00573	192.168.56.101	192.168.56.102	M3UA	78	ASPUP_ACK
8	0.00576	192.168.56.102	192.168.56.101	SCTP	62	SACK (Ack=0, Arwnd=106480)
9	0.00695	192.168.56.101	192.168.56.102	M3UA	86	ASPAC
10	0.00791	192.168.56.102	192.168.56.101	M3UA	102	SACK (Ack=1, Arwnd=106496) ASPAC_ACK
11	0.21195	192.168.56.101	192.168.56.102	SCTP	62	SACK (Ack=1, Arwnd=106496)
12	9.69052	1	2	GSM MAP	206	invoke updateLocation
13	9.73540	2	1	GSM MAP	238	SACK (Ack=2, Arwnd=106496) invoke insertSubscriberData
14	9.75713	2	1	GSM MAP	218	SACK (Ack=2, Arwnd=106496) returnResultLast insertSubscriberData
15	9.77689	2	1	GSM SMS	246	SACK (Ack=3, Arwnd=106496) invoke forwardSM
16	9.78737	1	2	GSM SMS	246	SACK (Ack=3, Arwnd=106496) invoke forwardSM
17	9.99219	192.168.56.101	192.168.56.102	SCTP	62	SACK (Ack=4, Arwnd=106496)
18	10.1224	192.168.56.102	192.168.56.101	SCTP	54	SHUTDOWN
19	10.1224	192.168.56.101	192.168.56.102	SCTP	50	SHUTDOWN_ACK
20	10.1224	192.168.56.102	192.168.56.101	SCTP	50	SHUTDOWN_COMPLETE

Таблиця 3.5 наглядно показує процес атаки:

- Пакетом № 12 зломисник, що діє як Фальшивий Новий MSC/VLR, надсилає запит invoke updatelocation до HLR абонента. Цей запит ініціює процедуру оновлення місцезнаходження абонента в базі даних HLR.

- У відповідь на запит `updateLocation`, HLR абонента надсилає повідомлення `invoke insertSubscriberData` до Фальшивого MSC (пакет № 13). Це повідомлення містить інформацію про абонента, яка має бути збережена у VLR (в даному випадку, у Фальшивому VLR зломисника) для подальшого використання.
- Пакетом №14 Фальшивий MSC підтверджує отримання даних абонента, та каже, що абонент наразі підключений до нього, надсилаючи повідомлення `returnResultLast insertSubscriberData` до HLR.
- Після цього HLR ініціює послідовність відміни місцезнаходження з попереднім обслуговуючим MSC. Після завершення цієї процедури HLR надсилає `Update Location Acknowledgement` до Фальшивого MSC зломисника. Усі наступні вхідні дзвінки та SMS-повідомлення до абонента тепер будуть надсилатися на Фальшивий MSC зломисника, що призведе до переривання отримання вхідних текстових повідомлень та голосових дзвінків абонентом.
- Пакет 15: Повідомлення `invoke forwardSM`. Цей пакет відображає передачу SMS, яка тепер маршрутизується через HLR до нового (фальшивого) MSC/VLR атакуючого (Рисунок 3.12).

```

15 9.77609... 2      1      GSM SMS      246 SACK (Ack=3, Arwnd=106496) invoke forwardSM
<
> Frame 15: 246 bytes on wire (1968 bits), 246 bytes captured (1968 bits) on interface lo, id 0
> Ethernet II, Src: 00:00:00_00:00:00 (00:00:00:00:00:00), Dst: 00:00:00_00:00:00 (00:00:00:00:00:00)
> Internet Protocol Version 4, Src: 192.168.56.102, Dst: 192.168.56.101
> Stream Control Transmission Protocol, Src Port: 2906 (2906), Dst Port: 2905 (2905)
> MTP 3 User Adaptation Layer
> Signalling Connection Control Part
> Transaction Capabilities Application Part
> GSM Mobile Application
v GSM SMS TPDU (GSM 03.40) SMS-DELIVER
  0... .... = TP-RP: TP Reply Path parameter is not set in this SMS SUBMIT/DELIVER
  .0.. .... = TP-UDHI: The TP UD field contains only the short message
  ..0. .... = TP-SRI: A status report shall not be returned to the SME
  .... 0... = TP-LP: The message has not been forwarded and is not a spawned message
  .... .1.. = TP-MMS: No more messages are waiting for the MS in this SC
  .... ..00 = TP-MTI: SMS-DELIVER (0)
> TP-Originating-Address - (2010789123456)
> TP-PID: 0
> TP-DCS: 0
> TP-Service-Centre-Time-Stamp
  TP-User-Data-Length: (12) depends on Data-Coding-Scheme
v TP-User-Data
  SMS text: Hello World!

```

Рисунок 3.12 – Перехоплене повідомлення

- У пакеті 16 MSC/VLR атакуючого перенаправляє перехоплене повідомлення до справжнього абонента використовуючи адресу, отриману в пакеті № 13.

3.6 SMS Spoofing

Цей експеримент демонструє можливість надсилати фішингові повідомлення. Він має на меті показати, що зловмисник може використати критично важливу мережеву інформацію, отриману за допомогою атаки IMSI Catch, на свою користь. Маніпулювання полем TP-Originating-Address та зміст SMS-повідомлення дозволяє здійснити фішингову атаку.

Експериментальну мережу наведено на Рисунку 3.13.

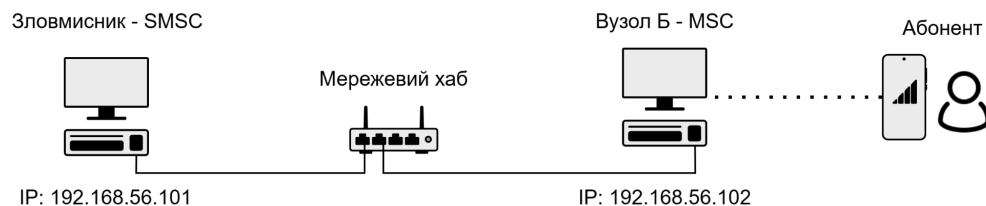


Рисунок 3.13 – Експериментальна мережа SMS Spoofing

Процедура тестування:

Була налаштована тестова мережа, що імітує частину SS7 мережі, доступну зловмиснику.

Зловмисник, використовуючи спеціалізоване програмне забезпечення SiGPloit, сформував SMS-повідомлення, маніпулюючи полем TP-Originating-Address для імітації легітимного відправника. Текст SMS-повідомлення було складено таким чином, щоб імітувати фішингову атаку. Сформоване SMS-повідомлення було відправлено на номер цільового абонента через імітовану SS7 мережу.

Використовуючи програмне забезпечення для перехоплення мережевого трафіку Wireshark, встановлене на своєму комп'ютері, зловмисник "прослуховував" мережу, щоб відстежувати активність між мережевими компонентами та переконатися у успішній доставці підробленого SMS.

Було здійснено живе захоплення мережевої активності за допомогою Wireshark та проведено його аналіз.

3.6.1 Отримані результати

Результати цього експерименту, які були вилучені зі знімка екрана Wireshark (Додаток Е), показані в Таблиці 3.6 нижче.

Таблиця 3.6 – Витягнуті результати тесту SMS Spoofing

No.	Time	Source	Destination	Protocol	Length	Info
1	0.00000	192.168.56.101	192.168.56.102	SCTP	82	INIT
2	0.00004	192.168.56.102	192.168.56.101	SCTP	306	INIT_ACK
3	0.00007	192.168.56.101	192.168.56.102	SCTP	278	COOKIE_ECHO
4	0.00012	192.168.56.102	192.168.56.101	SCTP	50	COOKIE_ACK
5	0.00699	192.168.56.101	192.168.56.102	M3UA	78	ASPUP
6	0.00699	192.168.56.102	192.168.56.101	SCTP	62	SACK (Ack=0, Arwnd=106480)
7	0.00817	192.168.56.101	192.168.56.102	M3UA	78	ASPUP_ACK
8	0.00817	192.168.56.102	192.168.56.101	SCTP	62	SACK (Ack=0, Arwnd=106480)

Кінець таблиці 3.6

9	0.01070	192.168.56.101	192.168.56.102	M3UA	86	ASPAC
10	0.01202	192.168.56.102	192.168.56.101	M3UA	102	SACK (Ack=1, Arwnd=106496) ASPAC_ACK
11	0.21374	192.168.56.101	192.168.56.102	SCTP	62	SACK (Ack=1, Arwnd=106496)
12	13.6027	1	2	GSM SMS	262	invoke forwardSM
13	13.8057	192.168.56.102	192.168.56.101	SCTP	62	SACK (Ack=2, Arwnd=106496)
14	13.9719	192.168.56.102	192.168.56.101	SCTP	54	SHUTDOWN
15	13.9719	192.168.56.101	192.168.56.102	SCTP	50	SHUTDOWN_ACK
16	13.9720	192.168.56.102	192.168.56.101	SCTP	50	SHUTDOWN_COMPLETE

Результати, представлені в Таблиці 6.1, чітко відображають наступну інформацію:

Пакети № 1-11 демонструють успішне встановлення SCTP та M3UA зв'язку між зломисником та цільовою мережею, аналогічно попереднім тестам.

У пакеті № 12 видно GSM SMS з інформацією invoke forwardSM. Це вказує на ініціацію процедури пересилання SMS. Вміст пакету (як показано на Рисунку 3.14) чітко показує, що поле TP-Originating-Address містить значення "Facebook". З того ж пакету видно, що поле SMS text містить фішинговий текст "Please verify your password at <http://facebuk.com>". Це демонструє здатність зломисника підробляти ідентифікатор відправника та вставляти довільний шкідливий контент у SMS-повідомлення.

12 13.6027... 1	2	GSM SMS	262 invoke forwardSM
<			
▼ GSM SMS TPDU (GSM 03.40) SMS-DELIVER			
0... = TP-RP: TP Reply Path parameter is not set in this SMS SUBMIT/DELIVER			
.0... = TP-UDHI: The TP UD field contains only the short message			
..1. = TP-SRI: A status report shall be returned to the SME			
.... 0... = TP-LP: The message has not been forwarded and is not a spawned message			
.... .1.. = TP-MMS: No more messages are waiting for the MS in this SC			
.... ..00 = TP-MTI: SMS-DELIVER (0)			
▼ TP-Originating-Address - (Facebook)			
Length: 14 address digits			
1... = Extension: No extension			
.101 = Type of number: Alphanumeric (coded according to 3GPP TS 23.038 GSM 7-bit default alphabet) (5)			
.... 0000 = Numbering plan: Unknown (0)			
TP-OA Digits: Facebook			
> TP-PID: 0			
> TP-DCS: 0			
> TP-Service-Centre-Time-Stamp			
TP-User-Data-Length: (49) depends on Data-Coding-Scheme			
▼ TP-User-Data			
SMS text: Please verify your password at http://facebuk.com			

Рисунок 3.14 – Фішингове повідомлення

Цей експеримент успішно продемонстрував, що SS7 мережі, через IP, є вразливими до SMS Spoofing атак. Можливість підробки ідентифікатора відправника та доставки фішингових повідомлень становить серйозну загрозу для користувачів мобільних мереж, підкреслюючи необхідність посилення заходів безпеки.

Висновки до розділу 3

Проведені в цьому розділі експерименти з моделювання атак на сигнальні мережі SS7, що транспортуються через IP-інфраструктуру за допомогою

протоколів SIGTRAN, переконливо довели вразливість сучасних телекомунікаційних мереж до кібератак. Завдяки використанню інструменту SiGPloit та програмного забезпечення для аналізу трафіку Wireshark, було продемонстровано, як зловмисник може збирати критично важливу мережеву інформацію та використовувати її для здійснення низки шкідливих дій.

Основні висновки, отримані в ході експериментів, включають:

Розкриття конфіденційної мережевої інформації (Network Enumeration): Було підтверджено, що базова мережева інформація, така як IP-адреси хост-вузлів та відкриті порти, може бути легко отримана за допомогою загальнодоступних інструментів, таких як Nmap та Wireshark. Ця інформація є первинною передумовою для подальших, більш складних атак.

Несанкціоноване отримання IMSI (IMSI Catch): Було доведено, що зловмисник може імітувати легітимний центр SMS-повідомлень (SMSC) та, шляхом надсилання запиту sendIMSI, отримати IMSI цільового абонента. Це відкриває шлях до подальших атак.

Витік інформації про місцезнаходження абонента (Any Time Interrogation): Експеримент успішно продемонстрував, що зловмисник, маючи доступ до SS7 хабу та знаючи лише номер телефону абонента, може визначити його точне місцезнаходження. Це свідчить про серйозні прогалини в конфіденційності даних абонентів у SIGTRAN-мережах.

Збір додаткових даних абонента (Provide Subscriber Info): Завдяки інформації, отриманій з попередніх атак (адреси MSC/VLR та IMSI), зловмисник зміг успішно ініціювати запит Provide Subscriber Info та отримати додаткові конфіденційні дані про абонента, включаючи детальну інформацію про місцезнаходження (Cell ID, MCC, MNC, LAC). Це підкреслює послідовність та ескалацію атак у вразливих мережах.

Перехоплення трафіку та SMS (Update Location MITM): Найбільш критичним результатом є демонстрація можливості здійснення атаки типу

"людина посередині" (Man-in-the-Middle) шляхом підробки процедури оновлення місцезнаходження (Update Location). Зловмисник, видаючи себе за MSC/VLR, зумів перехопити вхідні SMS-повідомлення, призначені для жертви, а також, за бажанням, перенаправляти їх до справжнього отримувача. Це підтверджує прямий вплив на доступність та конфіденційність комунікацій.

Підробка SMS-повідомлень (SMS Spoofing): Експеримент підтвердив, що зловмисники можуть легко маніпулювати полем TP-Originating-Address в SMS-повідомленнях, що дозволяє надсилати фішингові SMS з довільним текстом від імені будь-якого відправника. Це створює пряму загрозу для користувачів у вигляді шахрайства та компрометації облікових записів.

Таким чином, результати всіх проведених експериментів однозначно свідчать про те, що використання IP-мереж для транспортування SS7 сигналізації створює значні вразливості, які можуть бути експлуатовані для здійснення різноманітних кібератак. Ці атаки варіюються від розкриття конфіденційної мережевої інформації до прямого впливу на приватність абонентів, перехоплення їхніх комунікацій та проведення фішингових кампаній. Ця робота надає надійні докази того, що існуючі механізми безпеки в таких мережах є недостатніми, і вимагає негайного впровадження посиленних заходів захисту для забезпечення цілісності та конфіденційності SS7 сигналізації.

4 РЕКОМЕНДАЦІЇ

Розробка та впровадження ефективних заходів безпеки у сучасних телекомунікаційних мережах є критично важливим завданням, особливо з огляду на зростаючу конвергенцію традиційних сигнальних протоколів SS7 з IP-інфраструктурами через використання SIGTRAN. Розділ 3 цієї роботи переконливо продемонстрував низку вразливостей та потенційних кібератак, які можуть бути реалізовані проти сигнальних повідомлень SS7, що транспортуються через IP-мережі. Ці експерименти виявили суттєві недоліки в

безпеці, що дозволяють зловмисникам отримувати конфіденційну інформацію про абонентів, маніпулювати сигнальним трафіком та здійснювати атаки, спрямовані на перехоплення або фальсифікацію комунікацій.

В умовах таких виявлених загроз, четвертий розділ цієї роботи присвячений детальному аналізу та порівнянню розроблених рекомендацій та передових практик у сфері безпеки SS7/SIGTRAN. Основна увага буде зосереджена на настанові GSMA FS.11 "SS7 Interconnect Security Monitoring and Firewall Guidelines", яка є ключовим документом для операторів мобільного зв'язку у питанні захисту їхніх сигнальних мереж. Буде розглянуто, як класифікуються різні типи атак згідно з цією настановою, та порівняно виявлені в Розділі 3 вразливості з визначеними категоріями GSMA. Крім того, буде надано конкретні рекомендації щодо запобігання кожній з детально описаних атак, спираючись на найкращі галузеві практики та принципи побудови безпечних сигнальних мереж. Метою цього розділу є не тільки підтвердження відповідності виявлених проблем існуючим стандартам безпеки, але й надання практичних кроків для їх усунення, підвищення загального рівня захисту SS7/SIGTRAN інфраструктур.

4.1 Категорії атак GSMA FS.11

GSMA FS.11 (SS7 Interconnect Security Monitoring and Firewall Guidelines) [26] поділяє SS7 атаки на три основні категорії, базуючись на очікуваному місці походження та характері сигнального трафіку:

Категорія 1 – Prohibited Interconnect Packets (Заборонені пакети міжмережевого з'єднання).

До цієї категорії належать повідомлення, які в принципі не повинні надходити через міжмережеві з'єднання (інтерконекти) від інших операторів. Це трафік, який зазвичай є внутрішнім для мережі оператора або вимагає попередньої двосторонньої угоди для передачі між мережами. Отримання таких

пакетів через інтерконект майже завжди свідчить про спробу атаки або неправильну конфігурацію.

Зазвичай це трафік, що призначений для внутрішніх елементів мережі, або запити, які не мають сенсу з точки зору міжмережевої взаємодії. [26]

Категорія 2 – Unauthorised Packets (Несанкціоновані пакети).

Ця категорія включає повідомлення, які можуть бути легітимними в певних сценаріях роумінгу, але є несанкціонованими, якщо надходять не від домашньої мережі абонента, який перебуває в роумінгу (inbound roamer). Тобто, якщо абонент А перебуває в мережі В, його домашня мережа А може надсилати певні запити до мережі В. Однак, якщо такі ж запити надходять з іншої мережі С, це вважається несанкціонованим.

Повідомлення, що стосуються абонентів, які не перебувають у роумінгу, або ж повідомлення, які надходять не з домашньої мережі абонента, що в роумінгу. [26]

Категорія 3 – Suspicious Location Packets (Підозрілі пакети місцезнаходження).

До цієї категорії відносяться повідомлення, які можуть виглядати легітимними з точки зору протоколу, але їхній вміст або контекст (наприклад, невідповідність між реальною та заявленою локацією, або надмірна кількість запитів місцезнаходження для одного абонента) вказує на підозрілу активність. Ці атаки часто спрямовані на відстеження місцезнаходження абонента або обхід існуючих захисних механізмів. GSMA зазначає, що це категорія, яка вимагає постійного моніторингу та адаптації захисту, оскільки атакуючі постійно вдосконалюють свої методи.

Постійні запити на оновлення місцезнаходження, невідповідності між базовою станцією та країною абонента. [26]

4.2 Рекомендації

Network IP Enumeration Test (Мережеве перерахування)

Категорія за GSMA FS.11: Категорія 1 – Prohibited Interconnect Packets.

Хоча сам процес "перерахування" IP-адрес і портів (використання Nmap) може не бути безпосередньо MAP/CAMEL пакетом, він є попереднім етапом і не повинен бути можливим ззовні мережі без відповідних дозволів або доступу до приватного IP-пулу. Якщо зловмисник отримує доступ до того ж TCP/IP пулу, що й SIGTRAN вузли, це вже є порушенням безпеки на нижчому рівні (IP), яке дозволяє подальші "заборонені" запити. Отримання IP-адрес та відкритих портів SIGTRAN-вузлів, які зазвичай є внутрішньою конфіденційною інформацією, через зовнішній інтерконект (або несанкціонований доступ до внутрішнього IP-сегмента) вважається діяльністю, яка не повинна відбуватися. Це підготовка до атак, які потім можуть включати пакети Категорії 1, якщо вони націлені на внутрішні елементи.

Рекомендації для запобігання:

- Сегментація мережі: Ізолювати SIGTRAN-вузли та іншу критичну сигнальну інфраструктуру в окремі, суворо сегментовані підмережі.
- Міжмережеві екрани (Firewalls) на IP-рівні: Впровадити строгі правила міжмережевого екранування, які дозволяють доступ до SIGTRAN-вузлів лише з довірених IP-адрес та лише до необхідних портів. Блокувати будь-які спроби сканування портів або перерахування IP-адрес з неавторизованих джерел.

- IDS/IPS системи: Розгорнути системи виявлення/запобігання вторгнень (IDS/IPS), які можуть виявляти та блокувати аномальну активність, таку як сканування портів або незвичайний трафік на SIGTRAN-портах.
- Моніторинг мережі: Постійний моніторинг мережевого трафіку для виявлення несанкціонованих спроб доступу або сканування.

Any Time Interrogation (ATI) Attack Test

Категорія за GSMA FS.11: Категорія 2 – Unauthorised Packets.

Запит anyTimeInterrogation використовується HLR для запиту інформації про абонента, який може перебувати в роумінгу. Згідно з FS.11, такі пакети можуть бути легітимними, якщо вони надходять від домашньої мережі абонента, який перебуває в роумінгу. Однак, якщо зловмисник надсилає такий запит, не будучи домашньою мережею абонента (або не маючи на це дозволу), це є "несанкціонованим пакетом". Важливо, що зловмисник тут (в експерименті 3.2) не маскується під домашню мережу абонента, а просто ініціює запит до HLR.

Рекомендації для запобігання:

- SS7/SIGTRAN Firewall: Впровадження спеціалізованих SS7/SIGTRAN міжмережових екранів на межі мережі.
- Фільтрація на основі ідентифікаторів: Блокувати MAP/CAMEL повідомлення (зокрема anyTimeInterrogation), якщо їхній Originating Point Code (OPC)/Global Title (GT) не відповідає довіреним роумінг-партнерам або не є домашньою мережею для абонента, до якого надсилається запит.
- Перевірка контексту: Аналізувати контекст запиту. Наприклад, якщо запит ATI приходить для абонента, який, за даними HLR, не перебуває в роумінгу, або надходить від мережі, яка не повинна запитувати інформацію про цього абонента.
- Rate Limiting: Обмеження кількості запитів anyTimeInterrogation від одного джерела або на одного абонента за певний проміжок часу для запобігання флуд-атак або широкого сканування.

IMSI Catch Attack Test

Категорія за GSMA FS.11: Категорія 2 – Unauthorised Packets.

Атака IMSI Catch передбачає, що зловмисник видає себе за SMSC, щоб отримати IMSI абонента за допомогою запиту sendIMSI. Запит sendIMSI є легітимним MAP-повідомленням, яке використовується для маршрутизації SMS. Однак, якщо такий запит ініціюється з неавторизованого джерела (фальшивого SMSC), це є "несанкціонованим пакетом", оскільки відправник не має права запитувати IMSI абонента.

Рекомендації для запобігання:

- SS7/SIGTRAN Firewall з розширеним функціоналом: Фільтрація повідомлень sendIMSI. Перевіряти, чи Calling Party Address (SCCP Global Title або Point Code) відповідає дійсному SMSC або іншому авторизованому елементу мережі, який має право ініціювати такий запит.
- Перевірка джерела запиту: Впровадити строгі правила, які перевіряють легітимність джерела запиту sendIMSI. Запит повинен надходити лише від перевірених і авторизованих SMSC або елементів, які дійсно потребують IMSI для своєї функціональності.

Provide Subscriber Info Attack Test

Категорія за GSMA FS.11: Категорія 2 – Unauthorised Packets.

В цій атаці зловмисник видає себе за HLR і надсилає повідомлення MAP-Provide-Subscriber-Info (PSI) Request безпосередньо до MSC/VLR. Хоча HLR може надсилати такі запити до MSC/VLR, атакуючий є "фальшивим HLR". Відправлення такого запиту від несанкціонованої сутності, яка не є легітимним HLR для цього абонента, робить пакет "несанкціонованим".

Рекомендації для запобігання:

- SS7/SIGTRAN Firewall з глибоким аналізом: Фільтрувати повідомлення provideSubscriberInfo. Перевіряти, чи Calling Party Address (SCCP Global Title або Point Code) відповідає дійсному HLR, що обслуговує абонента.

- Валідація джерела запиту: Впровадити суворі правила валідації для provideSubscriberInfo запитів, перевіряючи, чи запит надходить від авторизованого HLR, яке дійсно має стосунок до абонента, чії дані запитуються.
- Виявлення підміни HLR: Розгорнути системи, які можуть виявляти підміну мережевих елементів, аналізуючи аномалії в поведінці або сигнальному трафіку.

Update Location (MITM) Attack Test

Категорія за GSMA FS.11: Категорія 3 – Suspicious Location Packets.

Атака "Update Location" (MITM) є класичним прикладом атаки Категорії 3. Хоча повідомлення Update Location є легітимним з точки зору протоколу (використовується, коли абонент переміщується до нового MSC/VLR), його ініціація зловмисником з метою перехоплення трафіку або видачі себе за легітимний MSC/VLR є "підозрілою" активністю, що не відповідає звичайній поведінці мережі. Ці атаки важче виявити, оскільки вони використовують легітимні сигнальні потоки, але з несанкціонованою метою.

Рекомендації для запобігання:

- SS7/SIGTRAN Firewall з розширеним контролем стану: Використання міжмережевих екранів, які здатні відстежувати стан (stateful firewall) SS7/SIGTRAN сесій. Це дозволяє виявляти аномалії в послідовностях повідомлень Update Location.
- Поведінковий аналіз: Запровадити системи моніторингу, які аналізують поведінку сигнального трафіку. Виявлення надмірної кількості запитів Update Location для одного абонента, або запитів від невідомих/нелегітимних MSC/VLR, може свідчити про атаку.
- Порівняння даних про місцезнаходження: Порівняння інформації про місцезнаходження, що надходить з сигнального трафіку, з даними з інших джерел (наприклад, з географічних баз даних або внутрішніх систем моніторингу).

- Фільтрація за GT/PC: Блокувати Update Location запити від MSC/VLR, які не належать до відомих роумінг-партнерів або не мають підтвердженої ідентичності.

SMS Spoofing (Phishing SMS) Attack Test

Категорія за GSMA FS.11: Категорія 2 – Unauthorised Packets.

Атака "SMS Spoofing" полягає у підробці ідентифікатора відправника SMS (TP-Originating-Address). Хоча повідомлення forwardSM є легітимним для доставки SMS, його відправлення від імені неіснуючого або неавторизованого відправника, який не має права надсилати повідомлення з цим ідентифікатором, робить цей пакет "несанкціонованим". Атакуючий не є легітимним відправником для цього SMS, навіть якщо протокольно повідомлення коректне.

Рекомендації для запобігання:

- SMS Firewall: Впровадження спеціалізованих SMS-міжмережевих екранів, які перевіряють поле TP-Originating-Address на відповідність дійсним абонентам/номерам або коротким кодам.
- Home Routing: Забезпечення того, що весь SMS-трафік (особливо A2P - Application-to-Person) проходить через домашню мережу абонента, що дозволяє контролювати джерела SMS.
- Фільтрація "сірих маршрутів" (Grey Routes): Виявлення та блокування SMS-трафіку, що надходить через неавторизовані маршрути, які часто використовуються для спуфінгу та спаму.
- Перевірка на наявність маніпуляцій: Аналіз заголовків SMS-повідомлень та їх вмісту на предмет невідповідностей або підозрілих URL-адрес, характерних для фішингу.

Висновки до розділу 4

У розділ 4 цієї роботи здійснено детальний аналіз виявлених в попередньому розділі вразливостей SS7/SIGTRAN мереж у контексті загальновизнаних галузевих стандартів безпеки, зокрема, настанов GSMA FS.11. Систематизація атак за категоріями "Prohibited Interconnect Packets", "Unauthorised Packets" та "Suspicious Location Packets" дозволила не лише підтвердити актуальність виявлених проблем, але й визначити їхнє місце у глобальному ландшафті загроз SS7.

Кожна з проведених в експериментах атак — від мережевого перерахування IP-адрес та портів до складних атак "Any Time Interrogation", "IMSI Catch", "Provide Subscriber Info", "Update Location (MITM)" та "SMS Spoofing" — була чітко віднесена до однієї з категорій GSMA FS.11. Це підтверджує, що виявлені вразливості є добре відомими та класифікованими загрозами в телекомунікаційній галузі, що підкреслює їхню критичність та необхідність впровадження захисних механізмів.

Факт успішної реалізації усіх вищезазначених атак в симульованому середовищі свідчить про те, що, незважаючи на наявність галузевих рекомендацій, їхнє повне або ефективне впровадження не завжди забезпечується на практиці, або існують прогалини, які дозволяють обходити поточні захисні заходи. Зокрема, атаки, віднесені до Категорії 2 та 3, вимагають більш глибокого аналізу та контекстної фільтрації, ніж прості правила блокування.

Аналіз показав, що ключовим компонентом для запобігання більшості з описаних атак є належне налаштування та функціонування спеціалізованих SS7/SIGTRAN міжмережевих екранів. Ці екрани повинні не лише фільтрувати трафік за базовими параметрами (OPC/DPC, GT), але й здійснювати глибокий аналіз сигнальних повідомлень (MAP/CAMEL), їхнього контексту та поведінки джерела, щоб виявляти несанкціоновані та підозрілі запити.

Для ефективного захисту від усього спектру виявлених загроз необхідний комплексний підхід, що включає:

- Строгу сегментацію мережі на IP-рівні для ізоляції критичних компонентів.
- Впровадження IDS/IPS систем для виявлення аномальної активності та сканування.
- Поведінковий моніторинг та аналіз логів для виявлення підозрілих патернів трафіку.
- Регулярне оновлення та перевірка конфігурацій всіх мережевих елементів та систем безпеки.
- Застосування принципів "нульової довіри" до трафіку, що надходить ззовні мережі.

Підсумовуючи, цей розділ не лише підтвердив теоретичні та практичні результати Розділу 3, класифікуючи їх відповідно до міжнародних стандартів, але й надав чіткі та практичні рекомендації для усунення виявлених вразливостей. Ефективне впровадження цих заходів є обов'язковим для захисту конфіденційності абонентів, цілісності сигнальних мереж та безперебійності надання телекомунікаційних послуг в умовах зростаючих загроз з боку кіберзлочинності.

ВИСНОВКИ

Ця дипломна робота була присвячена дослідженню вразливостей сигнальних мереж SS7, що транспортуються через IP-інфраструктуру за допомогою протоколів SIGTRAN, та розробці рекомендацій щодо їх запобігання. Проведені експерименти та їх аналіз дозволили отримати низку ключових висновків.

Конвергенція IP та SS7 створює нові вектори атак: Використання IP-мереж для передачі сигнального трафіку SS7, хоч і підвищує ефективність та гнучкість мережі, одночасно відкриває її для широкого спектру кібератак, характерних для IP-мереж, на додаток до специфічних SS7-вразливостей.

Підтверджено можливість збору конфіденційної мережевої інформації: Експерименти з "Network IP Enumeration" переконливо продемонстрували, що зломисники можуть легко виявляти внутрішні IP-адреси та відкриті порти критичних SIGTRAN-вузлів, що є першим і фундаментальним кроком для планування подальших атак.

Виявлено значні вразливості у конфіденційності абонентських даних:

- Атаки "Any Time Interrogation" та "Provide Subscriber Info" успішно показали, що знання лише номера телефону абонента дозволяє зломиснику отримати його точне місцезнаходження та іншу конфіденційну інформацію (Cell ID, MCC, MNC, LAC).
- Атака "IMSI Catch" підтвердила можливість несанкціонованого отримання унікального ідентифікатора IMSI абонента, що є критично важливою інформацією для подальших, більш таргетованих атак.

Доведено можливість компрометації комунікацій та послуг:

- Атака "Update Location (MITM)" наочно продемонструвала здатність зломисника перехоплювати та маніпулювати вхідними дзвінками та

SMS-повідомленнями для жертви, ефективно здійснюючи "людину посередині" між абонентом та його домашньою мережею.

- Атака "SMS Spoofing" підтвердила можливість підробки ідентифікатора відправника SMS, що створює широкі можливості для реалізації фішингових кампаній, шахрайства та компрометації користувачів.

Наявні галузеві рекомендації є необхідними, але їхнє впровадження вимагає посилення. Проведений аналіз атак у контексті настанов GSMA FS.11 показав, що виявлені вразливості відповідають визначеним категоріям (Prohibited Interconnect Packets, Unauthorised Packets, Suspicious Location Packets). Це свідчить про обізнаність галузі з цими загрозами, а успіх експериментів вказує на важливість застосування рекомендованих захисних механізмів на практиці. Нещодавні дослідження підтверджують що наразі розгорнутих безпекових рішень не вистачає для зменшення кількості кібератак, зокрема із малорозвинених частин світу [27].

Основний висновок полягає в тому, що ефективний захист вимагає не просто наявності міжмережевого екрану, а його належного налаштування з глибоким аналізом сигнального трафіку, поведінковим моніторингом, фільтрацією на основі контексту та джерела, а також інтеграції з іншими системами безпеки (IDS/IPS, сегментація мережі).

Усі отримані результати підкреслюють, що поточний рівень безпеки SS7 сигналізації через IP-мережі є недостатнім, що створює значні ризики для конфіденційності абонентів, цілісності мереж та безперервності надання послуг.

Рекомендації для подальшої роботи

На основі проведеного дослідження та виявлених вразливостей, можна сформулювати наступні рекомендації для подальших наукових та практичних робіт:

Розробка та тестування інтелектуальних систем виявлення аномалій на основі машинного навчання. Замість статичних правил фільтрації, які можна

обійти, доцільно дослідити застосування алгоритмів машинного навчання для аналізу поведінки сигнального трафіку. Такі системи могли б виявляти навіть нові, невідомі раніше атаки, що мають аномальні патерни.

Дослідження та розробка проактивних методів протидії. Зосередитися на механізмах, які не лише виявляють та блокують атаки, але й можуть автоматично реагувати на них, наприклад, ізолюючи скомпрометовані вузли або сповіщаючи про них інші мережеві елементи.

Аналіз вразливостей інших сигнальних протоколів (Diameter, GTP): Оскільки мобільні мережі активно переходять на нові архітектури (4G/5G), важливо дослідити вразливості протоколів Diameter та GTP, які є основою цих мереж. Атаки на ці протоколи можуть мати ще більш руйнівні наслідки.

Вплив віртуалізації та хмарних технологій на безпеку сигнальних мереж: Зростаюча тенденція до віртуалізації мережевих функцій (NFV) та розгортання мережевих елементів у хмарних середовищах створює нові виклики для безпеки. Подальші дослідження могли б зосередитися на виявленні та усуненні потенційних вразливостей, що виникають у цих нових парадигмах розгортання.

Практичні випробування запропонованих рекомендацій на реальних (тестових) мережах: Перевірка ефективності запропонованих захисних механізмів не лише в симульованих умовах, а й на контрольованих тестових стендах реальних операторів для підтвердження їхньої ефективності та виявлення можливих проблем впровадження.

Ці напрямки подальших досліджень та розробок є критично важливими для забезпечення стійкості та безпеки глобальних телекомунікаційних мереж у майбутньому.

ПЕРЕЛІК ДЖЕРЕЛ ПОСИЛАНЬ

1. Klaus D. Gradischnig and Michael Tuxen, Signaling transport over IP-based networks using IETF standards, 2001.
2. Т. Євгеній, Л. Гальчинський - Collection of scientific papers «SCIENTIA» Вразливості конфігурацій мобільних мереж та методи їх пом'якшення, 2024
3. Patton Electronics Company - Introduction to SS7 Signaling, 2012
https://www.patton.com/whitepapers/intro_to_ss7_tutorial.pdf
4. Richard P. Martin - Signaling System 7 (IEC tutorial), 2004
<https://people.cs.rutgers.edu/~rmartin/teaching/fall04/cs552/readings/ss7.pdf>
5. Bob Kamwendo. - Vulnerabilities of signaling system number 7 (SS7) to cyber attacks and how to mitigate against these vulnerabilities. Johannesburg, August 25, 2015
6. ITU-T recommendation Q.706, Specifications of Signaling System No. 7. Message Transfer Part. Signaling Performance, 1996.
7. ITU-T recommendation Q.709, Specifications of Signaling System No. 7. Message Transfer Part. Hypothetical Signaling Reference Connection, Rev.1, 1993.
8. K. D. Gradischnig, St. Kramer, M. Tuxen, Loadsharing – A key to the reliability of SS7- networks, DRCN 2000.
9. Introduction to SS7 Signaling, Training Document Nokia Networks Oy, TC Finland. Issue Jan 2002.
https://www.academia.edu/9689313/Student_Introduction_to_SS7_Signalling
10. Ericsson Mobility Report November 2024
<https://www.ericsson.com/en/reports-and-papers/mobility-report/reports/november-2024>
11. User Data Protocol, Accessed November 2014 <http://www.faqs.org/rfcs/rfc768>
12. Transmission Control Protocol
https://en.wikipedia.org/wiki/Transmission_Control_Protocol
13. MIA IMMONEN – Signaling over IP — a step closer to an all-IP network, Master of Science Thesis Stockholm, Sweden 2005

<https://people.kth.se/~maguire/DEGREE-PROJECT-REPORTS/050619-Mia-Immonen-with-cover.pdf>

14. Paul Stalvig, Introduction to the Stream Control Transmission Protocol (SCTP): The next generation of the Transmission Control Protocol (TCP), Technical Marketing Manager F5 Networks Inc, Oct 2007.
<https://www.f5.com/pdf/white-papers/sctp-introduction-wp.pdf>
15. European Telecommunications Standards Institute,
<http://www.etsi.org/index.php/servirces/plugtests>
16. SCTP Download Page, <http://www.sctp.de/sctp-download.html>
17. Kame Project, <https://www.kame.net/project-overview.html>
18. Linux Kernel SCTP, <https://docs.kernel.org/networking/sctp.html>
19. OpenSS7, http://www.openss7.org/openss7_pkg.html
20. Dialogic, <https://www.voip-info.org/dialogic/>
21. SiGploit, Rosalia D'Alessandro, Telecom Italia,
<https://github.com/ethicalhackeragnidhra/SigPloit-ss7>
22. G. Lorenz, T. Moore, G. Manes, J. Hale, S. Shenoi, Securing SS7 Telecommunications Networks, 2001,
https://www.researchgate.net/publication/216757769_Securing_SS7_Telecommunications_Networks
23. Scanning SS7 Networks and Telecom Backbones
<http://ethicalhackernet.blogspot.com/2010/08/scanning-ss7-networks-and-telecom.html>
24. Wireshark, <https://www.wireshark.org/about>
25. Nmap, <https://nmap.org/book/man.html>
26. FS.11 SS7 Interconnect Security Monitoring and Firewall Guidelines
27. The Network Effect of Telecommunications Vulnerabilities for Location Disclosure, Gary Miller, Christopher Parsons, October 26 2023
<https://citizenlab.ca/2023/10/finding-you-teleco-vulnerabilities-for-location-disclosure/>

ДОДАТОК А

Скріншот захоплення Network enumeration

nmmap_scan_for_sctp.pcapng

Файл Правка Вигляд Перехід Захоплення Аналіз Статистика Телефонія Wireless Інструменти Довідка

sctp

No.	Time	Source	Destination	Protocol	Length	Info
3	0.0355742...	192.168.56.101	192.168.56.102	SCTP	66	INIT
4	0.0356378...	192.168.56.102	192.168.56.101	SCTP	298	INIT_ACK
5	0.0356624...	192.168.56.101	192.168.56.102	SCTP	50	ABORT
6	0.0356713...	192.168.56.101	192.168.56.102	SCTP	66	INIT
7	0.0356742...	192.168.56.102	192.168.56.101	SCTP	50	ABORT

< >

> Frame 3: 66 bytes on wire (528 bits), 66 bytes captured (528 bits) on interface lo, id 0
 > Ethernet II, Src: 00:00:00_00:00:00 (00:00:00:00:00:00), Dst: 00:00:00_00:00:00 (00:00:00:00:00:00)
 > Internet Protocol Version 4, Src: 192.168.56.101, Dst: 192.168.56.102
 > Stream Control Transmission Protocol, Src Port: 60638 (60638), Dst Port: 2906 (2906)

```

0000  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  .....E.
0010  00 34 c5 cd 00 00 2b 84 d7 5b c0 a8 38 66 c0 a8  -4...+...[...8f..
0020  38 66 ec de 0b 5a 00 00 00 00 19 9c c5 4e 01 00  8f...Z...N..
0030  00 14 b0 e0 a5 68 00 00 80 00 00 0a 08 00 cc 8d  ....h.....
0040  a2 18  ..
  
```

Stream Control Transmission Protocol: Protocol | Packets: 7 · Displayed: 5 (71.4%) | Profile: Default

ДОДАТОК Б

Скріншот захоплення IMSI Catch

IMSI_Catch.pcapng

Файл Правка Вигляд Перехід Захоплення Аналіз Статистика Телефонія Wireless Інструменти Довідка

Apply a display filter ... <Ctrl-/>

No.	Time	Source	Destination	Protocol	Length	Info
1	0.00000...	192.168.58.2	192.168.58.3	SCTP	82	INIT
2	0.00001...	192.168.58.3	192.168.58.2	SCTP	306	INIT_ACK
3	0.00002...	192.168.58.2	192.168.58.3	SCTP	278	COOKIE_ECHO
4	0.00005...	192.168.58.3	192.168.58.2	SCTP	50	COOKIE_ACK
5	0.00659...	192.168.58.2	192.168.58.3	M3UA (RFC 4666)	78	ASPUP
6	0.00661...	192.168.58.3	192.168.58.2	SCTP	62	SACK (Ack=0, Arwnd=106480)
7	0.00800...	192.168.58.3	192.168.58.2	M3UA (RFC 4666)	78	ASPUP_ACK
8	0.00802...	192.168.58.2	192.168.58.3	SCTP	62	SACK (Ack=0, Arwnd=106480)
9	0.00917...	192.168.58.2	192.168.58.3	M3UA (RFC 4666)	86	ASPAC
10	0.01037...	192.168.58.3	192.168.58.2	M3UA (RFC 4666)	102	SACK (Ack=1, Arwnd=106496) ASPAC_ACK
11	0.21429...	192.168.58.2	192.168.58.3	SCTP	62	SACK (Ack=1, Arwnd=106496)
12	9.59159...	1	2	GSM MAP	186	invoke sendIMSI
13	9.70205...	2	1	GSM MAP	222	SACK (Ack=2, Arwnd=106496) returnResultLast sendIMSI
14	9.90631...	192.168.58.2	192.168.58.3	SCTP	62	SACK (Ack=2, Arwnd=106496)
15	10.0454...	192.168.58.2	192.168.58.3	SCTP	54	SHUTDOWN
16	10.0454...	192.168.58.3	192.168.58.2	SCTP	50	SHUTDOWN_ACK
17	10.0454...	192.168.58.2	192.168.58.3	SCTP	50	SHUTDOWN_COMPLETE

▼ Signalling Connection Control Part

Message Type: Unitdata (0x09)

.... 0001 = Class: 0x1

0000 = Message handling: No special options (0x0)

Pointer to first Mandatory Variable parameter: 3

Pointer to second Mandatory Variable parameter: 16

Pointer to third Mandatory Variable parameter: 27

> Called Party address (13 bytes)

▼ Calling Party address (11 bytes)

> Address Indicator

SubSystem Number: HLR (Home Location Register) (6)

[Linked to TCAP, TCAP SSN linked to GSM_MAP]

▼ Global Title 0x4 (9 bytes)

Translation Type: 0x00 (0)

0001 = Numbering Plan: ISDN/telephony (0x1)

.... 0010 = Encoding Scheme: BCD, even number of digits (0x2)

.000 0100 = Nature of Address Indicator: International number (0x04)

> Calling Party Digits: 201500000000

> Transaction Capabilities Application Part

▼ GSM Mobile Application

▼ Component: returnResultLast (2)

▼ returnResultLast

invokeID: 0

▼ resultretres

> opCode: localValue (0)

IMSI: 609156789123456

> [Association IMSI: 609156789123456]

```

0000 00 00 00 00 00 00 00 00 08 00 45 02  ....E-
0010 00 d0 00 00 40 00 40 84 44 52 c0 a8 3a 03 c0 a8  ....@- DR-:
0020 3a 02 0b 55 0b 59 53 2b 3e 6f 00 00 00 00 03 00  :..U-YS+ >o-
0030 00 10 5b 1f 26 03 00 01 a0 00 00 00 00 00 00 03  ..[.&-
0040 00 a0 a0 14 1c d3 00 02 00 00 00 00 00 03 01 00  .....
0050 01 01 00 00 00 90 00 06 00 08 00 00 00 64 02 10  .....d-

```

International mobile subscriber identity (IMSI) (e212.imsi), 8 byte(s) | Packets: 18 - Displayed: 18 (100.0%) | Profile: Default

ДОДАТОК В

Скріншот захоплення Any Time Interrogation

AnyTimeInterrogation_cat_1.pcapng

Файл Правка Вигляд Перехід Захоплення Аналіз Статистика Телефонія Wireless Інструменти Довідка

Apply a display filter ... <Ctrl-/>

No.	Time	Source	Destination	Protocol	Length	Info
6	175.964...	192.168.56.101	192.168.56.102	SCTP	82	INIT
7	175.964...	192.168.56.102	192.168.56.101	SCTP	306	INIT_ACK
8	175.964...	192.168.56.101	192.168.56.102	SCTP	278	COOKIE_ECHO
9	175.964...	192.168.56.102	192.168.56.101	SCTP	50	COOKIE_ACK
10	175.985...	192.168.56.101	192.168.56.102	M3UA (RFC 4666)	78	ASPUP
11	175.985...	192.168.56.102	192.168.56.101	SCTP	62	SACK (Ack=0, Arwnd=106480)
12	175.987...	192.168.56.102	192.168.56.101	M3UA (RFC 4666)	78	ASPUP_ACK
13	175.987...	192.168.56.101	192.168.56.102	SCTP	62	SACK (Ack=0, Arwnd=106480)
14	175.990...	192.168.56.101	192.168.56.102	M3UA (RFC 4666)	86	ASPAC
15	175.992...	192.168.56.102	192.168.56.101	M3UA (RFC 4666)	102	SACK (Ack=1, Arwnd=106496) ASPAC_ACK
16	176.193...	192.168.56.101	192.168.56.102	SCTP	62	SACK (Ack=1, Arwnd=106496)
17	185.657...	1	2	GSM MAP	210	invoke anyTimeInterrogation
18	185.773...	2	1	GSM MAP	294	SACK (Ack=2, Arwnd=106496) returnResultLast anyTimeIr
19	185.977...	192.168.56.101	192.168.56.102	SCTP	62	SACK (Ack=2, Arwnd=106496)
20	196.174...	192.168.56.101	192.168.56.102	SCTP	54	SHUTDOWN
21	196.174...	192.168.56.102	192.168.56.101	SCTP	50	SHUTDOWN_ACK
22	196.174...	192.168.56.101	192.168.56.102	SCTP	50	SHUTDOWN_COMPLETE

> Frame 18: 294 bytes on wire (2352 bits), 294 bytes captured (2352 bits) on interface lo, id 0

> Ethernet II, Src: 00:00:00_00:00:00 (00:00:00:00:00:00), Dst: 00:00:00_00:00:00 (00:00:00:00:00:00)

> Internet Protocol Version 4, Src: 192.168.56.102, Dst: 192.168.56.101

> Stream Control Transmission Protocol, Src Port: 2906 (2906), Dst Port: 2905 (2905)

> MTP 3 User Adaptation Layer

> Signalling Connection Control Part

> Transaction Capabilities Application Part

> GSM Mobile Application

> Component: returnResultLast (2)

> returnResultLast

> invokeID: 0

> resultretres

> opCode: localValue (0)

> subscriberInfo

> locationInformation

> ageOfLocationInformation: 30

> geographicalInformation: 10296de816715207

> 0001 = Location estimate: Ellipsoid point with uncertainty Circle (1)

> 0... = Sign of latitude: North (0)

> .010 1001 0110 1101 1110 1000 = Degrees of latitude: 2715112 (29,13000 degrees)

> 0001 0110 0111 0001 0101 0010 = Degrees of longitude: 1470802 (31,55999 degrees)

> .000 0111 = Uncertainty code: 7 (9,5 m)

> [Location OSM URI: <https://www.openstreetmap.org/?mlat=29,13000&mlon=31,55999&zoom=12>]

> vlr-number: 91025115428521f3

> cellGlobalIdOrServiceAreaIdOrLAI: cellGlobalIdOrServiceAreaIdFixedLength (0)

> currentLocationRetrieved

> subscriberState: assumedIdle (0)

> locationInformationGPRS

> imei: 53029900711684

resultretres (gsm_old.resultretres_element), 86 byte(s)

Packets: 22 · Displayed: 22 (100.0%)

Profile: Default

ДОДАТОК Г

Скріншот захоплення Provide Subscription Info

ProvideSubscriberInfo.pcapng

Файл Правка Вигляд Перехід Захоплення Аналіз Статистика Телефонія Wireless Інструменти Довідка

Apply a display filter ... <Ctrl-/>

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000...	192.168.56.101	192.168.56.102	SCTP	82	INIT
2	0.0000160...	192.168.56.102	192.168.56.101	SCTP	306	INIT_ACK
3	0.0000251...	192.168.56.101	192.168.56.102	SCTP	278	COOKIE_ECHO
4	0.0000504...	192.168.56.102	192.168.56.101	SCTP	50	COOKIE_ACK
5	0.0051004...	192.168.56.101	192.168.56.102	M3UA (...)	78	ASPUP
6	0.0051254...	192.168.56.102	192.168.56.101	SCTP	62	SACK (Ack=0, Arwnd=106480)
7	0.0063701...	192.168.56.102	192.168.56.101	M3UA (...)	78	ASPUP_ACK
8	0.0063935...	192.168.56.101	192.168.56.102	SCTP	62	SACK (Ack=0, Arwnd=106480)
9	0.0075244...	192.168.56.101	192.168.56.102	M3UA (...)	86	ASPAC
10	0.0086853...	192.168.56.102	192.168.56.101	M3UA (...)	102	SACK (Ack=1, Arwnd=106496) ASPAC_ACK
11	0.2111991...	192.168.56.101	192.168.56.102	SCTP	62	SACK (Ack=1, Arwnd=106496)
12	16.161687...	1	2	GSM MAP	202	invoke provideSubscriberInfo
13	16.209109...	2	1	GSM MAP	302	SACK (Ack=2, Arwnd=106496) returnResultLast provideSubscriberInfo
14	16.411246...	192.168.56.101	192.168.56.102	SCTP	62	SACK (Ack=2, Arwnd=106496)
15	26.557293...	192.168.56.101	192.168.56.102	SCTP	54	SHUTDOWN
16	26.557318...	192.168.56.102	192.168.56.101	SCTP	50	SHUTDOWN_ACK
17	26.557322...	192.168.56.101	192.168.56.102	SCTP	50	SHUTDOWN_COMPLETE

▼ GSM Mobile Application

▼ Component: returnResultLast (2)

▼ returnResultLast

invokeID: 0

▼ resultretres

opCode: localValue (0)

▼ subscriberInfo

locationInformation

subscriberState: assumedIdle (0)

locationInformationGPRS

routeingAreaIdentity: 062003402d21

geographicalInformation: 1027fba11728d202

sgsn-Number: 91025155555f5

currentLocationRetrieved

ageOfLocationInformation: 30

imei: 53029900711684

00f0 85 21 f3 a3 09 80 07 06 f2 30 04 d2 16 2e a1 02 .!.....0...
 0100 80 00 a3 20 81 06 06 20 03 40 2d 21 82 08 10 27@-!...
 0110 fb a1 17 28 d2 02 83 07 91 02 51 55 55 f5 88 ...(-...QUUU..
 0120 00 89 01 1e 85 07 53 02 99 00 71 16 84 00 S...q...

geographicalInformation (gsm_map.ms.geographicalInformation), 8 byte(s) | Packets: 21 · Displayed: 21 (100.0%) | Profile: Default

ДОДАТОК Д

Скріншот захоплення MITM (Update Location)

updateLocation.pcapng

Файл Правка Вигляд Перехід Захоплення Аналіз Статистика Телефонія Wireless Інструменти Довідка

Apply a display filter ... <Ctrl-/>

No.	Time	Source	Destination	Protocol	Length	Info
1	0.00000...	192.168.56.101	192.168.56.102	SCTP	82	INIT
2	0.00001...	192.168.56.102	192.168.56.101	SCTP	306	INIT_ACK
3	0.00002...	192.168.56.101	192.168.56.102	SCTP	278	COOKIE_ECHO
4	0.00005...	192.168.56.102	192.168.56.101	SCTP	50	COOKIE_ACK
5	0.00373...	192.168.56.101	192.168.56.102	M3UA (RFC 4666)	78	ASPUP
6	0.00374...	192.168.56.102	192.168.56.101	SCTP	62	SACK (Ack=0, Arwnd=106480)
7	0.00573...	192.168.56.102	192.168.56.101	M3UA (RFC 4666)	78	ASPUP_ACK
8	0.00576...	192.168.56.101	192.168.56.102	SCTP	62	SACK (Ack=0, Arwnd=106480)
9	0.00695...	192.168.56.101	192.168.56.102	M3UA (RFC 4666)	86	ASPAC
10	0.00791...	192.168.56.102	192.168.56.101	M3UA (RFC 4666)	102	SACK (Ack=1, Arwnd=106496) ASPAC_ACK
11	0.21195...	192.168.56.101	192.168.56.102	SCTP	62	SACK (Ack=1, Arwnd=106496)
12	9.69052...	1	2	GSM MAP	206	invoke updateLocation
13	9.73540...	2	1	GSM MAP	238	SACK (Ack=2, Arwnd=106496) invoke insertSubscriberData
14	9.75713...	1	2	GSM MAP	218	SACK (Ack=2, Arwnd=106496) returnResultLast insertSubscriberData
15	9.77609...	2	1	GSM SMS	246	SACK (Ack=3, Arwnd=106496) invoke forwardSM
16	9.78737...	1	2	GSM SMS	246	SACK (Ack=3, Arwnd=106496) invoke forwardSM
17	9.99219...	192.168.56.102	192.168.56.101	SCTP	62	SACK (Ack=4, Arwnd=106496)
18	10.1224...	192.168.56.101	192.168.56.102	SCTP	54	SHUTDOWN
19	10.1224...	192.168.56.102	192.168.56.101	SCTP	50	SHUTDOWN_ACK
20	10.1224...	192.168.56.101	192.168.56.102	SCTP	50	SHUTDOWN_COMPLETE

> Ethernet II, Src: 00:00:00_00:00:00 (00:00:00:00:00:00), Dst: 00:00:00_00:00:00 (00:00:00:00:00:00)

> Internet Protocol Version 4, Src: 192.168.56.102, Dst: 192.168.56.101

> Stream Control Transmission Protocol, Src Port: 2906 (2906), Dst Port: 2905 (2905)

> MTP 3 User Adaptation Layer

> Signalling Connection Control Part

> Transaction Capabilities Application Part

> GSM Mobile Application

▼ GSM SMS TPDU (GSM 03.40) SMS-DELIVER

0... .. = TP-RP: TP Reply Path parameter is not set in this SMS SUBMIT/DELIVER

.0.. = TP-UDHI: The TP UD field contains only the short message

..0. = TP-SRI: A status report shall not be returned to the SME

... 0... = TP-LP: The message has not been forwarded and is not a spawned message

.... .1.. = TP-MMS: No more messages are waiting for the MS in this SC

.... ..00 = TP-MTI: SMS-DELIVER (0)

> TP-Originating-Address - (2010789123456)

> TP-PID: 0

> TP-DCS: 0

> TP-Service-Centre-Time-Stamp

TP-User-Data-Length: (12) depends on Data-Coding-Scheme

▼ TP-User-Data

SMS text: Hello World!

The text of the SMS (gsm_sms.sms_text), 11 byte(s)

Packets: 20 · Displayed: 20 (100.0%)

Profile: Default

ДОДАТОК Е

Скріншот захоплення SMS Spoofing

The screenshot displays a Wireshark interface with a packet capture of SMS Spoofing. The main packet list shows a sequence of SCTP and M3UA packets, followed by a GSM SMS packet (No. 12) which is an 'invoke forwardSM'. The packet details pane shows the structure of the GSM SMS, including TP-UDHI, TP-SRI, TP-LP, TP-MMS, and TP-MTI. The TP-UDHI field contains the text 'Please verify your password at http://facebuk.com'.

No.	Time	Source	Destination	Protocol	Length	Info
1	0.00000...	192.168.56.101	192.168.56.102	SCTP	82	INIT
2	0.00004...	192.168.56.102	192.168.56.101	SCTP	306	INIT_ACK
3	0.00007...	192.168.56.101	192.168.56.102	SCTP	278	COOKIE_ECHO
4	0.00012...	192.168.56.102	192.168.56.101	SCTP	50	COOKIE_ACK
5	0.00697...	192.168.56.101	192.168.56.102	M3UA (RFC 4666)	78	ASPUP
6	0.00699...	192.168.56.102	192.168.56.101	SCTP	62	SACK (Ack=0, Arwnd=106480)
7	0.00817...	192.168.56.102	192.168.56.101	M3UA (RFC 4666)	78	ASPUP_ACK
8	0.00820...	192.168.56.101	192.168.56.102	SCTP	62	SACK (Ack=0, Arwnd=106480)
9	0.01070...	192.168.56.101	192.168.56.102	M3UA (RFC 4666)	86	ASPAC
10	0.01202...	192.168.56.102	192.168.56.101	M3UA (RFC 4666)	102	SACK (Ack=1, Arwnd=106496) ASPAC_ACK
11	0.21374...	192.168.56.101	192.168.56.102	SCTP	62	SACK (Ack=1, Arwnd=106496)
12	13.6027...	1	2	GSM SMS	262	invoke forwardSM
13	13.8057...	192.168.56.102	192.168.56.101	SCTP	62	SACK (Ack=2, Arwnd=106496)
14	13.9719...	192.168.56.102	192.168.56.101	SCTP	54	SHUTDOWN
15	13.9719...	192.168.56.101	192.168.56.102	SCTP	50	SHUTDOWN_ACK
16	13.9720...	192.168.56.102	192.168.56.101	SCTP	50	SHUTDOWN_COMPLETE

GSM SMS TPDU (GSM 03.40) SMS-DELIVER

- 0... = TP-RP: TP Reply Path parameter is not set in this SMS SUBMIT/DELIVER
- .0.. = TP-UDHI: The TP UD field contains only the short message
- ..1. = TP-SRI: A status report shall be returned to the SME
- 0... = TP-LP: The message has not been forwarded and is not a spawned message
- 1.. = TP-MMS: No more messages are waiting for the MS in this SC
- 00 = TP-MTI: SMS-DELIVER (0)
- TP-Originating-Address - (Facebook)
 - Length: 14 address digits
 - 1... = Extension: No extension
 - .101 = Type of number: Alphanumeric (coded according to 3GPP TS 23.038 GSM 7-bit default alphabet) (5)
 - 0000 = Numbering plan: Unknown (0)
 - TP-OA Digits: Facebook
- TP-PID: 0
- TP-DCS: 0
- TP-Service-Centre-Time-Stamp
- TP-User-Data-Length: (49) depends on Data-Coding-Scheme
- TP-User-Data
 - SMS text: Please verify your password at http://facebuk.com

serviceCentreAddressOA (gsm_old.serviceCentreAddressOA), 7 byte(s) | Packets: 16 · Displayed: 16 (100.0%) | Profile: Default