МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
ДОНЕЦЬКИЙ НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ ІМЕНІ ВАСИЛЯ СТУСА

ЧУЙКО НІКІТА ВАЛЕРІЙОВИЧ

Допускається до захисту:
в. о. завідувача кафедри
прикладної математики та
кібербезпеки,
д – р філософії з математики,
_____ А.В.Луценко
«__»_____20__ р.

БЕЗПЕКА В МЕРЕЖАХ IP-ТЕЛЕФОНІЇ

Спеціальність 125 Кібербезпека

Кваліфікаційна (бакалаврська) робота

Керівник:
канд. техн. наук, доцент,
старший викладач кафедри прикладної
математики та кібербезпеки,
Чернов Д. В.

Оцінка:___/___/_____
(бали за шкалою ЄКТС/за національною шкалою)
Голова ЕК:_____
(підпис)

Вінниця - 2024

АНОТАЦІЯ

Чуйко Н.В. Безпека в мережах IP-телефонії. Спеціальність 125 «Кібербезпека». Донецький національний університет імені Василя Стуса, Вінниця, 2024. У кваліфікаційній (бакалаврській) роботі досліджено загрози в мережах IP-телефонії, зокрема прослуховування, DDoS-атаки та підробку ідентифікатору абонента. Проаналізовано методи захисту від цих загроз та обрано найефективніші з них для забезпечення безпеки в мережах IP-телефонії. Ключові слова: IP-телефонія, VoIP, кібербезпека, прослуховування, DDoS-атака, підробка ідентифікатора, захист. 52 с., 22 рис., 22 джерела.

ANNOTATION

Chuiko N.V. Security in IP Telephony Networks. Specialty 125 "Cybersecurity". Vasyl Stus Donetsk National University, Vinnytsia, 2024. The qualification (bachelor's) work investigates threats in IP telephony networks, including eavesdropping, DDoS attacks, and caller ID spoofing. Methods of protection against these threats are analyzed, and the most effective ones are selected to ensure security in IP telephony networks. Keywords: IP telephony, VoIP, cybersecurity, eavesdropping, DDoS attack, caller ID spoofing, protection. 52 pages, 22 figures, 22 sources.

ЗМІСТ

ПЕРЕЛІК СКОРОЧЕНЬ

IP - Internet Protocol

VoIP - Voice over IP

TCP - Transmission Control Protocol

GSM - Global System for Mobile Communications

GPRS - General Packet Radio Service

EDGE - Enhanced Data rates for GSM Evolution

CDMA - Code Division Multiple Access

EV-DO - Evolution-Data Optimized

WAP - Wireless Application Protocol

MNP - Mobile Number Portability

SIP - Session Initiation Protocol

UDP - User Datagram Protocol

OSI - Open Systems Interconnection

HTTP - Hypertext Transfer Protocol

RFC - Request for Comments

RTP - Real-time Transport Protocol

ITU - International Telecommunication Union

QoS - Quality of Service

RTCP - Real-Time Control Protocol

IETF - Internet Engineering Task Force

ISDN - Integrated Services Digital Network

RAS - Remote Access Service

SRTP - Secure Real-time Transport Protocol

WebRTC - Web Real-Time Communication

SDP - Session Description Protocol

MGCP - Media Gateway Control Protocol

SGCP - Simple Gateway Control Protocol

IPDC - Internet Protocol Datacasting

MGCP - Media Gateway Control Protocol

OpenSIPS - Open Session Initiation Protocol Server

TDM - Time-Division Multiplexing

DoS - Denial of Service

DDoS - Distributed Denial of Service

TLS - Transport Layer Security

IPsec - Internet Protocol Security

ZRTP – Zimmermann Real-time Transport Protocol

IPS - Intrusion Prevention System

IDS - Intrusion Detection System

MPLS - Multiprotocol Label Switching

VPN - Virtual Private Network

SIEM - Security Information and Event Management

CDN - Content Delivery Network

TACACS+ - Terminal Access Controller Access-Control System Plus

RADIUS - Remote Authentication Dial-In User Service

AAA - Authentication, Authorization, Accounting

ВСТУП

Актуальність теми дослідження

З поглибленням цифровізації суспільства та поширенням використання IP-телефонії зростає і ризик зловживання, кібератак та порушення конфіденційності. IP-телефонія, яка використовує Інтернет-протокол для передачі голосових даних, є важливою складовою сучасних комунікаційних систем. Однак, зростання популярності цієї технології привертає увагу кіберзлочинців, які можуть використовувати уразливості в системах для несанкціонованого доступу, прослуховування розмов або викрадення даних.

Таким чином, впровадження комплексного підходу до безпеки IP-телефонії є критично важливим для забезпечення надійності та безперебійності комунікаційних процесів в умовах сучасного цифрового світу.

Мета - проаналізувати основні загрози безпеці в мережах IP-телефонії, промоделювати їх та визначити ефективні засоби захисту для запобігання потенційним атакам.

Завдання дослідження:

1. Аналіз основних загроз безпеці в мережах IP-телефонії.
2. Моделювання сценаріїв можливих кібератак на мережі IP-телефонії.
3. Визначення методів виявлення потенційних загроз та вразливостей.
4. Розробка стратегій та технічних засобів для захисту мереж IP-телефонії від атак.

Об'єкт дослідження - мережі IP-телефонії, які використовуються для проведення голосових та інших комунікаційних послуг через інтернет.

Предмет дослідження - основні загрози безпеці мереж IP-телефонії

РОЗДІЛ 1. МЕРЕЖІ IP-ТЕЛЕФОНІЇ

1.1. Поняття IP-Телефонії та принцип її роботи

IP-телефонія - це технологія, що використовує мережі з комутацією пакетів на основі IP-протоколів для здійснення міжнародних, міжміських і місцевих дзвінків і факсів у режимі реального часу. Інакше кажучи, за наявності доступних інтернет-каналів дзвінок можна здійснити в будь-яку точку світу, де є телефон або доступ в інтернет. IP-телефонія - це набір традиційних телефонних дзвінків, викликів, двостороннього голосового та відеозв'язку через інтернет та інші IP-мережі. Вона належить до набору комунікаційних протоколів, технологій і методів, які забезпечують Сигнали передаються каналом зв'язку в цифровому вигляді та, зазвичай, перетворюються (стискаються) перед передачею з метою видалення надлишкової інформації та зниження навантаження на мережі передачі даних.

VoIP - це технологія обробки дзвінків через IP-мережу передачі даних, яка може бути інтернетом або власною мережею організації. Одна з головних переваг VoIP полягає в тому, що дзвінки обробляються мережею передачі даних швидше, ніж телефонною мережею компанії, що дає змогу скоротити витрати.

Принцип роботи можна пояснити наступним чином: коли один з абонентів посилає іншому мовний сигнал, мова обробляється кодеком і передається у вигляді пакетних даних через Інтернет у режимі реального часу (рис. 1.1). Максимальна затримка під час передачі голосу становить приблизно 300-400 мілісекунд, залежно від того, скільки часу потрібно обладнанню для створення цифрового голосового сигналу. Ви її не помітите, оскільки нині розроблено технології, які дають змогу мінімізувати втрати сигналу в мережі та уникнути зникнення звуку. У результаті вартість такої розмови обходиться набагато дешевше, ніж при використанні традиційних телекомунікацій. Для передачі сигналу потрібен спеціальний пристрій, який називається IP-шлюзом. Це пристрій для передавання даних із мережі одного типу в мережу іншого типу: IP-

шлюз (також званий IP-сервером) під'єднується до телефонної лінії та може бути з'єднаний із будь-яким телефоном у світі, при цьому він може спілкуватися з будь-яким комп'ютером, під'єднаним до Інтернету. Він також може взаємодіяти з будь-яким комп'ютером, підключеним до Інтернету [1].

Рисунок 1.1 – Принцип роботи IP-телефонії

Телефонний сигнал оцифровується, стискається, розбивається на пакети і надсилається до місця призначення по IP-мережі з використанням протоколу TCP/IP. Потім сигнал проходить через інший шлюз, де він знову перетворюється на телефонний сигнал, і абонент отримує дзвінок. Сьогодні доступ до Інтернету можна отримати безпосередньо з мобільних телефонів, що підтримують такі технології: GSM data, GPRS (General Packet Radio Service), EDGE (Enhanced Data rates for Global Evolution), CDMA (Code Division Multiple Access), EV-DO (Evolution-Data Optimised) та інші технології, які надають широкий спектр послуг мобільного інтернету та WAP [1].

У зв'язку з цим аудіосигнал з каналу VoIP може бути переданий безпосередньо на IP-телефони, підключені до IP-мереж, мобільні телефони компаній стільникового зв'язку або аналогові телефони, підключені до звичайних телефонних мереж.

Сумісність мобільного номера (MNP) також впливає на комерційне застосування IP-телефонії, іншими словами, VoIP. Голосові виклики, що надходять каналом зв'язку і направляються на мобільний телефон традиційного мобільного оператора, також стикаються з проблемою досягнення місця призначення, що у випадку з мобільними телефонами означає, що виклик (сигнал) повинен досягти порту. Сумісність мобільних номерів - послуга, що дає змогу користувачам зберігати наявний номер телефону під час переходу від одного оператора мобільного зв'язку до іншого.

Таким чином, IP-телефонія дає змогу передавати голосові сигнали з комп'ютера на комп'ютер, з комп'ютера на телефон і з телефона на телефон. Дзвінки здійснюються через провайдера послуг VoIP. Якість передачі голосу залежить від постачальника послуг VoIP і підключення до Інтернету.

1.2. Протоколи в IP-телефонії та їх взаємодія

Процедури обміну інформацією між різними мережевими пристроями визначаються набором стандартних протоколів, створених для вирішення проблем, що виникають час від часу. Ці протоколи також є елементами мультисервісних мереж.

Протокол ініціювання сеансу (SIP). Це протокол сигналізації, що використовується для встановлення "сеансу" між двома або більше учасниками, зміни цього сеансу і, нарешті, його завершення. Фактична передача даних здійснюється за допомогою протоколу управління передачею (TCP) або протоколу користувацьких дейтаграм (UDP) на п'ятому рівні моделі OSI (рис. 1.2) [1].

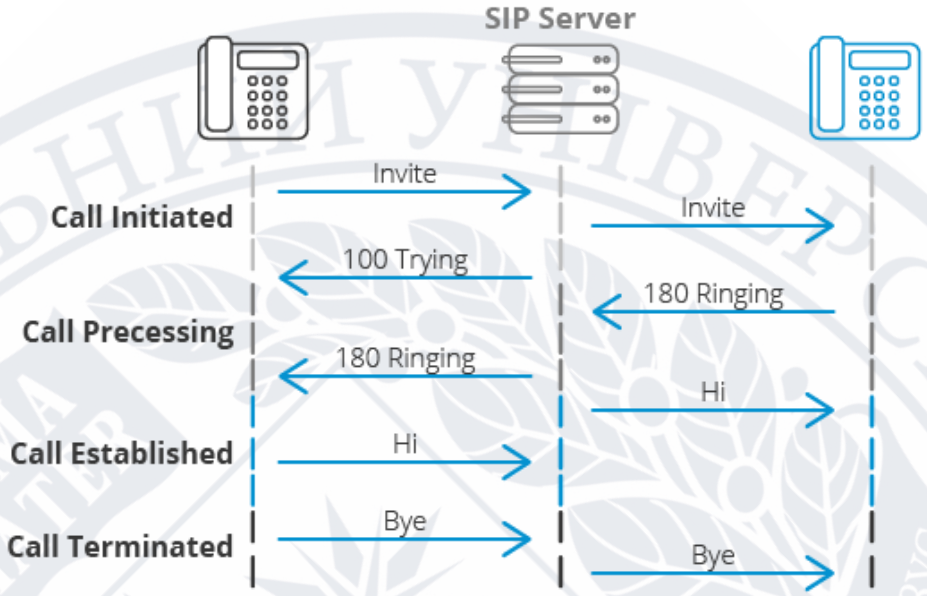


Рисунок 1.2 - Приклад ініціювання сеансу дзвінку між двома IP-телефонами

Цей протокол базується на текстах і дуже схожий на HTTP. І ці текстові повідомлення, разом з механізмом "запит-відповідь", полегшують пошук і усунення несправностей.

SIP-клієнти використовують TCP і UDP порти для зв'язку між сервером та іншими SIP-клієнтами. Протокол SIP в основному використовується для встановлення і роз'єднання голосових і відеодзвінків. Однак SIP також може використовуватися для інших додатків, які вимагають встановлення з'єднання, таких як підписка на події та сповіщення, мобільність терміналів тощо. Існує низка RFC, пов'язаних з SIP, які визначають поведінку таких додатків. Протокол RTP (Real-Time Transport Protocol) використовується для передачі аудіо- та відеоданих.

Основним і найважливішим завданням при розробці SIP було створення протоколу сигналізації та встановлення з'єднання, який міг би підтримувати розширений набір функцій обробки викликів для IP-зв'язку.

Сам протокол SIP не визначає ці функції і зосереджується лише на процедурах встановлення виклику та сигналізації. Протокол SIP був створений

для забезпечення функцій проксі-сервера та агента користувача. Таким чином, він може підтримувати необхідні телефонні операції (набір номера, прослуховування мелодії, дзвінок); реалізація цих функцій і термінологія, що використовується в SIP, відрізняється від традиційної телефонії, але поведінка для кінцевого користувача залишається такою ж.

Цей список також включає H.323, який має ту саму функціональність, що й SIP. Цей протокол також відповідає за запуск, зміну та завершення сеансів. H.323 - протокол у наборі стандартів ITU-T, який формує набір протоколів для забезпечення аудіо/візуального зв'язку комп'ютерними мережами (рис. 1.3). На практиці це двійковий протокол для передавання аудіо та відео мережею.

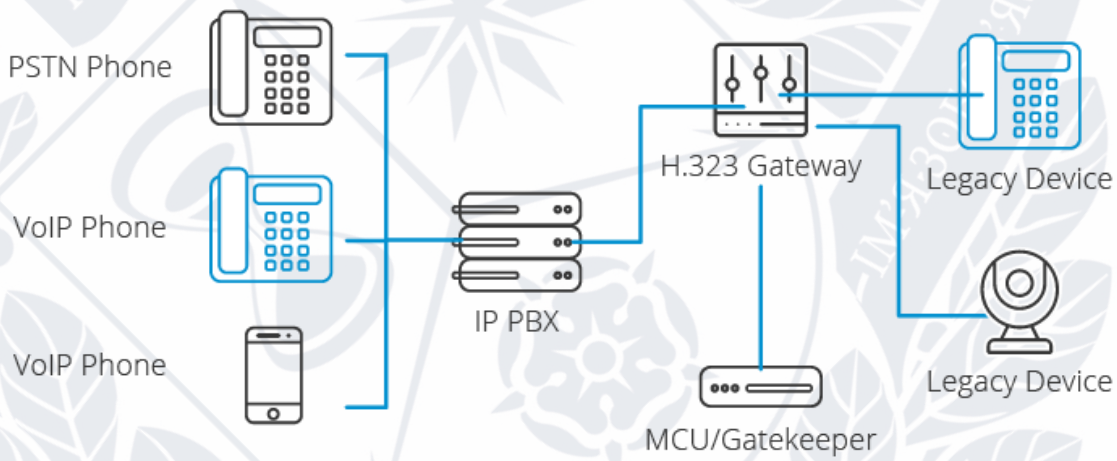


Рисунок 1.3 - Принцип роботи протоколу H.323

Стандарт ITU-T H.323 був розроблений для забезпечення налаштування викликів і передачі голосового та відеотрафіку через пакетні мережі, які не гарантують якість обслуговування (QoS), такі як Інтернет та Інтранет. Він використовує протокол RTP/RTCP (Real-Time Transport Protocol і Real-Time Transport Control Protocol), розроблений групою IETF, і серію стандартних кодеків ITU-T G.xxx.

Протокол H.323 був першим протоколом, який реалізував технологію VoIP, але під час активного розвитку IP-телефонії він почав витіснятися більш простим і масштабованим протоколом SIP, розробленим IETF. Проте ITU також

удосконалив цей протокол, збільшивши швидкість і масштабованість встановлення з'єднання. Мережі на основі H.323 призначені для інтеграції з мережами телефонії, що накладаються поверх мереж передачі даних. При встановленні з'єднання в таких мережах IP-телефонії використовуються процедури, засновані на рекомендації Q.931, аналогічні тим, що застосовуються в мережах ISDN [2].

Рекомендація H.323 являє собою доволі складний набір протоколів не тільки для передавання голосової інформації IP-мережами з комутацією пакетів; мета H.323 - забезпечити роботу мультимедійних додатків у мережах, де якість обслуговування не гарантується. Голосовий трафік є лише одним із додатків H.323, поряд із відео та даними. Тому потрібні значні зусилля для забезпечення сумісності H.323 з різними мультимедійними додатками. Наприклад, для реалізації функції переадресації викликів потрібна окрема специфікація H.450.2.

Принцип побудови мережі IP-телефонії, запропонований Міжнародним союзом електрозв'язку в рекомендації H.323, підходить для операторів місцевих телефонних мереж, зацікавлених у наданні послуг міжміського та міжнародного зв'язку з використанням мереж з комутацією пакетів (IP-мереж). H.323 - це сімейство протоколів, протокол RAS, що може контролювати використання мережевих ресурсів, підтримувати автентифікацію користувачів і забезпечувати виставлення рахунків за послуги.

RTP (Real-time Transport Protocol). Протокол RTP, визначений у RFC 1889, має стандартний формат пакетів для передачі аудіо/відео через Інтернет. Протокол широко використовується в комунікаційних і розважальних системах, що передбачають потокове передавання мультимедійних даних, включаючи телефонію, телевізійні сервіси, програми для проведення відеоконференцій і можливості push-to-talk в Інтернеті [2].

На практиці RTP працює у зв'язці з RTCP (Real Time Transport Protocol), в якій RTP передає медіапотоки, а RTCP відстежує статистику передавання (якість обслуговування, QoS) і допомагає встановити синхронізацію різних потоків; RTP походить із парних портів, а RTCP із верхніх непарних портів. (рис. 1.4)

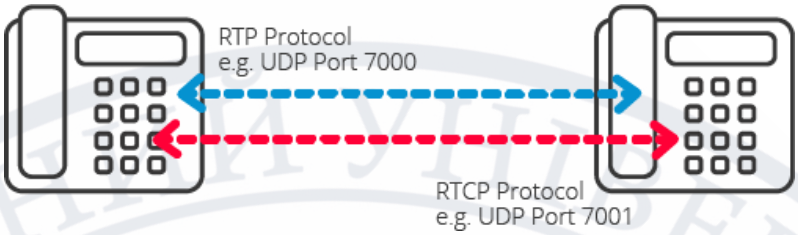


Рисунок 1.4 – Взаємодія протоколів RTP та RTCP

SRTP (Secure Real-time Transport Protocol). Це один з протоколів безпеки, що використовується в технології WebRTC, опублікований як RFC 3711 в 2004 році. Вперше був визначений у RFC 3550 і працює у зв'язці з RTP. Цей протокол відповідає за надсилання пакетів управління учасникам конкретного дзвінка (рис. 1.5). По суті, його основне завдання - забезпечити зворотний зв'язок QoS з RTP. RTCP надсилає інформацію та статистику, наприклад кількість пакетів, час передавання та приймання тощо. Деякі застосунки використовують ці дані для керування параметрами QoS, вибору використання певних кодеків тощо [2].

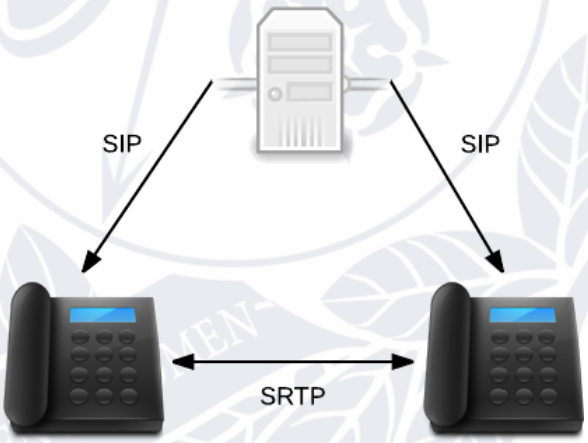


Рисунок 1.5 – Принцип роботи протоколу SRTP

Протокол опису сеансу (Session Description Protocol, SDP). SDP, опублікований IETF як RFC 4566, визначає спеціальний стандарт для визначення параметрів, що використовуються під час обміну медіа (переважно потоковими медіа) між двома кінцевими точками. Фактично, SDP лише інкапсульований в

інший протокол, що має широке застосування, і в більшості додатків присутній всередині SIP [2].

Session Description Protocol може вказувати (рис. 1.6):

- номер версії протоколу;
- початковий ідентифікатор та ідентифікатор сеансу;
- ім’я користувача, ідентифікатор, номер версії, мережева адреса;
- ім’я сеансу;
- коротка інформація про сеанс;
- URI опису;
- адресу електронної пошти;
- номер телефону;
- інформацію про з’єднання;
- інформацію про пропускну здатність;
- коригування часового поясу;
- ключ шифрування;
- атрибути сеансу;

Protocol version number	v = 0
Owner/creator of session	o = khanvilkar 8988234542 8988234542 IN IP4 192.168.0.201
Session name	s = Presentation on multimedia
Session information	i = Topics on multimedia communication
URI	u = http://mia.ece.uic.edu/sip
E-mail address	e = shashank@evl.uic.edu
Phone number	p = 1-312-413-5499
Connection information	c = IN IP4 192.168.0.201
Bandwidth information	b = CT:144
Time session starts/stops	t = xxxxxxxxxx xxxxxxxxxx
Media information	m = audio 56718 RTP/AVP 0
Media attributes	a = rtpmap : 0 PCMU/8000
Media information	m = video 67383 RTP/AVP 31
Media attributes	a = rtpmap : 31 H261/90000

Рисунок 1.6 – Приклад інформації, яку надає протокол SDP

У типовому процесі ініціювання сеансу в ньому беруть участь дві кінцеві точки. Кожна кінцева точка відправляє SDP іншій кінцевій точці, щоб повідомити про свої характеристики та можливості. На практиці SDP сам по собі не

відправляє медіа, а обмежується узгодженням добре підібраного набору параметрів обміну медіа. Медіапотоки також обробляються в окремому протоколі та каналі.

MGCP. Насправді протокол MGCP являє собою ціле сімейство концептуально схожих рішень. До цієї групи входять такі специфікації: SGCP, IPDC, MGCP, MEGACO, H.248. Створений протокол був у далекому 1999 році [2].

Основна відмінність цього протоколу від двох попередніх полягає в способі управління системою сигналізації. Процесом керує централізований блок управління, повністю відокремлений від медіапотоку. Для роботи з ними в системі передбачені термінали, так звані німі шлюзи або абонентські термінали. Ці термінали можуть виконувати лише обмежену кількість команд. Архітектура цього протоколу надзвичайно проста і складається лише з двох компонентів. Це сам шлюз і пристрій, що відповідає за обробку викликів. (рис. 1.7)

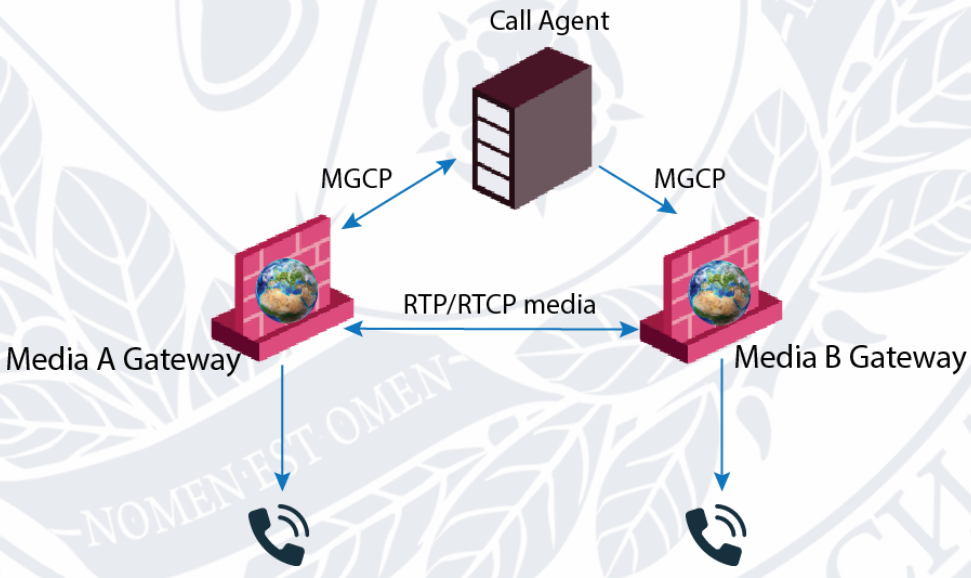


Рисунок 1.7 – Архітектура протоколу MGCP

1.3. Організація та використання мережі IP-телефонії

Комутація телефонних дзвінків - важливе завдання для IP-мереж. Сама по собі IP-адреса не є "телефонним номером" для зв'язку з VoIP-телефонами, оскільки багато користувачів динамічно підключаються до Інтернету і IP-адреси часто змінюються [3].

VoIP-телефон підключається до сервера (наприклад, SIP-сервера), тому серверу відома поточна IP-адреса телефону.

Використовуючи IP-адресу IP-телефону, відому серверу, сервер може перебрати на себе керування комутатором, і набраний IP-телефон дзвонитиме відповідно до цієї IP-адреси (тобто в будь-якій точці світу, якщо IP-телефон зареєстровано в Інтернеті). Зв'язок між IP-телефонами є не залежним від сервера.

Існують також комерційні послуги, що надають місцевий телефонний зв'язок із рахунком для сервера комутації, який також може бути під'єднаний до фіксованої мережі; IP-телефонію зазвичай надають безкоштовно.

Якщо існує фіксована IP-адреса, можна управляти сервером комутації на відповідному комп'ютері (наприклад, OpenSIPS), щоб з'єднати кілька серверів комутації один з одним аналогічно з'єднанню декількох локальних мереж у фіксованій мережі. Комерційні рішення часто включають партнерські мережі, які встановлюють безкоштовне з'єднання між партнерськими мережами VoIP. Вибір мережі часто обмежений, тому що компанії повинні отримувати дохід від телефонних з'єднань VoIP зі звичайною фіксованою мережею. Безкоштовні, самоврядні сервери телефонії з відкритим вихідним кодом можуть технічно сформувати мережу обміну, незалежну від цих економічних обмежень в Інтернеті. Незважаючи на те, що сервери SIP-телефонії технічно добре функціонують, в даний час немає офіційних мереж таких серверів-комутаторів SIP [3].

За наявності фіксованої IP-адреси кілька серверів комутації можуть бути з'єднані між собою аналогічно з'єднанню декількох локальних мереж у стаціонарній мережі, за умови, що серверами комутації керує відповідний

комп'ютер (наприклад, OpenSIPS). Комерційні рішення часто містять партнерські мережі, які встановлюють безкоштовні з'єднання між партнерськими VoIP-мережами. Оскільки компаніям доводиться отримувати дохід від підключення VoIP-телефонії до звичайних фіксованих мереж, вибір мереж часто обмежений. Безкоштовні, автономні сервери телефонії з відкритим вихідним кодом можуть утворювати мережі обмінів, технічно незалежні від таких економічних обмежень в Інтернеті. Хоча сервери SIP-телефонії технічно повністю функціональні, наразі не існує жодної офіційної мережі таких комутаторів SIP-серверів.

Для абонента дзвінок за допомогою IP-телефонії - це те ж саме, що і звичайний телефонний дзвінок. Як і у випадку з традиційною телефонією, виклик поділяється на три основні процеси (налаштування виклику, передача виклику і завершення виклику). На відміну від традиційної телефонії, VoIP не з'єднує по виділеній "лінії", а оцифровує голос і передає його в невеликих пакетах даних за допомогою інтернет-протоколів.

З'єднання (управління викликами, сигналізація) встановлюються і розриваються з використанням протоколів, відмінних від протоколів передачі голосу. Узгодження та обмін параметрами передачі голосу здійснюється за допомогою протоколів, відмінних від протоколів управління викликами.

Для встановлення з'єднання між абонентами в IP-мережі поточна IP-адреса абонента повинна бути відома в мережі, але не обов'язково самому абоненту. Доступ до абонента можливий шляхом попередньої автентифікації абонента і відповідного оприлюднення його поточної IP-адреси, як у мобільних мережах.

Фіксоване присвоєння телефонних номерів IP-адресам неможливе, оскільки місцезнаходження абонента змінюється, змінюються користувачі на одному комп'ютері, а адреси присвоюються динамічно при встановленні мережевого з'єднання. Поширеним рішенням є зберігання абонентом або його терміналом поточної IP-адреси з ім'ям користувача на сервісному комп'ютері (сервері). Комп'ютер управління з'єднанням, або в деяких випадках термінал абонента, може запросити поточну IP-адресу потрібного абонента з цього сервера через вибране ім'я користувача і встановити з'єднання.

Офісна IP-телефонія складається з різних елементів, кожен з яких виконує певну функцію [4]:

- АТС для IP телефонії. Це основний комутаційний пристрій, який, крім забезпечення підключення до традиційних телекомунікаційних послуг, створює локальну мережу передачі даних всередині компанії і звільняє зовнішні лінії. Ця лінійка обладнання має безліч додаткових функцій, які оцінять власники бізнесу, таких як автоматична або ручна переадресація дзвінків, внутрішньофірмові безкоштовні номери, конференц-набір, утримання і заборона (обмеження) дзвінків з певних номерів;
- сервера для IP телефонії. Серверні станції керують локальною мережею і з'єднують АТС з кінцевим користувачем. Кожен сервер може бути оснащений цифровим і аналоговим обладнанням для перетворення (кодування) сигналу і спеціальними платами для передачі інформації на різні зовнішні пристрої. Комбіновані елементи дозволяють, при необхідності, значно розширити внутрішню мережу абонента і навіть забезпечити повноцінний мобільний зв'язок за допомогою встановленого в сервері GSM-модуля;
- телефони для IP телефонії. Це термінал, який використовується для обміну інформацією між абонентами. Вони схожі на звичайні телефони, але мають спеціальні роз'єми для підключення до мережі. Крім того, багато сучасних терміналів підтримують відеозв'язок, що значно розширює їх функціональність;
- гарнітура для IP телефонії. Це незамінний допоміжний пристрій для кол-центрів. На відміну від традиційної телефонної трубки, гарнітура одягається на голову оператора, звільняючи обидві руки і дозволяючи співробітникам одночасно розмовляти і працювати на комп'ютері. Гарнітура також значно покращує якість сигналу та усуває ефекти

відлуння порівняно із зовнішнім підключенням динаміків та мікрофонів;

- програми для IP телефонії. Якісний та стабільний зв'язок неможливий без спеціального програмного забезпечення, призначеного для кодування і перетворення сигналів, стиснення пакетів даних, моніторингу трафіку та виконання інших функцій.

За своїм масштабом всі мережі IP-телефонії можна розділити на міжнародні, регіональні і місцеві [5].

Міжнародні мережі IP-телефонії мають елементи, присутні в багатьох країнах, і відповідають за передачу даних по всьому світу, використовуючи існуючі інтернет-канали з невеликою кількістю TDM або взагалі без нього.

Регіональні мережі обслуговують лише місцевих операторів і обмежуються однією або кількома сусідніми країнами. За необхідності регіональні мережі можуть надавати абонентам можливість завершувати дзвінки в будь-якій точці світу.

Місцеві мережі дозволяють місцевим компаніям та їхнім філіям спілкуватися один з одним і з клієнтами в місцевій телефонній мережі за допомогою IP-телефонії. У більшості випадків оператори місцевих мереж надають доступ до IP-телефонії своїм клієнтам. Як правило, такі мережі використовують лише один шлюз, який з'єднується з регіональною або міжнародною мережею через виділений канал. Для більшості операторів місцеві мережі знаходяться на проміжному етапі розвитку і прагнуть вийти на міжнародний рівень.

Висновки до розділу

Проаналізувавши історію розвитку протоколів, які використовуються в мережах IP-телефонії, неважко припустити, що відмінності в їх функціональності в основному пов'язані з тим, що розробники мали різні уявлення про майбутнє IP-мереж. H.323 і сьогодні широко використовується і

його можна сміливо назвати транзитним рішенням. Це технічно відпрацьоване рішення, яке довело свою успішність при побудові великих операторських мереж; SIP класифікується як "абонентський" протокол, оскільки в першу чергу використовується для оптимізації комунікаційних процесів користувацьких мереж. А от MGCP є оптимальним рішенням, коли IP-мережі необхідно об'єднати з телефонними мережами загального користування.

Розглянувши теоретичну сторону IP-телефонії, варто зазначити її важливість у сучасному світі зв'язку. Ця технологія представляє собою перехід від старих аналогових систем до цифрових розв'язок на основі Інтернет-протоколу.

Основними принципами її функціонування є протоколи, такі як SIP і RTP, які дозволяють здійснювати дзвінки та передавати дані в реальному часу через IP-мережу.

Для успішної організації та ефективного використання IP-телефонії необхідний комплексний підхід до проектування, впровадження та управління, який враховує аспекти якості зв'язку, безпеки і надійності. В цілому, IP-телефонія відображає технологічний прогрес у галузі зв’язку і стає все більш значущою складовою сучасних комунікаційних інфраструктур.

РОЗДІЛ 2. ЗАГРОЗИ В МЕРЕЖАХ IP-ТЕЛЕФОНІЇ

Конфіденційність і безпека є фундаментальними вимогами до будь-якої телефонної мережі. Традиційні мережі досягли певного рівня безпеки, хоча й далекого від досконалості, а поширення IP-телефонії і твердження, що вона незабаром стане домінуючою технологією передачі голосу, є викликами, які ставлять перед багатьма IP-телефонами.

У сучасному корпоративному світі є як противники, так і прихильники використання IP-телефонії як альтернативної технології передачі голосу. Перші кажуть, що їм немає про що турбуватися, тоді як другі повинні усвідомити, що нові інтегровані мережеві та голосові сервіси принесуть нові вразливості в мережу.

2.1. Види загроз в IP телефонії

Безпека зв'язку є одним з найважливіших питань в телекомунікаційних мережах. Сьогодні стрімкий розвиток глобальних комп'ютерних мереж, в тому числі мереж IP-телефонії, робить ще більш важливим забезпечення безпеки передачі інформації. Формулювання заходів безпеки повинно базуватися на аналізі ризиків, визначенні критичних ресурсів системи та ідентифікації можливих загроз

Існує кілька основних типів загроз, які становлять найбільшу небезпеку в мережах IP-телефонії [6]:

- Прослуховування (Eavesdropping). Якщо дані користувача (ідентифікатори та паролі) та приватні конфіденційні дані передаються незахищеними маршрутами, їх можуть підслуховувати і згодом використовувати не за призначенням. Схеми шифрування даних зменшують ймовірність цієї загрози.
- Відмова в обслуговуванні (Denial of Service - DoS) - це тип хакерської атаки, яка робить критично важливі системи непридатними для

використання. Це досягається шляхом переповнення системи непотрібним трафіком, використовуючи всю пам'ять і процесорні ресурси системи. Комунікаційні системи повинні знати про такі атаки та мати інструменти для обмеження їхнього впливу на мережу.

- Підробка ідентифікатору абонента (Caller-ID Spoofing) означає, що якийсь користувач мережі видає себе за іншого. Це створює потенціал для несанкціонованого доступу до критично важливих функцій системи. Використання механізмів автентифікації та авторизації в мережі підвищує впевненість у тому, що користувач, який спілкується, не є імітатором, і йому може бути наданий санкціонований доступ.

2.2. Прослуховування

Прослуховування голосу через Інтернет-протокол (VOIP) – це процес перехоплення або підслуховування голосового трафіку, що передається через мережу VOIP. Це може бути зроблено з різними цілями, включно з кібербезпекою, відстеженням злочинної діяльності або з метою керування мережею [7].

У деяких випадках прослуховування може відбуватися з дозволу учасників спілкування, наприклад, у корпоративному середовищі для навчання або аудиту. Однак у разі підслуховування без належного дозволу можуть статися порушення конфіденційності та законодавства [7].

Щоб забезпечити безпеку мереж VOIP, важливо використовувати засоби шифрування трафіку та автентифікації, щоб запобігти несанкціонованому доступу до голосових повідомлень.

Розглянемо два основних методи прослуховування:

- Перехоплення розмови за допомогою аналізатора трафіку Wireshark
- Закладні пристрої

Експеримент перехоплення розмови за допомогою аналізатора трафіку WireShark. Для цього експерименту ми будемо використовувати:

- Cisco IP Communicator - це програмне забезпечення, розроблене компанією Cisco Systems, яке надає можливість здійснювати голосові та відеодзвінки через мережу IP. Це програмне забезпечення дозволяє працювати з IP-телефонами безпосередньо на комп'ютері користувача, що дозволяє використовувати його як звичайний телефон через мережу даних.
- Wireshark - це додаток для аналізу мережевого трафіку. Він дозволяє перехоплювати та аналізувати пакети даних, що пересилаються через комп'ютерну мережу. Wireshark може бути використаний для розв'язання проблем мережі, виявлення зловмисних атак або відлагодження програмного забезпечення, що використовує мережевий зв'язок. Його інтерфейс простий у використанні, і він підтримує різні протоколи мережі, що дозволяє ретельно аналізувати трафік.

Запускаємо Cisco IP Communicator. Після запуску потрібно налаштувати з'єднання. Для цього зазвичай потрібно вказати IP-адресу або DNS-ім'я сервера Cisco CallManager або Unified Communications Manager. Після того, як все налаштували маємо два IP-телефони для експерименту.

Рисунок 2.1 – Інтерфейс першого телефону

Рисунок 2.2 – Інтерфейс другого телефону

Для того щоб бачити усі пакети, які надсилаються через мережу під час телефонної розмови робимо захват трафіку, обираємо для захвату мережевий адаптер Ethernet за допомогою Wireshark (рис. 2.3) та починаємо захват кнопками Capture >>> Start (рис 2.4).

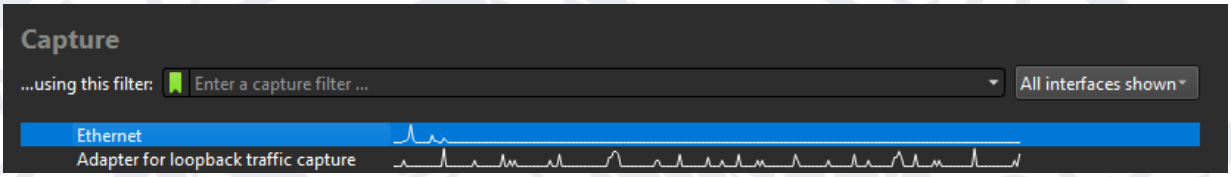


Рисунок 2.3 – Вибір мережевого адаптеру для захвату трафіку

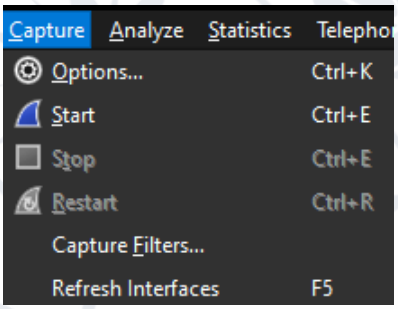


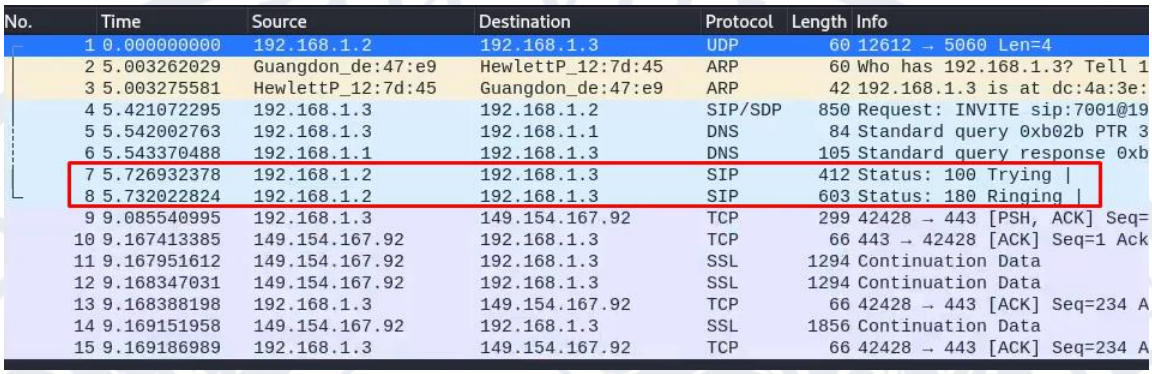
Рисунок 2.4 – Вибір мережевого адаптеру для захвату трафіку

Одразу як Wireshark почав аналіз пакетів, робимо дзвінок з одного телефону на інший.

Рисунок 2.5 – Інтерфейс телефону 1001 під час дзвінку

Рисунок 2.6 – Інтерфейс телефону 1000 під час дзвінку

Як тільки ми зробили дзвінок, бачимо пакет SIP зі статусом дзвінку (рис. 2.7)



No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000000	192.168.1.2	192.168.1.3	UDP	60	12612 → 5060 Len=4
2	5.003262029	Guangdon_de:47:e9	HewlettP_12:7d:45	ARP	60	Who has 192.168.1.3? Tell 1
3	5.003275581	HewlettP_12:7d:45	Guangdon_de:47:e9	ARP	42	192.168.1.3 is at dc:4a:3e:
4	5.421072295	192.168.1.3	192.168.1.2	SIP/SDP	850	Request: INVITE sip:7001@19
5	5.542002763	192.168.1.3	192.168.1.1	DNS	84	Standard query 0xb02b PTR 3
6	5.543370488	192.168.1.1	192.168.1.3	DNS	105	Standard query response 0xb
7	5.726932378	192.168.1.2	192.168.1.3	SIP	412	Status: 100 Trying |
8	5.732022824	192.168.1.2	192.168.1.3	SIP	603	Status: 180 Ringing |
9	9.085540995	192.168.1.3	149.154.167.92	TCP	299	42428 → 443 [PSH, ACK] Seq=
10	9.167413385	149.154.167.92	192.168.1.3	TCP	66	443 → 42428 [ACK] Seq=1 Ack
11	9.167951612	149.154.167.92	192.168.1.3	SSL	1294	Continuation Data
12	9.168347031	149.154.167.92	192.168.1.3	SSL	1294	Continuation Data
13	9.168388198	192.168.1.3	149.154.167.92	TCP	66	42428 → 443 [ACK] Seq=234 A
14	9.169151958	149.154.167.92	192.168.1.3	SSL	1856	Continuation Data
15	9.169186989	192.168.1.3	149.154.167.92	TCP	66	42428 → 443 [ACK] Seq=234 A

Рисунок 2.7 – Захоплені пакети протоколу SIP в Wireshark

Також як тільки з другого телефону прийняли виклик, бачимо пакети RTP (рис. 2.8), цей протокол відповідає за передачу аудіо і відеоданих через IP мережі в режимі реального часу.

No.	Time	Source	Destination	Protocol	Length	Info
953	23.143642747	192.168.1.3	192.168.1.2	RTP	214	PT=ITU-T G.711 PCMU,
954	23.148048516	192.168.1.2	192.168.1.3	RTP	214	PT=ITU-T G.711 PCMU,
955	23.163317429	192.168.1.3	192.168.1.2	RTP	214	PT=ITU-T G.711 PCMU,
956	23.167548716	192.168.1.2	192.168.1.3	RTP	214	PT=ITU-T G.711 PCMU,
957	23.180252173	192.168.1.3	192.168.1.2	RTP	214	PT=ITU-T G.711 PCMU,
958	23.187242078	192.168.1.2	192.168.1.3	RTP	214	PT=ITU-T G.711 PCMU,
959	23.199986179	192.168.1.3	192.168.1.2	RTP	214	PT=ITU-T G.711 PCMU,
960	23.208592313	192.168.1.2	192.168.1.3	RTP	214	PT=ITU-T G.711 PCMU,
961	23.222307210	192.168.1.3	192.168.1.2	RTP	214	PT=ITU-T G.711 PCMU,
962	23.228330536	192.168.1.2	192.168.1.3	RTP	214	PT=ITU-T G.711 PCMU,
963	23.241970724	192.168.1.3	192.168.1.2	RTP	214	PT=ITU-T G.711 PCMU,
964	23.248690578	192.168.1.2	192.168.1.3	RTP	214	PT=ITU-T G.711 PCMU,
965	23.259123300	192.168.1.3	192.168.1.2	RTP	214	PT=ITU-T G.711 PCMU,
966	23.268029703	192.168.1.2	192.168.1.3	RTP	214	PT=ITU-T G.711 PCMU,
967	23.284403430	192.168.1.3	192.168.1.2	RTP	214	PT=ITU-T G.711 PCMU,

Рисунок 2.8 – Захоплені пакети протоколу RTP в Wireshark

Після закінчення розмови, переходимо у вкладку Telephony, вибираємо пункт VoIP Calls.

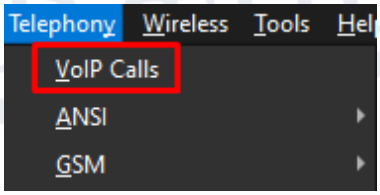


Рисунок 2.9 – Перехід до списку захоплених дзвінків

Після чого бачимо перелік усіх дзвінків, які відбулися під час захвату трафіку мережі (рис. 2.10).

Start Tim	Stop Time	Initial Speaker	From	To	Protocol	Duration	Packets	State	Comments
5.421072	28.818445	192.168.1.3	<sip:7002@192.168.1.3>	<sip:7001@192.168.1.2:12612>	SIP	00:00:23	9	COMPLETED	INVITE 200

Рисунок 2.10 – Список захоплених дзвінків

Після чого переходимо в RTP Player і бачимо запис нашої розмови (рис. 2.11).

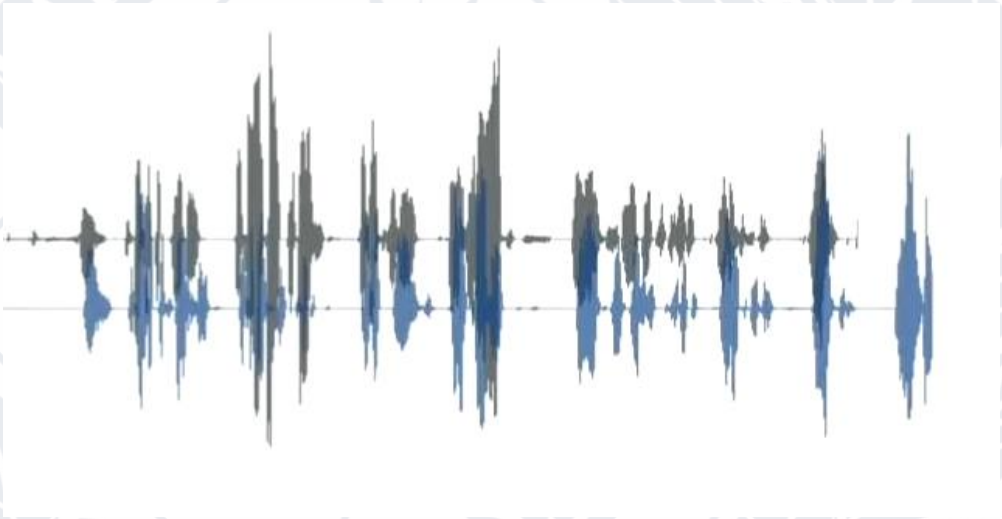


Рисунок 2.11 – Аудіодоріжка запису захопленої телефонної розмови

Для того щоб повністю прослухати запис розмови потрібно натиснути кнопку Analyze (рис. 2.12).

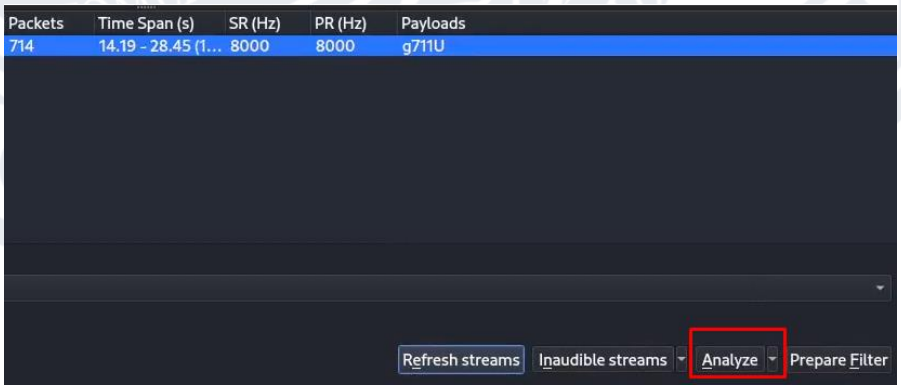


Рисунок 2.12 – Інтерфейс RTP Player

В результаті цього експерименту ми побачили, що перехоплення викликів IP-телефонів за допомогою Wireshark може призвести до серйозних наслідків. Зловмисники можуть отримати доступ до конфіденційної інформації, порушити безпеку мережі, використовувати отримані дані для атак або шпигунства, що може призвести до фінансових втрат і втрати репутації для бізнесу.

Закладні пристрої в IP-телефоніїї. Закладний пристрій - мініатюрний радіоелектронний пристрій перехоплення мовної інформації, який складається з мікрофона і радіопередавача, що забезпечує передачу звукового сигналу на досить значну відстань (рис. 2.13). Закладні пристрої є найпоширенішими технічними засобами знімання акустичної інформації. Їх полулярність пояснюється простотою використання, малими розмірами [8].

Рисунок 2.13 – Приклад встановлення закладного пристрою

Після набору номера телефону, в якому (або біля якого) є відповідна закладка, система переводить апарат у режим очікування кодованого продзвінка в певному інтервалі часу (дзвінок телефону відключається). Після подачі відповідного коду телефон підключається до лінії (трубка "штучно піднімається"), включається вбудований мікрофон і здійснюється акустичний контроль приміщення. При піднятій трубці здійснюється перехоплення та

передавання телефонної розмови, а при покладеній трубці підключається мікрофон закладки і перехоплюється акустична інформація з приміщення.

2.3. Відмова від обслуговування

Будь-яка атака, яка робить цільову службу або ресурс SIP недоступними для законних користувачів, є DoS-атакою. Зловмисник зазвичай націлюється на SIP-сервер, щоб запобігти абонентам використовувати послуги VoIP або погіршити якість пропонованих послуг. Найпоширенішими DoS-атаками є флуд і неправильно сформовані повідомлення (також ці атаки можна зробити розподіленими).

Флуд атаки (Flooding Attacks). Ці атаки базуються на створенні великої кількості SIP-повідомлень, щоб змусити SIP-клієнт або сервер споживати свої ресурси (наприклад, пам’ять і ЦП). Тому компонент SIP буде вимкнено для законних користувачів. Ця атака має кілька форм, таких як INVITE флуд (рис. 2.14), REGISTER флуд, BYE флуд і багатоатрибутний флуд [9].

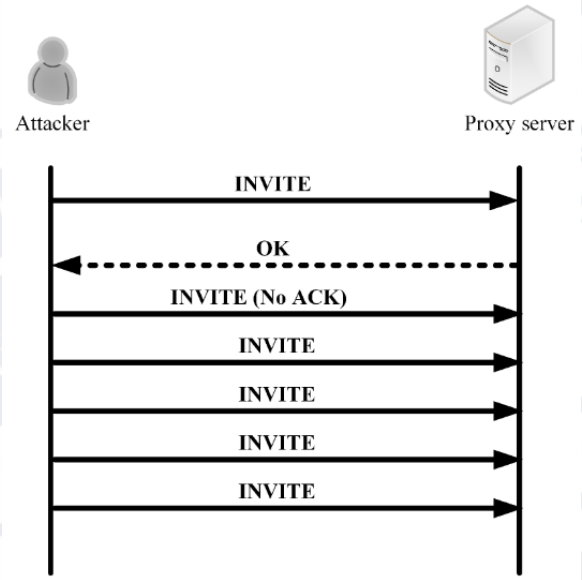


Рисунок 2.14 – Приклад флуд атаки типу «INVITE»

Атаки з хибними повідомленнями (Malformed Message Attacks). Зловмисник змінює правильне повідомлення SIP, яке потім викликає часткову помилку або перезавантаження компонента SIP (тобто клієнта або сервера SIP), коли робиться спроба обробити це повідомлення. Будь-яке повідомлення SIP, несумісне з правильним синтаксисом SIP, вважається неправильним повідомленням. Оскільки аналізатор компонента SIP був написаний для обробки правильно відформатованих повідомлень SIP, існує велика кількість повідомлень SIP, які вважатимуться синтаксично неправильними (рис. 2.15) [9].

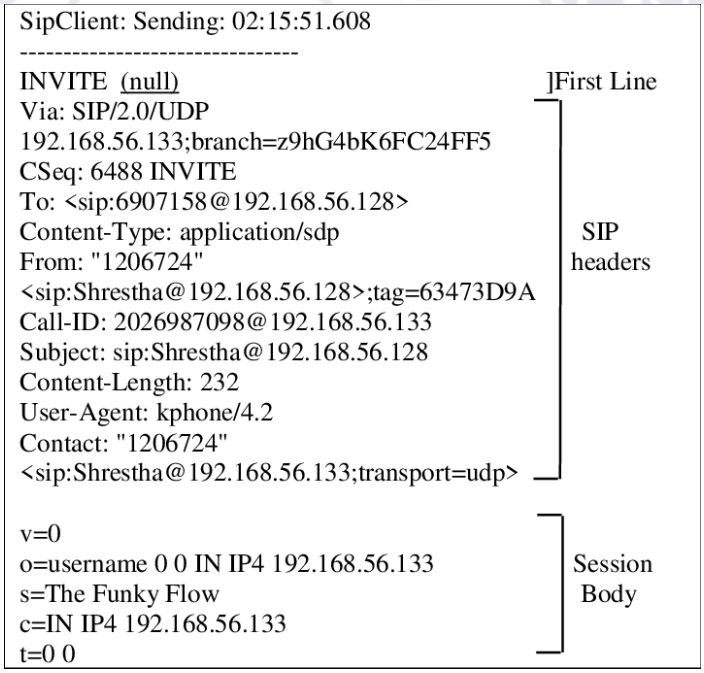


Рисунок 2.15 – Приклад некоректного повідомлення

Неправильне повідомлення може приймати різні форми, наприклад, з недійсною назвою методу, порушенням ієрархії повідомлень або відсутнім обов’язковим заголовком SIP. Інструмент SIP-Msg-Gen може генерувати некоректні повідомлення за допомогою багатьох різних сценаріїв.

Розподілені атаки на відмову в обслуговуванні (Distributed Denial of Service Attacks). DDoS-атака — це DoS-атака, яка виконується одночасно з використанням багатьох комп’ютерів. Ці атаки завжди здійснюються з використанням групи комп’ютерів, якими керує зловмисник (Botnet).

Зловмисник заражає комп'ютери скомпрометованих користувачів, який використовується для контролю та використання їхніх комп'ютерів у DDoS-атаці. Виявлення DDoS-атак складніше, ніж DoS-атак, оскільки блокування джерела на основі обмежень трафіку недостатньо. Крім того, скомпрометовані користувачі зазвичай не знають, що їхні комп'ютери є частиною DDoS-атаки.

Приклад атаки. Останнім часом VoIP-компанії стали мішенню серії розподілених DDoS-атак з вимогою викупу по всьому світу: британські провайдери VoIP, включаючи VoIP Unlimited, та канадська компанія VoIP.ms зазнали агресивних і тривалих атак, що дестабілізували їхню інфраструктуру та спричинили масові перебої в наданні послуг.

Ці DDoS-атаки на VoIP-провайдерів потрапляли в заголовки новин, і, за даними Hackread.com, атаки на VoIP.ms почалися 16 вересня, націлені на їхні сервери імен DNS та іншу інфраструктуру, щоб порушити їхні послуги телефонії, в результаті чого люди не могли здійснювати або приймати дзвінки. Веб-сайт компанії залишався важкодоступним протягом декількох днів після того, як стало відомо про атаки.

Група, відома як REvil, взяла на себе відповідальність за ці DDoS-атаки на сектор VoIP, вимагаючи від VoIP.ms 1 біткойн (приблизно 55 000 доларів США) за припинення атак, але невідомо, чи це та сама група, що займається викупом і має таку ж назву. Компанія VoIP unlimited також заявила, що отримала масову вимогу викупу за припинення атак.

2.4. Підробка ідентифікатору абонента

Caller-ID Spoofing (підробка ідентифікатору абонента) викликає все більше занепокоєння в сфері телекомунікацій, оскільки вона дозволяє зловмисникам маніпулювати інформацією про ідентифікатор (номер) абонента, що відображається на пристрої одержувача.

Найпоширенішим методом здійснення атак на підміну ідентифікатора абонента є використання VoIP-телефонії. Технологія VoIP дозволяє передавати

голосовий зв'язок через Інтернет, а не через стаціонарну телефонну лінію або стільникову мережею. Ця зручність призвела до поширення VoIP-провайдерів, які пропонують клієнтам можливість налаштовувати свої інформацію про ідентифікатор абонента за допомогою своїх послуг [10].

Підробку ідентифікатора абонента також можна здійснити за допомогою готових веб- або мобільних додатків. Ці додатки зазвичай дозволяють користувачам вводити номер телефону, на який вони хочуть зателефонувати, а потім номер телефону, який буде відображатися як ідентифікатор абонента. Потім дзвінок надсилається через VoIP-провайдера, який змінює інформацію про вихідний ідентифікатор абонента перед тим, як з'єднання з потрібним номером телефону.

Крім готових додатків, можна використовувати спеціалізовані сервіси, такі як SpoofCard, для генерації підроблених дзвінків у невеликих обсягах. Автоматичні генератори викликів, такі як Mr.SIP або SIPp, можна використовувати для генерації великих обсягів дзвінків, кожен з яких має індивідуальний, випадковий або ретельно підібраний номерами викликів. Індивідуальні сценарії також можуть бути створені за допомогою VoIP-провайдера, підключеного до системи Asterisk [11].

Варто зазначити, що можливість підміни ідентифікатора абонента варіюється в різних країнах і регіонах. У країнах із суворим законодавством, таких як Сполучені Штати Америки (США) та Велика Британія (Великобританія), ініціювати дзвінок з підробленим ідентифікатором абонента надзвичайно складно. Однак у країнах з меншим регулюванням або наглядом, таких як регулювання або нагляду, наприклад, у країнах, що розвиваються, підробка ідентифікатора абонента є відносно простою. Можливість підробляти інформацію про абонента і переривати дзвінки в будь-якій країні незалежно від нормативних актів, підкреслює потребу в комплексному рішення, яке може ефективно вирішити цю проблему. Крім того, легкість, з якою підробка ідентифікатора абонента може бути здійснена за допомогою готових веб- або мобільних додатків, спеціалізованих сервісів та автоматизованих генераторів

дзвінків, ще більше підкреслює необхідність рішення, здатного вирішити цю проблему в глобальному масштабі [11].

Збільшення кількості інцидентів підміни ідентифікатора абонента можна пояснити широким розповсюдженням VoIP-телефонії. Технологія VoIP робить підробку ідентифікатора абонента дешевшою, гнучкішою та більш доступним для глобальної аудиторії. Крім того, природа VoIP, яка передає лише аудіосигнал, а не пов'язані з ним метадані, значно полегшує здійснення підробки ідентифікатора абонента, ніж інші форми шахрайства, такі як електронний фішинг.

Оскільки заходи безпеки покращилися в інших сферах, таких як фільтрація електронної пошти, освіта щодо різних форм шахрайства, зменшення використання незахищених кредитних карток, а також розвиток технологій автентифікації, таких як мобільна автентифікація та двофакторна автентифікація (2FA), інші форми шахрайства стали більш складними для здійснення. Однак користувачі продовжують покладатися на телефонну систему і схильні довіряти інформації про ідентифікатор абонента, що відображається на екрані, що робить їх більш вразливими до атак підміни ідентифікатора абонента.

Висновки до розділу

Аналіз основних загроз для мереж IP-телефонії дає можливість зрозуміти серйозність проблем, пов'язаних із безпекою в цьому типі мереж. Прослуховування, відмова в обслуговуванні та підміна даних про користувача — це лише деякі з найбільш поширених загроз, які можуть призвести до серйозних наслідків для користувачів та компаній. Знання цих загроз і прикладів їх реалізації допомагає підвищити свідомість і забезпечити належний рівень захисту для мереж IP-телефонії. Реалізація ефективних заходів захисту, таких як шифрування даних, встановлення захисту від відмови в обслуговуванні та моніторинг мережі для виявлення підозрілих активностей, може значно зменшити ризики і забезпечити безпеку використання IP-телефонії.

РОЗДІЛ 3. МЕТОДИ ЗАХИСТУ МЕРЕЖ IP-ТЕЛЕФОНІЇ

При обговоренні використання IP-телефонії в повсякденному житті, питання безпеки сприймається дуже серйозно. Чим більше нашої інформації потрапляє в Інтернет, тим більше ми стаємо вразливими. У зв'язку з цим виникає питання, наскільки конфіденційною є інформація, яку ми передаємо через відкриті мережі. Наскільки конфіденційними є внутрішні зустрічі в компаніях.

За результатом аналізу основних загроз виявилося, що IP-телефони можна захистити лише за умови впровадження заходів безпеки на всіх рівнях мережевої інфраструктури. По суті, злом IP-телефону - це такий самий вид хакерської атаки, як злом веб-сайту або клієнтської бази з використанням тих самих прийомів і методів. Тому за безпеку IP-телефонії, як і за всю безпеку локальної мережі, повинні відповідати фахівці з мережевої безпеки, які не повинні забувати про основні методи захисту мережі:

- Детальна побудова топології мережі.
- Використання захисту від прослуховування.
- Використання захисту від DDoS-атак.
- Використання захисту від підміни ідентифікатору абонента.
- Використання технологій автентифікації.

3.1. Методи захисту від прослуховування

Достатня кількість компаній в Україні ще досі не використовує шифрування в мережах IP-телефонії через лишні витрати, застаріле обладнання, відсутність обізнаності про небезпеку тощо. При цьому воно в край необхідне, адже, якщо дані під час дзвінку не шифруються, то зловмисник може їх перехопити без жодних проблем.

Загалом шифрування в IP-телефонії використовується для захисту конфіденційності та цілісності голосового трафіку, що передається через IP-

мережі. Конфіденційність та цілісність інформації під час дзвінку забезпечується різними протоколами шифрування, наприклад такими як [12]:

1. TLS (Transport Layer Security): TLS використовується для захисту сеансових з'єднань між клієнтами та серверами; в контексті IP-телефонії TLS використовується для захисту сигнального трафіку, такого як SIP (Session Initiation Protocol).

2. SRTP (Secure Real-time Transport Protocol): SRTP використовується для захисту голосового трафіку в режимі реального часу. Симетричні ключі шифрування забезпечують шифрування аудіопотоку між двома пристроями, що здійснюють дзвінок.

3. IPsec (Internet Protocol Security): IPsec можна використовувати для захисту трафіку на рівні мережі шляхом шифрування всієї інформації IP-пакетів. Це включає заголовки IP-пакетів, що містять голосові дані.

4. ZRTP (Zimmermann Real-time Transport Protocol): ZRTP - це протокол, спеціально розроблений для захисту VoIP-дзвінків, що забезпечує захист від атак типу "людина посередині" і надає можливість використання ефемерних ключів для зниження ризику витоку конфіденційної інформації.

Найкращим варіантом захисту інформації, що передається мережами IP-телефонії, є поєднання протоколів шифрування Secure Real-Time Transport Protocol (SRTP) і Transport Layer Security (TLS). Там, де голос передається через VoIP і необхідне шифрування, слід використовувати протокол SRTP. Він забезпечує шифрування трафіку, автентифікацію повідомлень і захист від атак повторного відтворення. Це доступний та швидкий криптографічний протокол, який захистить вашу інформацію у відкритих мережах. Другий протокол — TLS, який шифрує іншу інформацію. В процесі дзвінка фігурують службові повідомлення, такі як номери телефонів та імена користувачів, які також повинні бути надійно "приховані". Цей протокол захищає SIP-повідомлення від підслуховування та модифікації [12].

Для забезпечення ефективного шифрування TLS та SRTP, мережа повинна бути швидка та надійна тому, що шифрування може додати затримку до передачі

даних та шифрування вимагає стабільного та надійного з'єднання для забезпечення безперервності розмов.

Для більшості малих та середніх підприємств достатньо сучасних IP-телефонів, які підтримують протоколи TLS та SRTP.

Наприклад такі, як:

Cisco

- Cisco 8800 Series (напр., Cisco 8841, Cisco 8851)
- Cisco 7800 Series (напр., Cisco 7841, Cisco 7861)
- Cisco 6900 Series (напр., Cisco 6941)

Yealink

- Yealink T5 Series (напр., Yealink SIP-T58A, Yealink SIP-T56A)
- Yealink T4 Series (напр., Yealink SIP-T48S, Yealink SIP-T42S)
- Yealink T2 Series (напр., Yealink SIP-T29G, Yealink SIP-T27G)

Grandstream

- Grandstream GXP Series (напр., Grandstream GXP2170, Grandstream GXP2135)
- Grandstream GRP Series (напр., Grandstream GRP2616, Grandstream GRP2604)

Однак для великих організацій або мереж з високим навантаженням може знадобитися спеціалізовані пристрої, які займаються шифруванням трафіку та знижують навантаження на IP-телефони та сервери (наприклад Cisco Adaptive Security Appliance) або сервери безпеки для управління ключами шифрування та аутентифікації, що може підвищити рівень безпеки і масштабованість системи (наприклад Asterisk з використанням FreePBX або інших інтерфейсів).

Таким чином, TLS і SRTP - це два криптографічні протоколи, але вони захищають різні типи інформації: SRTP захищає ваш голос, а TLS - службову інформацію, яка передається через протокол SIP.

3.2. Методи захисту від закладних пристроїв

Закладні пристрої - це технічні засоби негласного отримання інформації, що таємно розміщуються в об'єктах розвідувальної діяльності та призводять до загрози витоку інформації [8];

Виявлення засобів негласного знімання інформації в IP-телефонії, може бути складним завданням, оскільки багато з них можуть бути дуже майстерно замасковані. Однак є кілька методів, які можуть допомогти виявити такі пристрої [8]:

- візуальне обстеження (візуальний пошук) – різновид фізичного пошуку, який містить безпосередній (та/або за допомогою візуально-оптичних та освітлювальних засобів та пристроїв) візуальний огляд будівельних, огороджувальних та оздоблювальних конструкцій (матеріалів), меблів, предметів інтер’єру, сувенірів, технічних засобів, їх комунікацій тощо, які встановлені (розміщені) на об’єкті інформаційної діяльності, з метою виявлення та аналізу “підозрілих” місць, де можуть бути встановлені закладні пристрої, виявлення закладних пристроїв або їх демаскувальних ознак [8];
- діяльність (надання послуги) з виявлення закладних пристроїв – проведення пошукових дій з виявлення технічних каналів витоку інформації, що утворюються за рахунок використання закладних пристроїв на об’єктах інформаційної діяльності [8];
- легенда прикриття робіт з виявлення закладних пристроїв – призначені для маскування (прикриття) факту проведення робіт з виявлення закладних пристроїв, спеціально підготовлені та впроваджені (доведені до відома визначених співробітників замовника), зовнішньо правдоподібні дезінформуючі відомості про виконавців робіт та їх діяльність [8];
- спеціальний захисний знак – знак (голограма, клейка стрічка, саморуйнівна плівка, мітка, речовина, пломба тощо), що встановлюється (наноситься) на предмет з метою контролю несанкціонованого доступу до нього шляхом

визначення оригінальності і цілісності цього знака візуальним, інструментальним або іншим способом [8];

- фізичний пошук – прослуховування з метою виявлення сторонніх акустичних сигналів на об’єкті інформаційної діяльності, візуальний огляд, прощупування та розбирання (за необхідності) будівельних, огороджувальних та оздоблювальних конструкцій (матеріалів), меблів, предметів інтер’єру, сувенірів, технічних засобів, ліній зв’язку, пожежної та охоронної сигналізації, інших комунікацій тощо, які встановлені (розміщені) на об’єкті інформаційної діяльності, з метою встановлення та аналізу “підозрілих” місць, де можуть бути встановлені закладні пристрої, виявлення закладних пристроїв або їх демаскувальних ознак [8].

3.3. Методи захисту від DDoS-атак

Всім компаніям необхідно інвестувати в постійний захист від DDoS, який здатний пом’якшувати атаки DDoS на VoIP та інші атаки за лічені секунди.

При захисті від DDoS-атак діє емпіричне правило: "Хвилини на збій, години на відновлення". Тому при захисті від атак важлива кожна секунда.

Існує кілька методів захисту від DoS (Denial of Service) та DDoS (Distributed Denial of Service) атак в мережах IP-телефонії. Деякі з них включають:

1. Фільтрація пакетів на рівні мережевого обладнання: Використання фаєрволів, IPS (Intrusion Prevention Systems) та IDS (Intrusion Detection Systems) для фільтрації трафіку на рівні мережевого обладнання. Це дозволяє виявляти та блокувати небажаний трафік, включаючи пакети, які можуть бути частиною DoS або DDoS атак.

2. Методи розпізнавання і обробки трафіку на рівні застосунків: Ці методи включають в себе використання розуміння протоколів IP-телефонії для виявлення аномального або небажаного трафіку. Наприклад, системи IDS/IPS можуть аналізувати SIP (Session Initiation Protocol) трафік для виявлення атак на протоколи.

3. Методи розпізнавання і виявлення аномалій: Використання алгоритмів машинного навчання та штучного інтелекту для аналізу нормального трафіку мережі та виявлення аномалій, що можуть свідчити про DoS або DDoS атаки.

4. Захист на рівні мережі: Використання різних технологій та протоколів на рівні мережі, таких як MPLS (Multiprotocol Label Switching) або VPN (Virtual Private Network), щоб забезпечити відокремлення та захист від атак на рівні мережі [13].

5. Географічне розподілення серверів і мережевих ресурсів: Використання розподілених центрів обробки даних та CDN (Content Delivery Networks) для розподілу навантаження та захисту від DDoS атак, шляхом редиректу трафіку із зони атаки на інші географічно віддалені сервери.

Серед усіх цих методів найефективнішим є Intrusion Prevention Systems (IPS). Одна з провідних IPS це Imperva DDoS Protection. Ця IPS забезпечить захист від специфічних загроз IP-телефонії таких, як SIP-атаки та Voice Flooding.

Imperva DDoS Protection пропонує низку функцій, які можуть бути корисними для захисту IP-телефонії, таких як:

- Миттєві повідомлення про атаку
- Легкий моніторинг
- Інтеграція з вашою SIEM
- Швидке розгортання та масштабування
- Найкраща маршрутизація трафіку
- Управління потужністю в реальному часі
- Мінімальна затримка

Лідери різних галузей, які покладаються на Imperva:

- 4 з 5 найкращих банків США
- 7 з 10 найкращих світових компаній з надання фінансових послуг
- 5 з 10 найкращих світових страхових компаній
- 6 з 10 найкращих телекомунікаційніх компаній

Ця IPS не тільки зможе захистити вашу IP-телефонію, а й інші компоненти вашої мережі. Однак, перед тим як вибирати конкретний захист від DDoS для IP-телефонії, важливо ретельно проаналізувати потреби вашої організації і можливості Imperva DDoS Protection, щоб переконатися, що він відповідає вашим вимогам.

3.4. Методи захисту від атак з підміною ідентифікатора абонента

Виявлення та запобігання підміні ідентифікатора абонента є складним завданням, оскільки телефонна мережа є складною системою операторів і постачальників рішень, що ускладнює для більшості провайдерів та урядових установ відстежувати та переслідувати тих, хто займається цією незаконною діяльністю. Крім того, розрізнити легітимний та підроблений ідентифікатор абонента важко, оскільки багато VoIP-серверів зараз дозволяють своїм користувачам обирати власний ідентифікатор абонента, а оператори можуть не виконувати перевірку автентичності перед з'єднанням перед підключенням дзвінка. Ця проблема віддзеркалює проблеми, що виникають з підміною IP-адрес і підкреслює необхідність для постачальників послуг впроваджувати фільтрацію вихідного трафіку, що ще більше ускладнює виявлення та запобігання підміні [14].

Щоб запобігти підміні ідентифікатора абонента на індивідуальному рівні, доступні різноманітні додатки для смартфонів, які можуть перевірити інформацію про ідентифікатор абонента. Однак цей підхід не є достатнім, оскільки він покладається на те, що реальний абонент встановив додаток. У банківському секторі, де доступ до рахунків клієнтів надається через перевірку банківського номера або номера кредитної картки, пов'язаного з ідентифікатором абонента, застосовуються додаткові заходи, такі як секретні запитання, для виявлення потенційних підробок. Однак, не всі банки беруть до уваги цей ризик і продовжують покладатися на запевнення постачальника послуг щодо заборони підміни ідентифікатора абонента [14].

Складність виявлення та запобігання підробці ідентифікатора абонента в поєднанні зі зростаючою поширеністю цієї атаки, підкреслює необхідність комплексного рішення, яке може ефективно вирішити цю проблему в глобальному масштабі.

Існує кілька добре відомих і широко використовуваних механізмів, які використовуються існуючими системами запобігання атак підробки ідентифікатора абонента [11]:

- Керований чорний список: Більшість постачальників телекомунікацій використовують активний чорний список. Цей список визначає, чи вхідні дзвінки слід заблокувати або дозволити, а він оновлюється в результаті відгуків користувачів. Однак ця стратегія має свої обмеження, оскільки вона не ефективна для нових дзвінків з номерів, яких немає в списку або для дзвінків, що використовують випадкові підроблені номери набору. Крім того, керувати та розповсюджувати чорний список складно, ризиковано, і вразливо до маніпуляцій. Суб'єкти інфраструктури потрібно змінити для підтримки чорного списку. Крім того, кількість записів у чорному та білому списках вплине на затримку.
- Власне автентифікація: Автентифікація в IP-мережах полягає в перевірці та підтвердженні ідентичності користувача або пристрою, який намагається отримати доступ до мережевих ресурсів. Цей процес використовується для контролю доступу до мережі та її ресурсів, забезпечуючи лише авторизованим користувачам або пристроям можливість з'єднання. Аутентифікація зазвичай використовує ідентифікаційні дані, такі як ім'я користувача та пароль, але також може використовувати інші методи, такі як сертифікати, біометричні дані або двофакторна аутентифікація. Це допомагає забезпечити безпеку мережі та зберегти конфіденційність і цілісність даних.

Підводячи підсумок, в порівнянні з чорним списком, автентифікація зазвичай вважається кращим засобом захисту. Вона не обмежена лише наявністю

відомих або підозрілих номерів, а забезпечує перевірку ідентичності кожного користувача або пристрою перед наданням доступу до мережі. Автентифікація дозволяє зменшити ризик несанкціонованого доступу, навіть у випадках, коли сторона атаки використовує нові методи або технології.

3.5. Технології автентифікації

Використання відкритих мереж для передачі даних несе за собою потенційні ризики. Тому однією з основних проблем забезпечення безпеки інформації при взаємодії користувачів є використання методів та інструментів, які дозволяють одній стороні перевірити автентичність іншої сторони. Для вирішення цієї проблеми зазвичай використовуються спеціальні методики перевірки автентичності сторони, що верифікується.

Кожен об'єкт (користувач або процес, що діє від імені користувача), зареєстрований у комп'ютерній системі, має певну інформацію, яка його унікально ідентифікує. Це може бути число або рядок символів, який називає об'єкт. Ця інформація називається ідентифікатором об'єкта. Якщо користувач має ідентифікатор, зареєстрований у мережі, він вважається легітимним користувачем; в іншому випадку він вважається неавторизованим користувачем. Перш ніж користувач отримає доступ до ресурсів комп'ютерної системи, він повинен пройти початковий процес взаємодії з комп'ютерною системою, включаючи автентифікацію.

Автентифікація - це процедура перевірки автентичності заявленого користувача, процесу або пристрою. Ця перевірка забезпечує надійну гарантію того, що користувач (процес або пристрій) відповідає заявленому. Виконуючи автентифікацію, сторона, що перевіряє, узгоджує справжність особи, яка автентифікується, а особа, яка автентифікується, бере активну участь в обміні інформацією. Зазвичай користувачі автентифікуються, вводячи в систему унікальну інформацію про себе (наприклад, паролі або сертифікати), яка невідома іншим користувачам [11].

Методи автентифікації також можна класифікувати за рівнем безпеки. Таким чином, процеси автентифікації можна розділити на наступні типи [11]:

- автентифікація за допомогою пароля або PIN-коду;
- надійна автентифікація на основі використання методів та інструментів шифрування;
- біометрична автентифікація користувача.

З точки зору безпеки, кожен з цих типів сприяє вирішенню певної проблеми, саме тому процеси та протоколи автентифікації активно використовуються на практиці.

Серед багатьох проколів автентифікації найпопулярнішими та найбільш надійними є:

- TACACS+ - це вдосконалена версія оригінального мережевого протоколу TACACS, розробленого компанією Cisco. Він зараз широко використовується в галузі (AAA) для автентифікації, авторизації та обліку у безпеці мережі [15].
- RADIUS - це мережевий протокол, який авторизує та автентифікує користувачів, які отримують доступ до віддаленої мережі. RADIUS був розроблений компанією Livingston Enterprises, Inc. у 1991 році та перетворився на стандарт для IETF [16].

Порівняння протоколів TACACS+ та RADIUS. TACACS+ і RADIUS функціонально дуже схожі, але є деякі важливі відмінності.

Механізм авторизації. При використанні TACACS+ сервер схвалює або відхиляє запити на автентифікацію обробляючи інформацію профілю користувача. Вміст профілю користувача невідомий клієнту. В той самий час в системі RADIUS всі атрибути профілю користувача, надіслані з відповіддю, надсилаються на сервер мережевого доступу. Сервер схвалює або відхиляє запит на автентифікацію на основі отриманих значень атрибутів.

Загалом, протокол RADIUS не підтримує авторизацію. Виходячи з цього можна сказати, що використовувати RADIUS варто тільки в тому випадку, якщо

заздалегідь відомо, які саме сервіси будуть доступні конкретному RADIUS-клієнту. В той час як TACACS+ підтримує аутентифікацію. Однак слід відмітити, що кількість сервісів, дозволених в поточній версії, є обмеженою. Це означає, що для доступу до сервісу RADIUS обробляє один запит (автентифікація - запит, відповідь), тоді як TACACS+ обробляє два запити (автентифікація і авторизація), але в той же час за допомогою TACACS+ можна отримати доступ до іншого сервісу.

Аудитом в TACACS+ передбачено використання обмеженого числа інформаційних полів. В той час як аудитом в RADIUS надається більше інформації, ніж в TACACS+, що є значною перевагою над TACACS+.

Обмін повідомленнями між клієнтом і сервером захисту. TACACS+ підтримує двонаправлений потік запитів та відповідей між клієнтом (наприклад, маршрутизатором або комутатором) і сервером мережевого доступу. Це означає, що як клієнт, так і сервер можуть ініціювати комунікацію та обмін даними під час процесу аутентифікації та авторизації.

В той час як RADIUS використовує однонаправлений потік запитів та відповідей від клієнта (наприклад, мережевого пристрою) до сервера безпеки RADIUS. У цьому сценарії клієнт ініціює запит, а сервер відповідає на нього з відповідними даними. Однак, після успішної аутентифікації та авторизації сервер може ініціювати відправку додаткових даних до клієнта для обліку або інших цілей.

Така особливість TACACS+ дає більшу гнучкість та контроль над обробкою запитів і дозволяє більш точно налаштувати права доступу до мережевих ресурсів.

Шифрування даних. TACACS+ забезпечує шифрування всього вмісту пакетів, включаючи не лише атрибути пароля, а й інші чутливі дані, що передаються між клієнтом та сервером. Це означає, що весь обмін даними між ними зашифрований, що забезпечує більш високий рівень захисту і збереження цілісності. В той час як RADIUS шифрує лише атрибути пароля в пакеті Access-Request, залишаючи інші частини пакету незашифрованими. Це означає, що інші

дані, наприклад, інформація про авторизацію чи інші атрибути, піддаються ризику в разі несанкціонованого доступу до мережевого трафіку.

Таким чином, захищеність TACACS+ може бути вищою, оскільки вона забезпечує повне шифрування всього обміну даними між клієнтом та сервером, що сприяє підвищенню безпеки мережі.

Різноманітність налаштування. Гнучкість протоколу TACACS+ дозволяє адміністраторам створювати різноманітні конфігурації, які відповідають індивідуальним потребам користувачів та вимогам мережі. Ця гнучкість проявляється у можливості налаштування різних аспектів аутентифікації, авторизації та обліку, таких як права доступу, маршрутизація запитів, обробка помилок та багато інших.

Наприклад, TACACS+ підтримує каталоги повідомлень, що дозволяє адміністраторам налаштовувати різні повідомлення для різних ситуацій, таких як успішна аутентифікація, невдача аутентифікації, відхилення доступу тощо. Це дозволяє створювати більш інформативні та корисні повідомлення для користувачів та адміністраторів мережі.

Навпаки, RADIUS, хоча й підтримує можливість зміни наборів атрибутів і значень, він має меншу гнучкість порівняно з TACACS+. Багато функцій, таких як каталоги повідомлень, доступні в TACACS+, але відсутні в RADIUS. Це може обмежувати можливості налаштування та адаптації до конкретних потреб мережі та користувачів.

Отже, TACACS+ зазвичай вважається більш гнучким та розширюваним протоколом в порівнянні з RADIUS, оскільки він дозволяє більш широкий спектр конфігураційних можливостей, що відповідають різним вимогам мережі та її користувачів.

Перенаправлення запиту. В цьому випадку RADIUS має перевагу перед TACACS+ у здатності перенаправляти запити між різними регіонами мережі. Наприклад, якщо у компанії є різні офіси в різних регіонах з серверами RADIUS, то клієнт може надіслати свій запит на автентифікацію до локального сервера

RADIUS, який потім може перенаправити цей запит до відповідного регіону для обробки. TACACS+ не має такої можливості.

Також, коли клієнт відправляє запит до RADIUS, він може чекати на відповідь протягом певного часу, а якщо відповідь не надходить, то повторно відправляти запит. У випадку TACACS+ цього не відбувається, але забезпечується доставка запитів через встановлене TCP-з'єднання, що може бути повільним у великих мережах.

Транспортний протокол. TACACS+ використовує протокол TCP і служить для адміністративного доступу до мережевих пристроїв. Він має окремі запити на автентифікацію, авторизацію та облік. Через окремий запит на авторизацію він може враховувати всі введені команди, що дозволяє більш точно контролювати доступ і дії адміністраторів. Проте, TACACS+ має обмежений облік, тобто не збирає детальну інформацію про використання мережевих ресурсів.

RADIUS, у свою чергу, є стандартним протоколом, який працює над протоколом UDP і використовується для автентифікації, авторизації та обліку користувачів у мережі. Є два стандартних порти: один для автентифікації та відповіді на неї, інший для обліку. RADIUS зазвичай збирає більше інформації про трафік та системні параметри у порівнянні з TACACS+.

Отже, з порівняння цих протоколів можна зробити висновок, що для більшої безпеки мережі мають будуватися з використанням технології AAA з протоколом TACACS+.

Висновки до розділу

В результаті аналізу методів захисту мереж IP-телефонії виявлено, що найефективнішим підходом є комбінація різних технологій і заходів безпеки. Для захисту від прослуховування краще використовувати поєднання протоколів шифрування SRTP і TLS, що забезпечує безпечну передачу даних через мережу.

Для виявлення та пом'якшення DDoS-атак варто використовувати системи запобігання вторгнень (IPS). Один з провідних IPS - Imperva DDoS Protection - дозволяє вчасно виявляти та мінімізувати негативний вплив таких атак на мережеву інфраструктуру.

Щодо виявлення та запобігання підміни ідентифікатора абонента, найефективнішим методом є використання протоколу автентифікації, зокрема TACACS+. Цей протокол надає додаткові можливості контролю доступу та забезпечує безпеку під час аутентифікації користувачів у мережі.

Загалом, захист мереж IP-телефонії вимагає комплексного підходу та впровадження різноманітних технологій і заходів безпеки на всіх рівнях мережевої інфраструктури. Тільки такий підхід може забезпечити надійний захист від різноманітних загроз та атак у сучасних мережах IP-телефонії.

ВИСНОВКИ

У ході роботи було розглянуто питання безпеки в мережах IP-телефонії, що є актуальною та важливою проблемою у сучасному світі з розвитком технологій. Розглянуті аспекти включали в себе основні концепції IP-телефонії, її принцип роботи та взаємодію протоколів, а також загрози, які можуть виникнути в таких мережах, такі як прослуховування, відмова в обслуговуванні та підробка ідентифікатору абонента.

Для ефективного захисту мереж IP-телефонії використання комплексного підходу є важливим. Наприклад, для захисту від прослуховування рекомендується використовувати поєднання протоколів шифрування SRTP і TLS. Для виявлення і пом'якшення DDoS-атак рекомендується використовувати системи запобігання вторгнень (IPS), такі як Imperva DDoS Protection. А для виявлення та запобігання підміні ідентифікатора абонента рекомендується використовувати автентифікацію, зокрема протокол TACACS+.

Такий комплексний підхід дозволяє ефективно захищати мережі IP-телефонії від різноманітних загроз і забезпечує безпеку та надійність їхньої роботи. Важливою складовою є постійне оновлення та адаптація заходів безпеки до змінних умов та розвитку технологій, щоб забезпечити найвищий рівень захисту мереж IP-телефонії.

СПИСОК ВИКОРИСТАНИХ ПОСИЛАНЬ

1. Мітраков М. А. Аналіз методів реалізації IP-телефонії у корпоративних мережах : пояснювальна записка до кваліфікаційної роботи здобувача вищої освіти на другому (магістерському) рівні, спеціальність 172 Телекомунікації та радіотехніка / М. А. Мітраков ; М-во освіти і науки України, Харків. нац. ун-т радіоелектроніки. – Харків, 2022. – 77 с.

2. Kantola, R. IP telephony protocols, architectures and issues, Helsinki University of Technology, 2001. 121 p.

3. Мілєвський, О. А. Принцип побудови та впровадження в корпоративну мережу IP телефонії на базі Asterisk : магістерська дис. : 172 Телекомунікації та радіотехніка / Мілєвський Олександр Андрійович. – Київ, 2022. – 76 с.

4. Ружинський, Т. І. Корпоративна мережа VoIP: пояснювальна записка випускника освітнього ступеня бакалавр, спеціальність 172 Телекомунікації та радіотехніка, 2023. 57с.

5. Черкасов Д. І. Основи технології VoIP та IP-телефонії / Дмитро Черкасов // Телеком. Військовий зв'язок. - 2017. - № 2. - С. 98-104.

6. Suthar D., Rughani P. H. A Comprehensive Study of VoIP Security. *2020 2nd International Conference on Advances in Computing, Communication Control and Networking (ICACCCN)*, Greater Noida, India, 18–19 December 2020. 2020.

7. Biondi P., Bognanni S., Bella G. VoIP Can Still Be Exploited - Badly. *2020 Fifth International Conference on Fog and Mobile Edge Computing (FMEC)*, Paris, France, 20–23 April 2020. 2020.

8. НД ТЗІ 2.7-011-2012 «Захист інформації на об'єктах інформаційної діяльності. Методичні вказівки з розробки Методики виявлення закладних пристроїв», 2012, 12с.

9. Yu J. An Empirical Study of Denial of Service (DoS) against VoIP. *2016 15th International Conference on Ubiquitous Computing and Communications and 2016 International Symposium on Cyberspace and Security (IUCC-CSS)*, Granada, Spain, 14–16 December 2016. 2016.

10. Buriachok V., Sokolov V., Mahyar T. D. Research of caller id spoofing launch, detection, and defense. *Cybersecurity: Education, Science, Technique*. 2020. Vol. 3, no. 7. P. 6–16.

11. Tas I. M., Baktir S. Blockchain-Based Caller-ID Authentication (BBCA): A Novel Solution to Prevent Spoofing Attacks in VoIP/SIP Networks. *IEEE Access*. 2024. P. 1.

12. Лізунов, А. О. Захист VoIP-телефонії в телекомунікаційних системах: пояснювальна записка випускника освітнього ступеня бакалавр, спеціальність 172 Телекомунікації та радіотехніка, 2021. 57с.

13. Bello, M. Z., Buhari, B. A., Bodinga, B. A., & Umar, M. M. (2022). Secure and Optimize VoIP Communication Using QoS Technologies and VPN. *Journal of Network Security and Data Mining*, *5*(3), 9-19.

14. End-to-End Detection of Caller ID Spoofing Attacks / H. Mustafa et al. *IEEE Transactions on Dependable and Secure Computing*. 2018. Vol. 15, no. 3. P. 423–436.

15. The Terminal Access Controller Access-Control System Plus (TACACS+) Protocol / T. Dahm et al. RFC Editor, 2020.

16. Szilagyi, D., Sood, A., & Singh, T. (2009). Radius: A remote authentication dial-in user service. *Rivier Academic Journal*, *5*(2), 1-12.

17. Cisco IP Telephony. Solution Reference Network Design. (SRND). Cisco CallManager Release 4.1. April 2005. 510 p.

18. IBM system in IP telephony and integrated collaboration / ed. by F. Jose, International Business Machines Corporation. International Technical Support Organization. [United States] : IBM, International Technical Support Organization., 2008. 228 p.

19. Uhl T. QoS by VoIP Under Use Different Audio Codecs. *2018 Joint Conference - Acoustics*, Ustka, 11–14 September 2018. 2018.

20. VoIP Capacity Analysis in Full Duplex WLANs / W. Kim et al. *IEEE Transactions on Vehicular Technology*. 2017. Vol. 66, no. 12. P. 11419–11424.

21. Srihari V., Kalpana P., Anitha R. Spam over IP telephony prevention using Dendritic Cell Algorithm. *2015 3rd International Conference on Signal Processing, Communication and Networking (ICSCN)*, Chennai, India, 26–28 March 2015. 2015.

22. Vennila G., Supriya Shalini N., Manikandan M. Performance analysis of VoIP spoofing attacks using classification algorithms. *2014 Applications and Innovations in Mobile Computing (AIMoC)*, Kolkata, 27 February – 1 March 2014. 2014.