УДК 004.056.5

МЕТОДИ ЗАХИСТУ ІНФОРМАЦІЙНИХ ДАНИХ КОРИСТУВАЧІВ В СФЕРІ VOICE OVER IP

Черкашинов Т.К.
Науковий керівник - старший викладач В'юхін Д.О.
Харківський національний університет радіоелектроніки, каф. БІТ,
м. Харків, Україна
e-mail:tymur.cherkashynov@nure.ua

Voice over IP telephony, which is replacing telecommunications and is becoming more common every day among companies that deal with telephone communications. Since VoIP is an Internet protocol, it has several vulnerabilities that depend on the use of data transfer protocols from VoIP service providers. He is also susceptible to many attacks (DoS, man-in-the-middle attack). The transition to VoIP has not created the opportunity for such attacks, but it may make them easier to execute. The main objective of this work will be to analyze the VoIP system and its data transmission protocols, consider potential risks for attacks and apply preventive measures to complicate or eliminate the possibility of attacks. Another important task is to ensure confidentiality for VoIP users.

Оскільки з часом поширеність використання VoIP сервісів тільки зростає, відповідно зростає попит користувачів та увага зловмисників до цього сервісу. Потреба в захисті особистих даних користувачів, а також в захисті постачальників від перевантаження мережі зростає з кожним днем, тому для забезпечення стабільної роботи VoIP сервісів та конфіденційності особистої інформації користувачів виникає потреба в аналізі, впровадженні та удосконалені систем та методів захисту як під час передачі трафіку, так і під час збереження інформації (історія та записи дзвінків, тарифікація клієнтів, історія змін тощо).

В сучасному світі існує безліч компаній, які так чи інакше пов'язані з Voice over IP (VoIP): це можуть бути компанії, які займаються налаштуванням цього трафіку, або компанії, чиї співробітники безпосередньо користуються Voice over IP трафіком. Безпека даного методу зв'язку дуже актуальна в наш час: через Voice over IP передається багато особистої інформації– починаючи від одноразових кодів аутентифікації через СМС та закінчуючи бесідами співробітників компанії на теми, оприлюднення яких може стати перевагою для компанії-конкурента.

Головною метою цієї роботи є розглядання, аналіз та пошук способів удосконалення для найпоширеніших методів захисту в сфері Voice over IP трафіку. Для розгляду ми охопимо усі розділи VoIP трафіку:

1. Протоколи передачі даних(SIP, TCP тощо): будуть розглянуті переваги та недоліки найбільш актуальних на даний момент часу протоколів, їхнє призначення та методи захисту від потенційних атак;

2. Сервери, які займаються структуруванням та збором даних; тарифікації услуг, обробкою платежів та виставленням платежів абонентам– білінги: без існування білінгу дуже важко уявити собі будь-якого оператора зв'язку. Оскільки білінг-сервери у більшості випадків є серверами з базами даних, які зберігають велику кількість даних(дані о дзвінках чи СМС, тарифи та дані про операторів дзвінків) та є найбільш пріоритетними через велику кількість конфіденціальної інформації, захист білінг-серверів є однією із найголовніших задач під час аналізу безпеки VoIP-мережі;

3. Сервери, які безпосередньо займаються передачею трафіку(наприклад, RTP-сервери): Захисту цих серверів також повинно приділятися багато уваги, оскільки саме через ці сервери йде трафік у реальному часі. Тож перевантаження цього серверу буде нести великі збитки для компанії, тому що це буде означати, що живий трафік, який надходить від клієнтів, не буде оброблятися через перевантаженість серверу.

Окрім указаних вище методів ми розглянемо та проаналізуємо найпоширеніші види загроз та атак на VoIP мережі, такі як:

1. Атаки типу чоловік посередині(man-in-the-middle attack, MITM attack): атака, яка спрямована на перехоплення трафіку, методологією якого є підключення до вже існуючих каналів зв'язку. Використовується для прослуховування та отримання конфіденційної інформації, або зміни переданої інформації з метою отримання потрібних відповідей від учасників розмови;

2. Атаки типу відмова в обслуговуванні(Denial of service attacks): мета такого типу атак– зробити сервіс недоступним для користувачів. Для VoIP методами таких атак є відмовлення сервісу через флуд дзвінків/СМС;

3. Шкідливе ПЗ та вірусі: оскільки VoIP є інтернет сервісом, існує вірогідність зараження шкідливим ПЗ(сніфери, черв'яки, шкідливі макроси тощо).

Метою розглядання атак на Voice over IP є їх аналіз та приведення заходів для мінімізації фактору ризику виникнення таких атак, або виконання заходів, які унеможливлюють їх проведення. Перш за все ми повинні розглядати можливість та основні ознаки певної атаки:

1. Man-in-the-middle attack: найбільш очевидною ознакою цієї атаки розриви у часі відповіді – під час розмови двох сторін дії двох користувачів можуть займати різну кількість часу під час виконання однакової дії з двох сторін. Така прірва у часі обробки запиту може позначати перехоплення та/або зміну даних зловмисником, що прослуховує дану розмову. Методи захисту від цих атак різні. Наприклад, користувачі та оператор мають користуватися захищеними протоколами HTTPS, оскільки під час користування протоколом HTTP зловмисник має змогу зробити підміну сайту. HTTPS протоколи мають свій SSL-сертифікат, що не дає змоги зловмиснику зробити підміну сертифікату, оскільки ліцензіати одразу фіксують підозрілу активність сайту та можуть заблокувати сертифікат тому що дорожать власною репутацією. Також

важливим кроком забезпечення безпеки є використання багатофакторної аутентифікації. Однак найбільш ефективним та важливим рішенням буде моніторинг мережі на ознаку підозрілої активності: це можуть бути сліди зламу, або виявлення третьої сторони з дампу дзвінка.

2. DoS: характерними ознаками для цієї атаки є перевантаження мережі великою кількістю запитів. Одним з рішень для захисту від такої атаки є обмеження кількості запитів від одного користувача(чудовим прикладом є використання rate функції веб серверу Nginx) а також аналіз цих запитів із виявленням IP, який намагається перевантажити сервіс. Після виявлення IP з якого зловмисник надсилає велику кількість запитів(наприклад, навантаження 600 запитами у секунду нашого RTP-серверу, який здатен підтримувати до 700 одночасних дзвінків).

3. Шкідливе ПЗ: ознак для даного пункту існує безліч: від навантаження серверу при відсутності запитів до видалення важливих для системи компонентів. Засоби захисту в цьому пункті повинні застосовуватися майже завжди: на серверному обладнанні повинно бути встановлено підтримувальні та регулярно оновлюванні версії ОС з метою мінімізації зламу через вразливості старих операційних систем. Також дуже важливе правильне налаштування фаерволу серверу, яке буде блокувати підключення з неавторизованих IP адрес. Дані для доступу до серверу повинні ретельно охоронятися, а співробітник компанії мають бути уважними під час роботи: не допускається з’єднання по небезпечним протоколам(тільки HTTPS) а також поширення конфіденційної інформації незнайомим користувачам, або тим, хто видає себе за авторизованих спіробітників/клієнтів.

Також важливою метою буде дотримання балансу між затратами на забезпечення безпеки та вірогідністю проведення атаки.

Список використаних джерел

1. «Стратегії кіберстійкості: управління ризиками та безперервність бізнесу». 2021. https://duikt.edu.ua/ua/lib/1/category/742/view/2173#page=51

2. Detection of Intruders and Flooding in VoIP using IDS, Jacobson Fast and Hellinger Distance Algorithms. 2020. https://www.researchgate.net/publication/3301407_Detecting_VoIP_Floods_Using_the_Hellinger_Distance

3. Involved Security Solution in Voice over IP Networks. 2023. https://www.ajrt.dz/index.php/ajrt/article/view/110

4. «Защита информации В IP-телефонии». А. А. Замула, Ю. С. Павленко. с.191–194. 2001. https://openarchive.nure.ua/handle/document/17305