УДК 004.4

ОГЛЯД SIP-АТАК У VOIP-МЕРЕЖАХ

Федоров С.О., Новогрудська Р.Л.
Навчально-науковий інститут телекомунікаційних систем
КПІ ім. Ігоря Сікорського, Україна
E-mail: alternative1398@gmail.com

OVERVIEW OF SIP BASED ATTACKS IN VOIP NETWORKS

The study is devoted to the analysis of typical attacks on VoIP networks using the SIP protocol. With the growing popularity of VoIP networks, the risks associated with the security of these networks are also increasing, creating new challenges and the need to improve protection methods.

Session Initiation Protocol (SIP) - протокол ініціювання сеансу - текстовий сигнальний комунікаційний протокол, який використовується для створення, керування та завершення кожного сеансу. Він відповідає за безперебійну передачу пакетів даних через мережу. Він розпізнає запит користувача на здійснення дзвінка, а потім встановлює з'єднання між двома або більше користувачами. Після завершення дзвінка сеанс завершується. Він працює разом з іншими протоколами прикладного рівня, які ідентифікують і передають носії сеансу.

[1] визначає різні типи повідомлень, які може підтримувати SIP. Повідомлення SIP в основному поділяються на дві категорії: Запити та Відповіді. Деякі з підтримуваних запитів і відповідей SIP наведені в таблицях 1 і 2.

Таблиця 1. Запити SIP.

Запит SIP	
INVITE	Ініціювання сессії
BYE	Завершення сессії
OPTIONS	Визначення SIP-повідомлень та кодеків які розуміє UA або сервер
REGISTER	Реєстрація місцезнаходження користувача SIP
ACK	Підтвердження відповіді на запит INVITE
CANCEL	Скасувати запит INVITE (при очікуванні відповіді)
NOTIFY	Надання інформації про зміну стану, що не пов'язана з конкретною сесією
REFER	Трансфер двізнків та контакт із зовнішніми ресурсами

Таблиця 2. Відповіді SIP.

Відповідь SIP	
100 Trying	Вказує на те, що довірена особа отримала запит INVITE і обробляє його.
180 Ringing	Команда INVITE надіслана до адресата
200 OK	Сесію зв’язку створено
401	Відповідь на запит REGISTER, якщо користувач не авторизований. Не надає коректну аутентифікаційну інф-ю
403	Сервер зрозумів запит, але відмовляється його виконувати
407	Запит вимагає автентифікації користувача. Ця відповідь видається проксі-серверами
408	Відсутність відповіді на запит протягом певного часу
503	Сервер недоступний. Запит наразі виконати неможливо

Очікування щодо безпеки та конфіденційності в мережах VoIP еквівалентні вимогам до PSTN(класичних телефонних мереж), але надання захищених інтернет-послуг є набагато складнішим. SIP-повідомлення можуть містити інформацію, яку користувач або сервер бажають зберегти в таємниці.

Гнучкість і багатий набір функцій IP-телефонії на основі протоколу SIP порівняно з традиційною телефонною мережею пов'язані з додатковими ризиками для безпеки. Система IP-телефонії на основі SIP вразлива як до загальних інтернет-атак, так і до атак, специфічних для SIP. Оскільки розробка SIP в першу чергу була зосереджена на розширенні функціоналу і сумісності, існує багато можливостей для роботи над безпекою SIP.

Основні типи атак з використанням протоколу SIP можна класифікувати наступним чином [2] :

1. Підміна реєстрації SIP

SIP - це протокол управління на прикладному рівні, який може встановлювати, змінювати або завершувати користувацькі сесії. У SIP та інших протоколах VoIP, користувач користувацький агент (UA)/IP-телефон повинен зареєструватися на SIP-проксі/реєстраторі (вузлі керування), що дозволяє проксі спрямовувати вхідні дзвінки на телефон. Підміна реєстрації відбувається коли зловмисник видає себе за дійсного користувача перед реєстратором і замінює законну реєстрацію на власну адресу. Ця атака призводить до того, що вхідні дзвінки, призначені для зареєстрованого користувача, перенаправляються на несанкціоновану адресу.

2. Модифікація SIP-повідомлень

SIP-повідомлення не мають вбудованого механізму цілісності. Виконуючи одну з атак типу «людина посередині»(man-in-the-middle) [3] (підміна IP-адреси, підміна MAC-адреси, реєстрація SIP), зловмисник може перехопити і модифікувати SIP-повідомлення, змінюючи деякі або всі атрибути повідомлення. Це може включати в себе підміну абонента, якому телефонують, в повідомленні про початок сеансу повідомлення, створюючи у жертви враження, що вона дзвонить одній людині, в той час як система з'єднує його з іншою. Змінивши SIP повідомлення, зловмисник може видати себе за абонента або перенаправити виклик за іншою адресою.

3. Скасування\завершення виклику

Зловмисник може створити SIP-повідомлення з командою Cancel або Bye і відправити його на кінцевий вузол (телефон) щоб завершити поточну розмову. Якщо зловмисник надсилає безперервний потік таких пакетів на телефон, телефон не зможе здійснювати або приймати дзвінки. Це може бути поширено на

на велику кількість телефонів, що призведе до загальносистемного збою в роботі.

4. Неправильна команда SIP

Протокол SIP покладається на hypertext markup language протокол (HTML), для передачі командної інформації. Це робить протокол SIP дуже гнучким і розширюваним для реалізації функцій VoIP. Недоліком є те, що стає дуже складно протестувати роботу SIP з усіма можливими вхідними даними. Зловмисники можуть використовувати ці вразливості, як тільки вони їх знайдуть, формуючи пакети з неправильно сформованими командами і відправляючи їх на вразливі вузли. Це призведе до погіршення роботи або виведення з ладу атакованого вузла, що зробить частину або всю систему VoIP недоступною. Це важко виправити з точки зору перевірки на помилки аналізатора повідомлень. Численні помилки та їхні експлойти, що з'являються в результаті в інтернет-браузерах показують, наскільки складно протестувати кожне можливе повідомлення, яке може бути надіслане [4].

Висновки. VoIP-мережі, як і будь-які інші мережі, піддаються атакам з боку зловмисників. SIP-протокол є однією з основних цілей цих атак.

Основні типи атак включать в себе різні способи махінацій пов’язаних з SIP, такі як підміна реєстрації SIP, модифікація SIP-повідомлень, скасування\завершення виклику, неправильні команди SIP та інші.

Важливою частиною управління мережею VoIP є збереження конфіденційності та цілісності даних, підвищення відмовостійкості, та здатність запобігати загрозам у реальному часі.

Вивчення та дослідження механізмів дій зловмисників є актуальним та важливим напрямком дослідження, що дозволить знайти способи для того щоб убезпечити широко використовувані нині VoIP-мережі, які використовують протокол SIP, від неправомірних дій.

Література

1. IETF Network Working Group. 2016. SIP: Session Initiation Protocol. Retrieved September 21, 2016. https://www.ietf.org/rfc/rfc3261.txt
2. M. Zubair Rafique, M. Ali Akbar and Muddassar Farooq. Evaluating DoS Attacks Against SIP-Based VoIPSystems, 2010, Global Telecommunications Conference.
3. David Butcher, Xiangyang Li, and Jinhua Guo. Security Challenge and Defense in VoIP Infrastructures, 2007, IEEE TRANSACTIONS ON SYSTEMS, MAN, AND CYBERNETICS.
4. Abdirisaq M. Jama, Othman Omran Khalifa. Review of SIP based DoS attacks, 2016, International Journal of Computer Applications Technology and Research.