УДК 621.391

АНАЛІЗ І КЛАСИФІКАЦІЯ АТАК В МЕРЕЖАХ IP-ТЕЛЕФОНІЇ НА БАЗІ SOFTSWITCH CLASS V

Романов О.І., Гордашник Є.С.
Інститут телекомунікаційних систем НТУУ «КПІ», Україна
E-mail: a_i_romanov@mail.ru; gordashnik@ukr.net

Analysis and attack classification in VoIP networks based on Softswitch class V

Ensuring security in VoIP network needs investigation of its vulnerabilities and attacks which pose a threat for stable network functioning. In this paper the most common and widespread attacks have been reviewed and analyzed. Classification and ensuring VoIP security method have been proposed.

Останнім часом оператори IP-телефонії, стрімко розвивають функціональність своїх послуг, надаючи користувачам все більш зручні та гнучкі можливості здійснення дзвінків, конференцій, колл-центрів. Разом з цим, з'явилося велика кількість вразливостей і атак, націлених на крадіжку особистих даних, перехоплення і запис розмов, доведення до відмови в обслуговуванні Softswitch, від яких провайдери послуг IP-телефонії все ще не захищені [1].

Існуючі види атак на безпеку мереж IP-телефонії можна розділити на 3 основні категорії [2]:

1. Атаки на сигналізаційну сесію - перехоплення, зміна тексту повідомлення і відправка його до Softswitch.
2. Атаки з метою розкриття змісту голосових повідомлень - перехоплення голосових потоків, запис і прослуховування.
3. Атаки на елементи мережі IP-телефонії, орієнтовані на відмову в обслуговуванні.

Структура мережі і принцип здійснення атак на елементи мережі IP-телефонії, показано на рис.1.

Розглянемо особливості проведення атак.

Перший клас атак - *атаки на сигналізаційну сесію*. Їх можна розглядати за наступними напрямками:

- руйнування сесії (TearingDownSessions)
- фальсифікація тіла повідомлення (TamperingwithMessageBodies)
- перехоплення реєстрації (RegistrationHijacking)
- голосовий фішинг і спам (SPIT - spamoverInternettelephony або VAM - voice / VoIPspam)

Принцип *руйнування сесії* (Tearing Down Sessions) полягає в тому, що хакери перехоплюють запити від різних абонентів і відправляють повідомлення BYE у відповідь (як якби він прийшов від проксі - сервера або іншого мережевого елемента). Це дозволяє завершити сесію достроково і обмежити доступ до послуг.

Атаки такого роду можуть бути запущені від окремих осіб, оскільки так набагато легше почати DoS атаку проти мережевих елементів і мережі в цілому, з набагато більш руйнівними і далекосяжними наслідками.

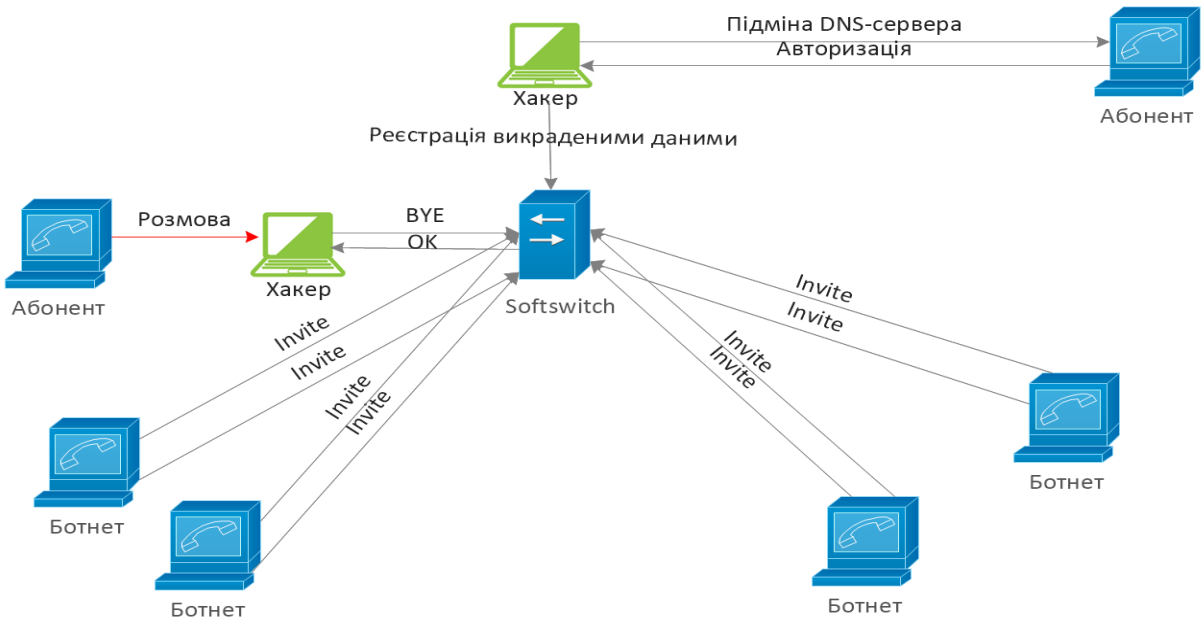

Рис.1.

Фальсифікація тіла повідомлення проводиться таким чином. Так як SIP повідомлення передаються в текстовому форматі (рис.2), тому шахраям абсолютно не обов'язково мати декодер для маніпуляції з повідомленнями. Просте захоплення повідомлення дає можливість втрутитися в роботу мережі. Як тільки хакер захопив повідомлення, тіло повідомлення і заголовки в протоколі SIP можуть бути змінені і використані зловмисником в своїх цілях.

Наприклад, хакер може захопити повідомлення INVITE (рис.2), що передається від абонента, і змінити його заголовок. Наприклад - адресу джерела, замінити своєю власною адресою. Це дозволяє хакеру підключатися до мережі, до якої він не має прав доступу. А далі, ініціювати сесію з іншими абонентами, видаючи себе кимось іншим.

```
INVITE sip:923406515540@192.95.30.203:5060;user=phone SIP/2.0
Allow: INVITE, ACK, BYE, CANCEL
Call-ID: sbcsipuac.2_66.33.182.50_b04sb13_1_1_2014111216265350_1758875847_402791
Contact: <sip:52710189@66.33.147.146:5060>
CSeq: 1001 INVITE
From: <sip:52710189@66.33.147.146:5060>;tag=1758875847_C
Max-Forwards: 70
P-Asserted-Identity: <sip:52710189@66.33.147.146:5060>
Privacy: none
To: <sip:923406515540@192.95.30.203:5060>
Via: SIP/2.0/UDP 66.33.147.146:5060;branch=z9hG4bK_1758875847_1957_1
Content-Type: application/sdp
Content-Length: 209
```

——— IP-адреса Softswitch

——— IP-адреса абонента, що ініціював виклик

Рис.2. Структура повідомлення Ivite

Є й інші типи атак, в яких застосовується фальсифікація повідомлень. Так хакер може перехоплювати SMS-повідомлення та змінювати їх зміст. Це може бути особливо небезпечно, якщо повідомлення були послані з боку державних органів.

Перехоплення реєстрації (Registration Hijacking) дозволяє зловмисникові добути інформацію про користувача, яка міститься в SIP повідомленні. Вона в подальшому може бути використана для авторизації і аутентифікації в мережі і користування її сервісами.

Спроба реєстрації зловмисника буде виглядати, ніби абонент змінив своє місце розташування і шле новий запит реєстрації (повідомлення REGISTER). Після вдалої реєстрації, всі дані які були призначені абонентському пристрою користувача, будуть направлятися до зловмисника, що дозволить використовувати ресурс мережі користувачем, що не має на це прав. Такий вид атаки найбільш поширений в наші дні.

Голосовий фішинг і спам (SPIT - spamoverInternettelephony або VAM - voice / VoIPspam) може бути двох типів. Перший - користувач замість того, щоб працювати, слухає рекламу. Другій - абонент отримує пропозицію зателефонувати на «сервісний» номер (на кшталт Pay Pal) для уточнення деяких питань. У підсумку, оплата йде за збільшеним тарифам та розкриває персональні дані. SPIT і фішинг ще не стали масовим явищем, але вже помічені, і обсяги збільшуються.

Таким чином, для того щоб забезпечити режим нормального функціонування IP - мереж, необхідно застосовувати методи захисту, такі як, наприклад, шифрування даних і протидія DDOS-атакам. А для цього необхідно вивчення різних видів атак, їх класифікація та детальне формалізоване описання. У лабораторії кафедри Телекомунікацій проводиться збір і узагальнення такого виду інформації на макеті ділянки мережі з реальним обладнанням.

Виявлено, що однією з найбільш небезпечних видів атаки з метою виведення з ладу сервера є атака з використанням запиту Invite. Такий тип запитів найбільш трудомісткий, тому що змушує Softswitch звертатися до бази даних і порівнювати іноді цілий ряд параметрів. А це потребує часу до 300 мс. У порівнянні обробка запиту Register, займає 45 мс.

Література

1. An Improved SIP Security Mechanism of Softswitch Network // Q. Lu, C.G. Zhang – 2013 – 3с
2. A Comprehensive Survey of Voice over IP Security // Angelos D. Keromytis, Senior Member, IEEE - 2012 – 24с
3. A Comprehensive Survey of Security Issues and Defense Framework for VoIP Cloud // Ashutosh Satapathy, L. M. Jenila Livingston, School of Computing Science and Engineering, VIT University, Chennai - 600127, Tamil Nadu, India- 2015 – 13с