УДК 621.395.74

ЗАХИСТ ГОЛОСОВИХ ДАНИХ В ПРОГРАМНО-АПАРАТНОМУ КОМПЛЕКСІ ASTERISK

Ткачук А. О., Могилевич Д. І.
Інститут телекомунікаційних систем НТУУ «КПІ», Україна
E-mail: Dumenko.ann@gmail.com

Protection of voice data in hardware-software solution Asterisk

This article describes the main types of confidential information threats in Asterisk IP-telephony systems and proposes a set of measures to protect the voice data from malicious attacks.

Важливою подією в історії телекомунікацій стала поява технології передачі голосу по IP-мережі. Використання VoIP є сучасною тенденцією, це зручно, дешево, оскільки можна об’єднати віддалені офіси, не звертаючись до послуг операторів телефонного зв’язку [1]. Однією з таких VoIP технологій є програмно-апаратний комплекс Asterisk.

Asterisk є відкритою платформою марки Digium, що працює з різними операційними системами (Linux, Windows, FreeBSD, OS X) і дозволяє будувати і модифікувати телефонну станцію малих і середніх розмірів. Відкрита платформа означає ліцензійну програму з початковим текстом, не пов’язаним обмеженнями на подальшу модифікацію. Asterisk має усі функції класичної АТС, і навіть більше [2].

На сьогоднішній день, інформація є одним з найцінніших ресурсів, тому її захист – дуже важливе завдання. Чималу роль в роботі організації будь-якого рівня грають телефонні переговори. В силу зростаючої популярності IP-телефонії, все гостріше постає питання забезпечення її безпеки в загальному і конфіденційності розмов зокрема.

Знання основних джерел небезпеки для мереж IP-телефонії, а також розуміння методів усунення цих загроз допоможе зберегти репутацію і фінансові ресурси компаніям, що використовують Asterisk [3].

Перехват та маніпулювання даними є одним з найбільш вразливих місць телефонних мереж. У разі застосування IP-телефонії зловмиснику не обов’язково потрібен фізичний доступ до лінії передачі даних. Пристрій перехоплення, що знаходиться всередині корпоративної мережі з великою вірогідністю може бути виявлений, а зовнішнє прослуховування відстежити практично неможливо. Крім того, перехоплені дані або голос можуть бути передані далі зі змінами.

Відмова від використання або спрощення механізмів аутентифікації і авторизації в IP-телефонії відкриває для зловмисника можливість не санкціоновано отримати доступ до системи, підмінивши дані про користувача своїми. Можливий також злом облікових даних користувачів за допомогою перебору або прослуховування незахищених каналів зв'язку. Подібна вразливість може бути використана для здійснення дорогих дзвінків за рахунок

користувача, зводячи нанівець всю можливу вигоду від використання IP-телефонії. Також це може застосовуватися для запису перехоплених дзвінків на носії зловмисника з метою застосування даної інформації в корисливих цілях.

Ще одним з різновидів атак є «відмова в обслуговуванні» (Denial of Service, DoS). Ця атака націлена на перевищення граничного навантаження на систему великою кількістю коротких дзвінків або інформаційного «сміття». Без постійного відстеження ознак подібних атак і застосування пасивних засобів захисту, це призводить до того, що сервери IP-телефонії не справляються із збільшеним навантаженням і не можуть обслуговувати підключених абонентів.

При проектуванні будь-якої комунікаційної системи важливо розуміти, що жодне з самостійних технічних рішень безпеки не в змозі забезпечити абсолютний захист від усіх можливих загроз. Для цього необхідний комплексний підхід.

Ключовими критеріями захищеності інформації можна назвати конфіденційність, цілісність та доступність.

Найголовнішим для захисту інформації є налаштування самого серверу IP-телефонії. Для цього на сервері налаштовуються такі функції: використовується політика складних паролів; налаштовується відключення гостьових дзвінків; використовується система блокування доступу після невдалої спроби реєстрації; обмежуються направлення дзвінків, що доступні абонентам; виконуються регулярні перевірки системи на спробу злому [4].

В комплексі Asterisk також застосовуються міжмережеві екрани. Вони пропускають вихідний трафік від сервера телефонії до SIP-провайдеру і фільтрують вхідний трафік за певними правилами. Раціональним рішенням можна вважати закриття на міжмережевому екрані всіх мережевих портів для IP-телефонії, крім необхідних для її коректної роботи і адміністрування.

Для захисту конфіденційних переговорів і мінімізації можливості потрапляння конфіденційної і комерційної інформації в руки зловмисника, необхідно захистити передані по відкритих каналах зв'язку дані від перехоплення і прослуховування.

Оскільки для здійснення дзвінка клієнт і сервер попередньо обмінюються службовими даними для встановлення з'єднання, дану проблему можна розділити на дві складові - захист службових даних IP-телефонії та захист голосового трафіку. Найкраще використовувати протокол TLS (Transport Layer Security) для захисту SIP сигналів і протокол SRTP (Secure Real Time Protocol) для захисту голосового трафіку. Схема шифрування голосу в IP-телефонії показана на рисунку 1.

TLS - криптографічний протокол, що забезпечує захищену передачу даних між вузлами в мережі, є методом для шифрування SIP-протоколу. TLS забезпечує конфіденційність і цілісність інформації, що передається, здійснює аутентифікацію.

Після встановлення захищеного з'єднання починається передача голосових даних, убезпечити які дозволяє застосування протоколу SRTP. Протокол SRTP є одним з кращих способів захисту IP телефонії на базі IP-АТС

Asterisk. Основна перевага цього протоколу - відсутність будь-якого впливу на якість зв'язку.

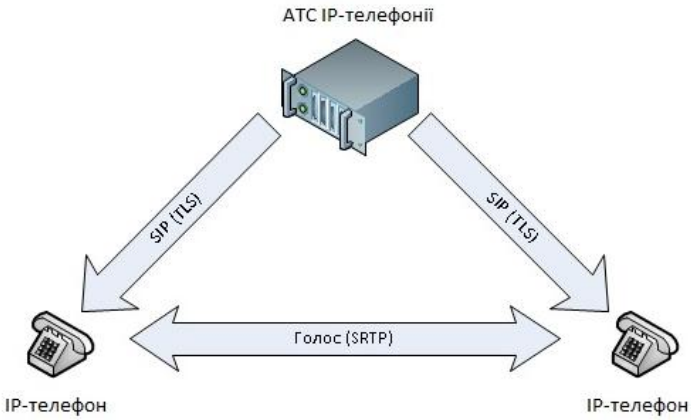

Рис. 1 Шифрування в IP-телефонії.

Але цього захисту може бути недостатньо для організації систем з підвищеними вимогами до захисту IP-телефонії (наприклад, для військових організацій). В таких випадках можна зашифрувати тунель, в якому буде передаватись голос, підключити віддалених користувачів через шифровані тунелі. Зміст перехоплених пакетів, відправлених по шифрованих тунелях буде відомий тільки власникам ключа шифрування. Цей же метод доцільно застосовувати для захисту підключень до постачальників послуг IP-телефонії. Це дозволить надійно передавати дані не лише всередині мережі, а також між віддаленими користувачами.

В роботі було проаналізовано атаки, які можуть загрожувати конфіденційності, цілісності та доступності інформації у VoIP системах. Для запобігання втраті інформації та захисту від можливих загроз, було запропоновано комплексний підхід. Він включає відповідні налаштування серверу VoIP, використання міжмережевих екранів, шифрування телефонних розмов. В результаті проведеного аналізу, пропонується використовувати поєднання протоколів TLS та SRTP для шифрування голосових даних в мережі. А також пропонується передавати голосові дані між віддаленими користувачами через зашифрований тунель. Використання всіх вищенаведених методів в комплексі забезпечить кращу безпеку інформації всередині мережі та з віддаленими користувачами.

Література

1. База знань Asterisk [Електронний ресурс]. – Режим доступу: http://asterisk.ru/knowledgebase.
2. Меггелен Дж., Мадсен Л., Сміт Дж. Asterisk: майбутнє телефонії, 2-е видання, Санкт – Петербург – Москва, 2009. — 652 с.
3. Безпека Asterisk [Електронний ресурс]. – Режим доступу : https://habrahabr.ru/post/188440/
4. Захист IP-телефонії [Електронний ресурс]. – Режим доступу: http://efsol.ru/articles/protection-ip-telephony.html.