Аналіз поточного стану дій в області захищеної IP- телефонії

Гулечко М.С., Джулій В.М., Тітова В.Ю.
Хмельницький національний університет

Протоколи IP-телефонії поділяються на дві великі групи, а саме протоколи передачі медіа інформації по пакетним мережам, а також протоколи управління встановленням з'єднання. В першу групу входить протокол RTP (Real-time Transport Protocol), що працює поверх UDP (User Datagram Protocol) протоколу. Сукупність протоколів RTP / UDP / IP забезпечує транспортний механізм для мовного трафіку. Протоколи другої групи забезпечують управління при обслуговуванні виклику між абонентами. До цієї групи належать протоколи SIP (Session Initiation Protocol), H.323, MGCP (Media Gateway Control Protocol). Протоколи встановлення з'єднання можуть працювати як поверх UDP транспорту, так і по TCP (Transmission Control Protocol). Таким чином, сукупність протоколів (SIP / H.323 / MGCP) / (UDP / TCP) / IP формують сигнальний механізм для передачі мовного і медіа трафіку.

В силу загальнодоступності використовуваних каналів передачі голосової інформації в IP мережах особливої актуальності набуває забезпечення конфіденційності VoIP-сервісів. Для вирішення цього завдання можуть бути використані різні підходи: забезпечення прямого захищеного каналу між кореспондентами (наприклад, VPN-тунель); застосування спеціальних протоколів забезпечення безпеки для IP-сервісів.

Перший спосіб набув широкого поширення при побудові віртуальних корпоративних мереж, але для його реалізації кореспонденти повинні підтримувати VPN-протокол. Однак, багато VoIP-пристрої не підтримують VPN. Тому, для забезпечення безпеки досить часто застосовуються спеціальні протоколи забезпечення безпеки IP-телефонії.

До спеціальних протоколів забезпечення безпеки IP-телефонії відносяться протоколи Secured SIP, SRTP, MIKEY, SDES, ZRTP, DTLS, S-MIME. Ці протоколи можна розділити на 3 категорії: протоколи захисту сигналізації (Secured SIP); протоколи захисту медіаінформації (SRTP); протоколи генерації і розподілу ключів для протоколів захисту медіаінформації (MIKEY, SDES, ZRTP, DTLS).

Протоколи захисту сигналізації призначені для забезпечення безпеки інформації про телефонні номери, підтримуваних кодеків. Для вирішення цього завдання використовується Secured SIP (SSIP, SIP / TLS). Цей протокол працює за аналогією з протоколом HTTPS, організовуючи між кореспондентом і сервером SSL тунель з використанням сертифікатів і відкритого ключа. Всі SIP-повідомлення (сигналізація) передаються з цього тунелю. Недоліком протоколу є необхідність застосування інфраструктури відкритих ключів, що використовується для організації TLS.

Для забезпечення конфіденційності при передачі мови широко використовується захищений протокол реального часу - Secure Real-time Transport Protocol (SRTP), який реалізує функції криптографічного захисту - шифрування і аутентифікації мовних повідомлень на основі алгоритму шифрування AES.

Криптографічний захист пакетів голосової інформації виконується протоколом SRTP в режимі реального часу і не вносить змін в ймовірносно-часові характеристики протоколу RTP. Але для його роботи необхідно попереднє формування криптографічних ключів. Це завдання вирішує протокол розподілу ключів (ПРК).

Рекомендація RFC 3711 описує дві складових - власне протокол SRTP для перенесення і криптозахисту медіа даних, а також протокол SRTCP (Secure Real-time Transport Control Protocol) для управління медіа сесією.

Основними завданнями протоколу SRTP є виконання таких функцій: шифрування переданих голосових даних; аутентифікація переданих повідомлень; захист від передачі повторних пакетів; збереження смуги пропускання, стиснення RTP заголовків.

Основними завданнями протоколу SRTCP є виконання таких функцій: шифрування переданих даних; аутентифікація переданих повідомлень. Аутентифікація і шифрування можуть працювати незалежно один від одного. Таким чином, можливий варіант, коли шифрування вимкнено і SRTP здійснюється виключно з метою аутентифікації. Обмеженням протоколу є те, що аутентифікація повідомлення обов'язкова в SRTP і не може бути відключена.

Протоколи генерації і розподілу ключів для захисту медіаінформації.

Протоколи третьої групи, за аналогією з протоколами розподілу ключів в бездротових мережах, призначені для генерації і розподілу між кореспондентами ключів шифрування медіаінформації. Для вирішення цього завдання можна використовувати протоколи MIKEY, SDES, ZRTP, DTLS.

Протокол обміну ключами MIKEY описаний в рекомендаціях RFC3830 і RFC6309. MIKEY має кілька режимів роботи, що визначають спосіб формування секретного ключа сесії SRTP: режим встановленого ключа, режим відкритого ключа та режим Діффі-Хелмана. Причому другий і третій режими не захищають від атаки вторгнення в середину (MiTM, Man In the Middle) і вимагають реалізації механізму аутентифікації повідомлень. Транспортом для переносу повідомлень протоколу може виступати як SIP / SDP, так і протокол RTSP (Real Time Streaming Protocol). SDES (Session Description Protocol Security) описується в RFC4568. Суть протоколу полягає в тому, що один з кореспондентів передає ключ в SIP повідомленні по сигнальному каналу. Кореспондент отримує його і використовує для шифрування. Однак при цьому обмін сигнальними повідомленнями повинен бути захищений від зловмисника. З цієї причини - SDES може

використовуватися тільки при наявності SIP / TLS захищеного з'єднання з цифровим сертифікатом сервера. Також даний спосіб не забезпечує безпеки з кінця в кінець. Це означає, що якщо з'єднання буде виконуватися через IP АТС, SDES буде виконувати розподіл ключів між кореспондентом А і IP PBX, між кореспондентом Б і IP-телефонною станцією, але не між кореспондентами А і Б безпосередньо.

Протокол DTLS для SRTP описується в RFC 5764. Протокол описує формування медіа-сесій точка-точка з двома учасниками з жорстким фіксуванням портів UDP кореспондента і респондента. Повідомлення протоколу передаються спільно з RTP пакетами. Кожна сесія містить одну DTLS асоціацію і два SRTP контексту (для SRTP і SRTCP). Для організації сесії (DTLS-асоціації) кореспонденти виконують обмін повідомленнями, DTLS handshake. Так як в основі протоколу лежить TLS, що використовує інфраструктуру відкритих ключів (Public Key Infrastructure, PKI), то застосування TLS можливо теж тільки при наявності PKI.

Одним з найбільш перспективних протоколів генерації ключів є ZRTP. Протокол застосовується в додатку для Android CsipSimple, програмних телефонах Jitsi, Phoner, програмних АТС FreeSwitch і Asterisk, апаратних VoIP шлюзах компанії UM-Labs. Відмінною особливістю ZRTP протоколу є можливість забезпечення безпеки від точки до точки, від одного кореспондента до іншого. Завданнями протоколу ZRTP є: генерація ключових параметрів SRTP сесії; забезпечення конфіденційності повідомлень протоколу; забезпечення аутентифікації кореспондентів; захист від атаки вторгнення посередині, як з використанням, так і без використання інфраструктури відкритих ключів.

Протокол передбачає роботу кореспондентів по топології точка-точка, при цьому окремо виділяється можливість застосування протоколу при багатопотоковому режимі, коли необхідно організувати кілька захищених медіа потоків. Крім того, передбачений режим роботи з легітимним посередником, яким може бути, наприклад, корпоративна телефонна станція. Кожен з кореспондентів-учасників протоколу повинен мати встановлений ідентифікатор (ZID), який повинен бути унікальний.

В основі протоколу - обмін ключами по алгоритму Діффі-Хелмана. Особливістю протоколу є передача параметрів всередині RTP пакетів, залишаючи пакети сумісними з RTP / AVP профілем. В цьому випадку, ZRTP-несумісним пристроєм ZRTP-пакети просто відхиляються і не впливають на встановлене з'єднання.

Для аутентифікації кореспондентів, а також виключення атаки вторгнення в середину (MiTM, Man in The Middle), протокол ZRTP передбачає використання короткого аутентифікаційного рядка (SAS, Short Authentication String), а також частини ключового матеріалу від попередніх сесій між кореспондентами. Для контролю цілісності переданих повідомлень

кожне повідомлення ZRTP включає в себе код CRC, а також код аутентифікації повідомлення MAC (Message Authentication Code). MAC обчислюється, як ключова хеш-функція, яка узгоджується на першій фазі протоколу.

Виявлення помилки тільки в хеш-повідомленні, як правило, означає виявлення атаки MiTM, оскільки спотворення за рахунок канальних помилок виявляються і при перевірці CRC ZRTP пакета. Протокол виконується послідовно в чотири фази: виявлення; підтвердження; обчислення ключів; завершення. У загальному випадку, ZRTP працює на самому початку розмови кореспондентів, відразу після завершення роботи протоколу SIP, як починає працювати в сторони протокол RTP

Існуючі дослідження в області робіт із захисту голосових зв'язків можна розділити на кілька категорій, а саме: розробка безпечних систем IP-телефонії; аналіз безпеки, що забезпечується системами IP-телефонії; аналіз безпеки, що забезпечується окремими протоколами VoIP, а також аналіз самих протоколів.

При оцінці впливу протоколів забезпечення безпеки на якість потрібно враховувати особливості IP-телефонії в порівнянні з традиційною телефонією. Так, в традиційній телефонії час відгуку вузла зв'язку, тобто час з початку передачі інформації про заняття абонентської лінії до моменту отримання кінцевим обладнанням сигналу готовності до прийому номера, визначається готовністю станції обслужити виклик. У IP-телефонії цей час визначається кінцевим обладнанням і не залежить від поточного стану телефонної станції.

Необхідно оцінити, як протоколи безпеки IP-телефонії можуть впливати на нормовані показники функціонування мереж телефонної мережі зв'язку. Застосування SIP-S може впливати на норму "втрати викликів" в разі, якщо при сценарії абонент-абонент один з кореспондентів використовує політику безумовного використання SIP-S, а другий не підтримує SIP-S протокол. Деяка затримка додатково може виникати за рахунок часу, необхідного на організацію TLS каналу між кореспондентами, необхідного для роботи SIP-S протоколу.

Протоколи розподілу ключів впливають на час встановлення з'єднання або на час організації захищеного мовного каналу, в залежності від місця спрацювання протоколу в сценарії з'єднання. Так протокол ZRTP може працювати після встановлення з'єднання, починаючи з етапу, коли один з кореспондентів зняв трубку. В цьому випадку, протокол впливає на норму "час встановлення з'єднання". Інші протоколи також вимагають передачу додаткових повідомлень, що може збільшувати значення нормованих параметрів.

Перелік посилань

1. Борисов М. А. Основы программно-аппаратной защиты информации. / М. А. Борисов, И. В. Заводцев, И. В. Чижов. – М.: УРСС: Либроком, 2013. – 370 с.

2. Гольдштейн Б.С. IP-телефония. / Б.С.Гольдштейн, А.В.Пинчук, А.Л.Суховицкий. - М.: Радио и связь, 2015-336 с.

3. Тарнавський Ю. А. Технології захисту інформації: підручник / Ю. А. Тарнавський; КПІ ім. Ігоря Сікорського. – Київ : КПІ ім. Ігоря Сікорського, 2018. – 162 с.

4. Бойко Ю. М. Теоретичні аспекти підвищення завадостійкості й ефективності обробки сигналів в радіотехнічних пристроях та засобах телекомунікаційних систем за наявності завад : монографія / Ю. М. Бойко, В. А. Дружинінін, С. В. Толюпа. - Київ : Логос, 2018. - 227 с.

5. Прикладна криптологія : системи шифрування : підручник / О. Г. Корченко, В. П. Сіденко, Ю. О. Дрейс. – К. : ДУТ, 2014. – 448 с.

6. Шинкарук О.М. Основи функціонування багатоканальних систем передачі інформації: навч. посіб./ О.М. Шинкарук, Ю.М. Бойко, І.І. Чесановський. – Хмельницький : ХНУ, 2011. – 245с.

7. Кодування джерел інформації та каналів зв'язку: навчальний посібник / [Беркман Л.Н., Бондарчук А.П., Гайдур Г.І., Чумак Н.С.]. – Київ: НННТІ ДУТ, 2018. – 91 с.

Інформаційна модель захисту інформації.

Даценко В.С., Тітова В.Ю., Шевчук І.М.
Хмельницький національний університет

Розуміючи інформаційну безпеку як «стан захищеності інформаційного середовища суспільства, що забезпечує її формування, використання і розвиток в інтересах громадян та організацій», правомірно визначити загрози безпеки інформації, джерела цих загроз, способи їх реалізації та цілі, а також інші умови і дії, що порушують безпеку [1]. При цьому, природно, слід розглядати і заходи захисту інформації від неправомірних дій, що призводять до заподіяння шкоди.

Практика показала, що для аналізу такого значного набору джерел, об'єктів і дій доцільно використовувати методи моделювання. При цьому слід враховувати, що модель не копіює оригінал, а є простішою. При цьому, модель повинна бути досить загальною, щоб описувати реальні дії з урахуванням їх складності [2].

Можна запропонувати компоненти моделі захисту інформації на першому (інформаційному) рівні декомпозиції. На нашу думку, такими компонентами інформаційної моделі можуть бути: