УДК 681.3.06

М. В. Васильківський[1]
О. В. Стальченко[1]
Бакіссі Едена Маурісіна Бонже [1]

ПІДВИЩЕННЯ ІНФОРМАЦІЙНОЇ ЗАХИЩЕНОСТІ IP-ТЕЛЕФОНІЇ

[1] Вінницький національний технічний університет;

Анотація

Розглянуті існуючі підходи вирішення актуальних проблеми в області захищеності IP-телефонії. Виконано огляд досліджень в області забезпечення безпеки IP-телефонії. Показано вплив протоколів безпеки на параметри функціонування мережі телефонії.

Ключові слова: бездротові технології, протоколи безпеки, час встановлення з'єднання, IP-телефонія.

Abstract

The considered existent approaches of decision of actual are problems in area of security of IP. The review of researches is executed in area of providing of safety of IP. Influence of protocols of safety is shown on the parameters of functioning of network of telephony.

Keywords: wireless technology, security protocols, connection time, IP.

Вступ

Стандартизація протоколів, а також широке використання персональних комп'ютерів в якості терміналів користувача для послуг IP-телефонії призвели до впровадження широкого кола програм для IP-телефонії, в тому числі програмного забезпечення (ПО) з відкритим вихідним кодом, що забезпечує розширені можливості, зокрема використання додаткових алгоритмів в програмах [1].

Метою дослідження є підвищення рівня захищеності інформації в сеансах безпечної IP-телефонії та скорочення часу встановлення захищеного з'єднання.

Результати дослідження

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 IP-сервісів.

Для забезпечення безпеки досить часто застосовуються спеціальні протоколи забезпечення безпеки IP-телефонії.

Secured SIP (SSIP, SIP / TLS) [3] працює за аналогією з протоколом HTTPS, організовуючи між кореспондентом і сервером SSL тунель з використанням сертифікатів і відкритого ключа. Недоліком протоколу є необхідність застосування інфраструктури відкритих ключів, що використовується для організації TLS.

Для забезпечення конфіденційності при передачі мовних сигналів широко використовується захищений протокол реального часу - Secure Real-time Transport Protocol (SRTP) [5], який реалізує функції криптографічного захисту - шифрування і аутентифікації мовних повідомлень на основі алгоритму шифрування AES. Але для його роботи необхідно попереднє формування криптографічних ключів.

Протоколи MIKEY, SDES, ZRTP, DTLS [2], призначені для генерації і розподілу між кореспондентами ключів шифрування медіаінформації.

При оцінці впливу протоколів забезпечення безпеки на якість зв’язку потрібно враховувати особливості IP-телефонії в порівнянні з традиційною телефонією.

Необхідно оцінити вплив протоколів безпеки IP-телефонії на нормовані показники функціонування систем 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 [4].

Протоколи розподілу ключів впливають на час встановлення з'єднання або на час організації захищеного мовного каналу, в залежності від місця спрацьовування протоколу в сценарії з'єднання. Інші протоколи також вимагають передачу додаткових повідомлень, що може збільшувати значення нормованих параметрів.

Висновки

Розглянуті актуальні проблеми та існуючі підходи їх вирішення в області захищеної IP-телефонії. Зокрема, розглянуті основні компоненти і протоколи IP-телефонії, а також можливі сценарії встановлення з'єднань.

Виконано огляд досліджень в області забезпечення безпеки IP-телефонії, і виявлено відсутність досліджень щодо впливу протоколів безпеки на нормовані параметри функціонування мережі телефонії. Показано вплив протоколів безпеки на параметри функціонування мережі телефонії, виражене в виникненні затримки при встановленні захищеного з'єднання між кореспондентами.

СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ

1. Десницкий, В. А. Обобщенная модель нарушителя и верификация информационно-телекоммуникационных систем со встроенными устройствами/ Десницкий В. А., Чеулин А. А. // Технические науки — от теории к практике. Сб. ст. по материалам XXXIX междунар. науч.-практ. конф. – Новосибирск: Издательство СибАК – 2014. – №10(35) – С. 7-20

2. Ковцур, М.М. Протоколы обеспечения безопасности IP-телефонии. / М.М. Ковцур // Первая миля. – 2012. – №5. – С.18-26.

3. Коржик, В.И. Основы криптографии/В.И. Коржик, В.П. Просихин, В.А.Яковлев - СПб.: СПбГУТ, 2014. - 276 с.

4. Лобашев, А.И. Защита сигнально-управляющего трафика стохастическими методами / А.И. Лобашев А.И., С.В. Баранов С.В., И.В. Симоненко И.В., Е.В. Шалашов //Вопросы оборонной техники. Серия 16: Технические средства противодействия терроризму. - 2015. - № 3-4.- С. 32-34.

5. Ковцур, М.М. Оптимизация вероятностно-временных характеристик криптографического протокола распределения ключей IP-телефонии / М.М. Ковцур // Universum: технические науки. – 2014. – № 2 (3). – С. 1-9..

Васильківський Микола Володимирович — канд. техн. наук, доцент кафедри телекомунікаційних систем та телебачення, Вінницький національний технічний університет

Стальченко Олександр Володимирович — канд. техн. наук, доцент кафедри телекомунікаційних систем та телебачення, Вінницький національний технічний університет

Бакіссі Едена Маурісіна Бонже — студент групи ТКС-18м, факультет інфокомунікацій, радіоелектроніки та наносистем, Вінницький національний технічний університет, Вінниця.

Науковий керівник: ***Стальченко Олександр Володимирович*** — канд. техн. наук, доцент кафедри телекомунікаційних систем та телебачення, Вінницький національний технічний університет, м. Вінниця

Vasylkivskiy Mykola V. — Cand. Sc. (Eng), Assistant Professor of Telecommunication systems and television, Vinnytsia National Technical University, Vinnytsia

Stalchenko Oleksandr V. — Cand. Sc. (Eng), Assistant Professor of Telecommunication systems and television, Vinnytsia National Technical University, Vinnytsia

Bakissi Edena M. — Department of Infocommunications, radio electronics and nanosystems, Vinnytsia National Technical University, Vinnytsia

Supervisor: ***Stalchenko Oleksandr V.*** — Cand. Sc. (Eng), Assistant Professor of Telecommunication systems and television, Vinnytsia National Technical University, Vinnytsia