УДК 681.395

ЗАХИСТ ПРОТОКОЛУ SIP: НОВАЦІЇ ТА НАПРЯМКИ РОЗВИТКУ

Курілко Марина

Вінницький міжшкільний навчально-виробничий комбінат, Україна

Анотація

Визначені основні механізми захисту протоколу SIP, що використовуються в даний час. Запропоновано використання комплексних заходів забезпечення безпеки протоколу та послуг, що на ньому засновані.

Annotation

The basic mechanisms of protection protocol SIP are presented. Proposed use of integrated security tools for SIP protocol and services based on it.

Однією з головних вимог при створенні сучасних систем будь-якого рівня та будь-якого направлення є їх інформаційна безпека. Найкращім для створення системи безпеки є комплексний підхід, в якому вирішуються питання безпеки всіх без виключення IT-сервісів на всіх рівнях функціонування.

З точки зору користувача важливою вимогою до будь-якого сервісу є його якість (QoS – quality of service), яка в широкому сенсі включає конфіденційність, цілісність та доступність інформації. Для забезпечення потрібної якості надання послуг (в тому числі IP-телефонії) з використанням протоколу SIP, можна застосовувати ті самі методи, що і при захисті традиційної передачі даних, а саме - шифрування або VPN.

Проте їх впровадження повинне відповідати спеціальним вимогам до якості голосового зв'язку. Захист інформації в родині протоколів SIP частіше всього реалізовано за допомогою наступних механізмів [1]:

1. Аутентифікація за допомогою дайджеста повідомлення RFC 2617. Використовується алгоритм MD5 для отримання хеш-значення від імені, паролю та URI. Для конфіденційності медіа даних використовують протокол SRTP, а для обміну ключами - SDP RFC 2327.
2. Використання протоколу TLS, який базується на криптографічному протоколі SSL, як для аутентифікації, так і для шифрування даних. Безпосередньо для захисту інформації на базі протоколу SIP розроблено протокол SIPS, який поєднує в собі аутентифікацію та збереження конфіденційності зв'язку за допомогою протоколу TLS.
3. Забезпечення безпеки тіла повідомлення SIP на основі стандарту S/MIME.
4. Використання протоколу IPSec; це дозволяє здійснювати підтвердження достовірності і шифрування IP-пакетів та розподілення ключів ручним методом або за допомогою протоколу IKE (Internet Key Exchange).

Пропонований комплексний підхід до захисту загалом передбачає використання на різних рівнях, до різних об'єктів протоколу SIP, деякого з вищенаведених механізмів.

Правильний вибір як конкретних механізмів, так і їх комбінацій, дозволяє забезпечити ефективність захисту даних при збереженні якості послуги. Наприклад, окремий захист за допомогою хешування заголовку повідомлення SIP, S/MIME захист тіла повідомлення SIP, використання IPSec на міжмережевому рівні і т.ін

Крім того, комплексність підходу передбачає також використання для захисту на системному рівні, наприклад, систем виявлення та запобігання вторгнень (IPS/IDS) як невід'ємної складової [2]. Це дозволяє забезпечити, при належній настройці IPS/IDS, як захист від вже відомих різновидів втручань, так і виявлення ще невідомих.

Потрібно систематизувати всі відомі механізми, їх комбінації, вивчити їх здатність до захисту від атак на протокол, та створити методику вибору системи захисту в залежності від умов експлуатації, набору сервісів, кількості клієнтів тощо.

Вибір основаного на протоколі SIP рішення створення інфраструктури IMS, при належній організації його захисту, надає цій інфраструктурі такі важелі як безпечний та ефективний доступ до високоякісних мультимедійних послуг незалежно від розташування користувача, способу доступу до послуги, програмних та апаратних засобів, які він при цьому використовує.

Список використаних джерел:

1. Литвинов В.В. Сучасний стан захисту інформації в IP-телефоніїї. / В.В. Литвинов, В.В. Казимир, Є.В. Риндич. — Київ: Математичні машини і системи, 2009, № 2. — с.76—84.
2. Ehlert S. Two layer Denial of Service prevention on SIP VoIP infrastructures. / S. Ehlert, G. Zhang, D. Geneiatakis, G.. Kambourakis, T. Dagiuklas, J. Markl, D. Sisalem. — Computer Communications 31 (2008) pp.2443—2456.