УДК 004.49

Цимбал Н.О.
Кіровоградський національний технічний університет

Основні види алгоритмів, специфікації та протоколи IP-телефонії

IP-телефонія є одним із пріоритетних напрямків розвитку телефонного зв'язку. З кожним роком кількість абонентів, які використовують IP-телефонію (VoIP – Voice Internet Protocal) для проведення голосових переговорів, збільшується. Це пов'язано, насамперед, з меншою вартістю передачі даних за допомогою мережі Інтернет. Вже не тільки окремі користувачі, але й цілі підприємства намагаються використовувати Інтернет як основний засіб міжміського зв'язку. Оскільки комерційна інформація звичайно є конфіденційною, питання безпеки такого зв'язку є все більш актуальним.

На відміну від класичної телефонії, де використовується комутація каналів, IP-телефонія базується на мережевих протоколах з комутацією пакетів [1]. У процесі передачі даних по IP-мережі вони проходять через певну кількість недостатньо захищених серверів, до того ж з'єднаних між собою незахищеними каналами. Одночасно IP-телефонія певним чином відрізняється і від звичайної передачі даних IP-мережами. Це пов'язано з необхідністю виконання аналого-цифрових перетворень даних в реальному часі [2, 3]. Зважаючи на необхідність дотримання вимог щодо якості зв'язку, такі перетворення, включаючи стискання, шифрування та інш., повинні відбуватися за мінімально короткий час. Від того, наскільки існуючі системи відповідають усім цим вимогам, залежать, значною мірою, перспективи подальшого розвитку цієї сфери.

IP-телефонія має ряд значних відмінностей від телефонної мережі загального користування, які роблять її особливо вразливою до зовнішнього втручання і ускладнюють застосування існуючих підходів до захисту голосової інформації в мережі Інтернет.

Захист інформації в IP-телефонії базується на використанні спеціальних протоколів захисту інформації (TLS – Transport Layer Security, VPN – Virual Private Network) або додаткових протоколів в межах існуючих протоколів IP – телефонії (SIP – Session Initiation Protocol, специфікація H.323, Skype).

Спеціальні протоколи

Протокол захисту інформації TLS є наступним поколінням поширеного криптографічного протоколу SSL (Secure Sockets Layer), який базується на асиметричній криптографії. Прикладом використання SSL є протокол HTTPS (Hypertext Transfer Protocol Secured). Протокол захисту інформації TLS включає в себе три фази [4]:

1) діалог між двома сторонами для вибору алгоритму шифрування;

2) обмін ключами за допомогою криптосистем з відкритим ключем або автентифікація за допомогою сертифікатів;

3) передача даних, які шифруються за допомогою симетричних алгоритмів шифрування.

Для обміну ключами використовують комбінації алгоритмів RSA (алгоритм розроблений в 80-х роках Р. Райвестом, А. Шаміром та Л. Адлеманом), алгоритм Діффі-Хелмана та DSA (Digital Signature Algorithm). Для симетричного шифрування використовують алгоритми RC2 (Ron's Code 2), RC4, IDEA (International Data Encryption Algorithm), DES (Data Encryption Standart), Triple DES або AES (Advanced Encryption Standard).

Як відомо, ці алгоритми мають свої вразливі місця, які дозволяють застосувати лінійний та диференційний методи криптоаналізу для зменшення кількості операцій порівняно з повним пошуком [5, 6].

Використання VPN дозволяє створити тунель між ініціатором та термінатором. Ініціатор тунелю інкапсулює мережеві пакети в новий пакет. Конфіденційність та цілісність даних досягається за допомогою не тільки шифрування початкових даних, але й усього IP-пакета. Протокол VPN реалізується не тільки програмно, але й апаратно в маршрутизаторах. Робота VPN пов'язана з використанням відкритих ключів [7].

Додаткові протоколи

Всі додаткові протоколи захисту інформації в IP-телефонії можна поділити на два види: відкриті, до яких можна віднести відомі міжнародні специфікації та стандарти, та закриті – протоколи з закритими стандартами. Так, закритим протоколом можна вважати будь-який протокол IP-телефонії, інформація щодо структури повідомлень якого є закритою.

Відкриті протоколи

Серед відкритих протоколів слід виділити такі:

родину протоколів SIP (Session Initiation Protocol), розроблених IETF (The Internet Engineering Task Force);

специфікацію протоколів H.323, розроблену ITU (International Telecommunication Union) для IP-телефонії .

SIP-протокол RFC (Request for Comments) 3261 розроблено на основі протоколу HTTP [8]. Він належить до сьомого рівня моделі OSI. Протокол SIP розроблено спеціально для використання в IP-мережах. Для з'єднання IP-мережі з мережею стільникового зв'язку існує модифікація протоколу SIP – протокол SIP-T, який визначає пряме та зворотне перетворення повідомлень SIP і ТМЗК (телефонних мереж загального користування). В даному протоколі передбачена автентифікація користувачів. Безпосередньо для захисту інформації на базі протоколу SIP розроблено протокол SIPS (Session Initiation Protocol Secured), який поєднує в собі автентифікацію та збереження конфіденційності зв'язку за допомогою протоколу TLS. Він може використовуватися лише в TCP з'єднанні. При цьому виникає необхідність створення сесії та обміну ключами на кожній ділянці мережі, тобто між кожною парою серверів або SIP-шлюзів. При використанні протоколу SIPS у глобальній мережі часові затрати на шифрування стають головною складовою затримки в передачі голосових даних. Протокол SIPS поширюється лише на IP-мережу і не підтримує з'єднання з ТМЗК.

Захист інформації в родині протоколів SIP реалізовано за допомогою п'яти механізмів [9]:

Автентифікація за допомогою дайджеста повідомлення RFC 2617. Використовується алгоритм MD5 для отримання хеш-значення від імені, паролю та URL. Для конфіденційності медіаданих використовують протокол SRTP (Secure Real-time Transport Protocol), а для обміну ключами використовують протокол SDP (Session Description Protocol) RFC 2327.

Забезпечення криптографічної безпеки електронної пошти на основі стандарту S/MIME (Secure/Multipurpose Internet Mail Extensions).

Використання протоколу TLS як для автентифікації, так і для шифрування даних.

Використання протоколу IPSec (протокол для забезпечення захисту даних, що передаються по міжмережевому IP-протоколу); це дозволяє здійснювати підтвердження достовірності і шифрування IP-пакетів та розподілення ключів за допомогою протоколу IKE (Internet Key Exchange).

Використання протоколу IPSec та ручне розподілення ключів.

Специфікація протоколів H.323 орієнтована на інтеграцію з ТМЗК і на відміну від SIP складається з великої кількості інших протоколів. На рис. 1 зображено структуру H.323.

<table>
<tr><td colspan="2">Гарантована доставка інформації за протоколом TCP</td><td colspan="3">Негарантована доставка інформації за протоколом UDP</td></tr>
<tr><td rowspan="2">H.245</td><td colspan="2">H.225</td><td colspan="2">Потоки мови та відеоінформації</td></tr>
<tr><td>Управління з'єднанням(Q.931)</td><td>RAS</td><td>RTCP</td><td>RTP</td></tr>
<tr><td colspan="2">TCP</td><td colspan="3">UDP</td></tr>
<tr><td colspan="5">IP</td></tr>
<tr><td colspan="5">Канальний рівень</td></tr>
<tr><td colspan="5">Фізичний рівень</td></tr>
</table>

Рисунок 1 – Структура протоколу H.323

Для захисту інформації в специфікації H.323 використовують протокол H.235, в якому передбачена автентифікація за допомогою сертифікатів або сигнальних повідомлень. H.235 дозволяє проводити автентифікацію, захист частини службових даних (H.225) чи медіа даних (RTP).

Автентифікація в специфікації H.323 базується на алгоритмах HMAC-SHA1-96, цифрових сертифікатах, створених за допомогою алгоритмів SHA1 та MD5. Конфіденційність медіа трафіка забезпечується завдяки симетричним алгоритмам шифрування DES, 3DES та AES [10].

Для захисту інформації в специфікації H.323 також використовують протокол IPSec в рамках VPN-з'єднання. При цьому шифруються всі дані, але тунель (захищене з'єднання між клієнтом та сервером) створюється тільки між двома кінцевими користувачами або серверами [11, 12].

Закриті протоколи

До закритих протоколів можна насамперед віднести протокол Skype, оскільки він є найпоширенішим представником цього виду протоколів (мережа IP-телефонії Skype вже налічує більше мільярда користувачів). Протокол Skype не відомий широкій громадськості, тобто точно не відомо, за яким алгоритмом іде вибір портів для встановлення сесій і який формат мають службові та інформаційні повідомлення, що, у свою чергу, вважається негативним фактором щодо безпеки інформації. Але аналіз повідомлень протоколу Skype, показав, що Skype використовує TCP та UDP-протоколи для установлення сесій [13, 14].

Недоліком протоколу Skype є необхідність підключення користувачів до мережі Internet для проведення автентифікації (дані також передаються за допомогою мережі Інтернет, навіть, якщо комп'ютери абонентів знаходяться в одній локальній мережі). Що стосується безпосередньо захисту інформації, в Skype використовуються RSA-ключі та шифрування, подібне AES, але офіційних даних щодо алгоритмів шифрування розробник не надає. Відомо тільки, що захист інформації відбувається лише до з'єднання з ТМЗК [15]. Таким чином, розподілена структура мережі Skype вносить досить суттєвий ризик в безпеку переговорів і є одним із дуже впливових факторів, чому Skype не може використовуватися як захищений зв'язок, незважаючи навіть на використання сучасних криптографічних алгоритмів [12, 16].

Висновки

Розглянувши основні види алгоритмів, специфікації та протоколи IP-телефонії, можна зробити висновок, що існуючі системи IP-телефонії реалізують недостатньо високий рівень захисту інформації та використовують відносно нестійкі криптографічні алгоритми або алгоритми, надійність і якість яких не доведена [6]. Використання асиметричних криптографічних схем для генерації ключів збільшує рівень інформаційної небезпеки. Для автентифікації та хеш-функцій, які використовуються при цьому, слід використовувати більш стійкі алгоритми, наприклад, ГОСТ Р 34.10-2001 та ГОСТ 34.11-94, або систему автентифікації, побудовану на стійких симетричних алгоритмах шифрування, наприклад, ГОСТ 28147-89 [17]. Важливим питанням залишається розповсюдження ключів. Але на даному етапі, при відсутності нормативно закріпленої структури обміну відкритих ключів, найліпший рівень конфіденційності можливий при умові безпечного постачання ключів обом сторонам при використанні симетричного алгоритму шифрування [18].

Слід зазначити, що створення комплексного протоколу IP-телефонії, який би підтримував також стільниковий зв'язок, вимагає проведення додаткового дослідження, оскільки мобільні телефони не підтримують передачу даних у форматах, які використовуються в IP-мережах.

Список використаних джерел

1. *Скляр Б. Цифровая связь. Теоретические основы и практическое применение. – М.: Издательский дом «Вильямс», 2003. – 1104 с.*
2. *Гольдштейн Б.С. и др. IP-телефония / Б.С. Гольдштейн, А.В. Пинчук, А.Л. Суховицкий. – М.: Радио и связь, 2001 – 336 с.*
3. *Бабкин В.В. и др. Оптимизационная задача выбора речевого и канального кодирования / В.В. Бабкин, А.А. Ланнэ, В.С. Шаптала // Труды 7-ой международной конференции и выставки ЦОС и ее применения DSPA. – 2005. – С. 28 – 32.*
4. *TLS – Википедия // Википедия – свободная библиотека [Електронний ресурс]. – Режим доступу:* http://ru.wikipedia.org/wiki/TLS.
5. *Баричев С.Г. и др. Основы современной криптографии / С.Г. Баричев, В.В. Гончаров, Р.Е. Серов. – М.: Горячая линия – Телеком, 2001. – 144 с.*
6. *Сравнение стандарта шифрования РФ и нового стандарта шифрования США [Електронний ресурс] / А. Винокуров, Э. Применко. – Режим доступу: http://www.enlight.ru/crypto/index.htm.*
7. *Росляков А.В. и др. IP-телефония / А.В. Росляков, М.Ю. Самсонова, И.В. Шибаева. – М.: Эко-Трендз, 2003. – 252 с.*
8. *Network Working Group Request for Comments: 3261 [Електронний ресурс]. – Режим доступу:* http://www.ietf.org/rfc/rfc3261.txt.
9. *Kuhn Richard D. Security Considerations for Voice Over IP Systems. Recommendations of the national Institute of Standards and Technology / Richard Kuhn D., Walsh Thomas J., Fries Steffen. – NIST Special Publication 800-58, 2005. – 100 p.*
10 *SERIES H: AUDIOVISUAL AND MULTIMEDIA SYSTEMS. Infrastructure of audiovisual services – Systems aspects Security and encryption for H-series (H.323 and other H.245-based) multimedia terminals. ITU-T Recommendation H.235, 2001 – 85 p. [Електронний ресурс]. – Режим доступу:* http://www.itu.int/rec/T-REC-h.
11. *Браун С. Виртуальные частные сети VPN. – М.: Лори, 2001. – 504 с.*
12. *Практические аспекты защиты корпоративных сетей IP-телефонии [Електронний ресурс] / А. Лукацкий. – Режим доступу:* http://www.pabx.ru/publications/more.html?id=723.
13. *Безопасность Skype в корпоративной среде [Електронний ресурс] / А. Доля. – Режим доступу: http://www.citcity.ru/security/articles/.*
14. *Уязвимости Skype [Електронний ресурс]. – Режим доступу: www.pgpru.com.*
15. *Porter T. Practical VoIP security / Porter Thomas, Jan Kanclirz Jr., Rockland MA.: SyngressPublishing Inc., 2006.– 592 p. – Режим доступу:* http://www.skype.co.ua/content/view/90/16/.
16. *Main Page [Електронний ресурс]. – Режим доступу:* http://yate.null.ro/pmwiki/.
17. *Сущность и результаты исследований свойств перспективных стандартов цифровой подписи x9.62-1998 и распределения ключей x9.63-199x на эллиптических кривых [Електронний ресурс] / М.Ф. Бондаренко, И.Д. Горбенко, Е.Г. Качко, А.В. Свинарев, Т.А. Гриненко. – Режим доступу: http://kiev-security.org.ua/box/19/84.shtml/.*
18. *Инфраструктура открытых ключей как основа обеспечения информационной безопасности национальных, ведомственных и коммерческих систем информационных технологий / М.Ф. Бондаренко, И.Д. Горбенко, С.П. Черных и др. // Радиотехника. – 2002. – № 126. – С. 5 – 17.*