УДК 004.46

Ю.А. Мілінчук[1], О.Р. Ярощук[1]
[1]Національний технічний університет «Дніпровська політехніка», Дніпро, Україна

АНАЛІЗ БЕЗПЕКИ ПЕРЕДАЧІ ГОЛОСОВОГО ТРАФІКУ У VOIP

Анотація. Запропоновано спосіб забезпечення безпечної взаємодії в рамках Skype, а саме використання кінцевого шифрування під час передачі голосу та повідомлень. Розроблено програмний засіб, що реалізує зазначений підхід, та підтримує весь необхідний для безпечної взаємодії функціонал.

Ключові слова: *технологія VoIP, конфіденційність, програмне забезпечення. Skype.*

Вступ. Інформаційні технології є невід'ємною частиною сучасного життя і використовуються для вирішення багатьох завдань, наприклад забезпечення віддаленого спілкування абонентів. Йдеться спілкування з допомогою IP-телефонії (VoIP). На початкових етапах ця технологія використовувалася в основному для спілкування звичайних абонентів по всьому світу і на сьогоднішній день спілкування користувачів за допомогою VoIP обчислюється сотнями мільярдів хвилин.

Згодом всі переваги використання IP-телефонії оцінили й інші учасники ринку. В наш час програмні клієнти, які забезпечують спілкування за допомогою IP-телефонії, використовуються не тільки на побутовому, але й на корпоративному рівні. VoIP є повноцінним інструментом ведення бізнесу нарівні зі стільниковим зв'язком, електронною поштою тощо. [1, 2]

Це можна пояснити багатьма факторами:

1. Висока якість передачі голосу.

2. Можливість передачі не лише голосу, а й відео в режимі реального часу.

3. Можливість обміну миттєвими текстовими повідомленнями.

4. Можливість організації відеоконференцій.

З цих причин VoIP сьогодні також використовується на державному рівні. Забезпечення взаємодії органів державної влади за допомогою відеоконференцзв'язку є одним із пріоритетних та стратегічних завдань з інформатизації міста та країни. Однак таке широке поширення VoIP спричинило ряд проблем, найзначніші з яких пов'язані з інформаційною безпекою. [3]

Основний матеріал. У зв'язку з тим, що часто за допомогою IP-телефонії передаються важливі дані корпоративного та державного характеру, забезпечення їх конфіденційності, цілісності та доступності має бути на найвищому рівні.

Це зобов'язує фахівців з інформаційної безпеки в Україні та світі щільно займатися такими питаннями:

1. Аналіз загроз VoIP.

2. Аналіз безпеки взаємодії за допомогою VoIP.

3. Вироблення методик та засобів, спрямованих на забезпечення безпечного спілкування з VoIP.

У цій роботі ми розглянемо один із можливих способів забезпечення конфідиційності під час використання VoIP-клієнта - Skype, а саме скористаємося кінцевим шифруванням, при якому можливість зашифрування і розшифрування мають лише сторони, які спілкуються. [4, 5]

Для забезпечення кінцевого шифрування в Skype необхідно виконати такі етапи:

1. Забезпечити можливість формування сеансового ключа для симетричного шифрування.

2. Забезпечити можливість зашифрування та розшифрування аудіопотоку. [6, 7]

При цьому у зв'язку з тим, що Skype є можливість обміну текстовими миттєвими повідомленнями, необхідно також реалізувати зашифрований обмін повідомленнями.

Для виконання цих етапів необхідно мати можливість програмно ініціювати надсилання повідомлень з метою:

- встановлення сеансового ключа;
- надсилання зашифрованих повідомлень.

Для цього використовуватимемо програмний інтерфейс (API), що надаються Skype. Ця робота є відображенням потреби сучасного суспільства в безпечному спілкуванні за допомогою IP-телефонії та відповідає викликам сьогодення з боку вороже настроєних країн та організацій.

Висновок. Окремо розглянуті проблеми протоколу Skype, найпоширенішого VoIP-клієнта у світі. Показано, що рівень безпеки Skype не є достатнім для безпечної взаємодії для передачі конфіденційних даних. У зв'язку з викладеним у цій роботі запропоновано спосіб забезпечення безпечної взаємодії в рамках Skype, а саме використання кінцевого шифрування при передачі голосу та повідомлень. Було розроблено програмний засіб, що реалізує зазначений підхід, і підтримує весь необхідний для безпечної взаємодії функціонал. В результаті було отримано засіб, що забезпечує безпечне спілкування через Skype.

ПЕРЕЛІК ПОСИЛАНЬ

1. VoIP Security and Privacy Threat Taxonomy. [Електронний ресурс] URL: http://www.voipsa.org/Activities/VOIPSA_Threat_Taxonomy_0.1.pdf (дата звернення: 01.12.2021).

2. Черкасов Д., Основи технології VoIP та IP-телефонії [Електронний ресурс]. URL: http://ekmair.ukma.edu.ua/bitstream/handle/123456789/13473/Cherkasov_Osnovy_tekhnolohii_VoIP_ta_IP_telefonii.pdf?sequence=1&isAllowed=y (дата звернення: 01.12.2021).

3. Himanshu D., Hacking VoIP [Електронний ресурс]. URL: https://ihatefeds.com/No.Starch.Hacking.VoIP.2010.pdf (дата звернення: 01.12.2021).

4. Baset S., Schulzrinne H. An Analysis of the Skype Peer-to-Peer Internet Telephony Protocol. Department of Computer Science Columbia University, New York 2004.

5. Does Skype use encryption? [Електронний ресурс]. URL: https://support.Skype.com/en/faq/FA31/does-Skype-use-encryption?q=security (дата звернення: 01.12.2021).

6. LoopbackAudioDriver. [Електронний ресурс] URL: https://github.com/02strich/LoopbackAudioDriver (дата звернення: 01.12.2021).

7. Microsoft Virtual Audio Device Driver Sample. [Електронний ресурс] URL: https://code.msdn.microsoft.com/windowshardware/virtual-audio-device-3d4e6150 (дата звернення: 01.12.2021).

УДК 004.056.53

С.І. Войцех[1], О.Є. Веріго[1]
[1]Національний технічний університет «Дніпровська політехніка», Дніпро, Україна

ПРОТИДІЯ АТАКАМ СОЦІАЛЬНОЇ ІНЖЕНЕРІЇ

Анотація. Розглянуті атаки соціальної інженерії які зростають за інтенсивністю та кількістю і спричиняють фінансові та іміджеві збитки користувачам і організаціям.

***Ключові слова**: політика безпеки підприємств, атаки соціальної інженерії.*

Вступ. Досягнення цифрових технологій зробили комунікацію між людьми доступною та простішою. Але через це особиста та конфіденційна інформація може бути доступною в Інтернеті через соціальні мережі та онлайн-сервіси, які не мають чітких алгоритмів та методів захисту цієї інформації. Соціальна інженерія є однією з найбільших інформаційних проблем стосовно безпеки у мережі, оскільки використовує природну схильність людини до довіри. Атаки соціальної інженерії спрямовані на введення в оману осіб для виконання дій, які приносять зловмисникам користь, надання їм конфіденційних даних, наприклад, медичних записів, паролів або ж банківських даних жертв їх атак.

Основний матеріал. Атаки соціальної інженерії розповсюджуються в сучасних мережах і є слабким місцем кіберзахисту підприємств та людей. Вони спрямовані на маніпулювання людьми і підприємствами з метою розголошування конфіденційних даних в інтересах кіберзлочинців. Соціальна інженерія ставить під загрозу безпеку усіх мереж, незалежно від надійності брандмауерів, методів криптографії, систем виявлення вторгнень і антивірусного програмного забезпечення [1]. Люди більше довіряють іншим людям, в порівнянні з комп'ютерами або технологіями, тому саме людина є