УДК 621.396:004.7]:004.056

ЗАХИСТ КОНФІДЕНЦІЙНОСТІ РОЗМОВ ПО МОБІЛЬНОМУ ТЕЛЕФОНУ

Катрич О.О.
Науковий керівник – к.т.н., доц. Юрій Ликов
Харківський національний університет радіоелектроніки, каф. КРіСТЗІ,
м. Харків, Україна
тел. +38(066) 785-14-91, e-mail: oleksandra.katrych@nure.ua

Current level of technology and cryptography development implies a wide range of special approaches of getting an unauthorized access to different devices and data they contain, including mobile phones. Confidentiality of phone conversations is highly threatened by spy software, attacks on cellular networks, unreliable messengers, means of acoustic data retrieval etc. However, there is a list of measures that prevent mobiles from illegal access and loosing privacy. Digital and hardware scrambling, high-secured messengers, detection means of acoustic intelligence devices and cryptophones are certain ways to tackle the problem.

Питання конфіденційності телефонних розмов нині особливо актуальне, оскільки у телефонному режимі часто вирішуються важливі ділові питання та озвучується конфіденційна інформація.

Основна мета роботи – проаналізувавши існуючі загрози конфіденційності розмов по мобільному телефону та наявні методи протидії їм сформулювати оригінальний метод захисту. Існує безліч способів перехоплення телефонних розмов і несанкціонованого доступу до мовної інформації, що передається:

1. Шпигунське програмне забезпечення, яке встановлюється на телефон, надає можливість скопіювати або знищити дані, які там зберігаються, у тому числі й отримати доступ до телефонних дзвінків. Приклади: Pegasus, троян FinFisher.

2. Різні способи атак на стільникові мережі, а саме прослуховування через оператора (підключення до комутатора зв'язку), мобільні комплекси перехоплення, підроблені базові станції, підключення до оптоволокна, перехоплення на рівні сигнальної мережі протоколи SS7.

3. Вразливість сучасних месенджерів. Telegram – збирає метадані (IP-адреса користувача, розмови), за замовчуванням розмови та чати не зашифровані, відсутнє наскрізне шифрування, повна історія чатів зберігається у хмарі. Viber і WhatsApp вважаються безпечнішими, бо вони оснащені наскрізним шифруванням, але також збирають метадані.

4. Засоби акустичного зйому інформації, радіоакустичні закладки (РЗП) та ЛСАР, які дозволяють перехоплювати мовну інформацію, навіть без необхідності доступу до телефону або використання програмних засобів.

Сучасні апаратні та програмні засоби дозволяють частково протидіяти переліченим вище загрозам. Методи захисту телефонних розмов:

1. Скремблювання – різновид кодування інформації, передачі по каналам связи. Може бути програмне або апаратне.

2. Використання безпечних месенджерів - Signal, Threema, Wire, Wickr. Головна їхня перевага - наскрізне шифрування (алгоритм AES з 256-бітним ключем), навіть розробники не можуть отримати доступ до даних користувачів, а також не зберігають історію чатів у своїх серверах. Приклад захищеного за багатьма параметрами месенджера -4xSecure. Безпека забезпечується за рахунок [ ]:

- End-2-End шифрування, сервер тільки для транспорту;
- Повідомлення шифруються за допомогою протоколу OTR;
- транспорт захищений за допомогою протоколу TLS.

3. Захист інформації від витоку по акустичному, вібро-акустичному, акусто-оптичному каналам - використання генераторів зашумлення, оснащення приміщень для переговорів (ЕМ екранування стін, звукоізоляція, перевірка на наявність закладних засобів акустичної розвідки, радіомоніторинг РЗП).

4. Криптофони - смартфони, оснащені особливими системами шифрування, які роблять їх потенційно захищеними від перехоплення. Розроблено у Нідерландах. Безпека базується на ОС із системами захисту від несанкціонованого доступу, спеціальних програмах з надійним шифруванням та підключенням пристроїв до мережі захищених серверів.

Ще один перспективний метод захисту конфіденційності розмов по телефону (при використанні месенджерів) - програмний прошарок між мікрофоном та месенджером.

Альтернативне рішення – зробити Bluetooth гарнітуру з другого телефону, який виконував би функцію цифрового скремблювання.

Описані два останні методи перебувають у стані розробки та будуть представлені на конференції.

Список використаних джерел:

1. Ю. А. Тарнавський (2018). Технології захисту інформації. КПІ ім. Ігоря Сікорського.

2. Способи захисту розмов по мобільному телефону від «прослушки» (2017, 25 липня) https://bastion.tv/tri-sposobi-zahistu-rozmov-po-mobilnomu-telefonu-vid-proslushki_n25843

3. Судаков, А. Н. Защита речевой информации на объекте [Текст] // А.Н. Судаков // Защита информации. Конфидент. – 2003. -N4. – С. 46-49с.