УДК 004.056

В. С. Катаєв

АНАЛІЗ ЗАГРОЗ ДЛЯ КОНФІДЕНЦІЙНИХ ПЕРЕГОВОРІВ, ЩО СТАНОВЛЯТЬ МОБІЛЬНІ ТЕЛЕФОНИ

Вінницький національний технічний університет

Анотація

У роботі проаналізовано основні загрози конфіденційності переговорів при використанні мобільних телефонів. Розглянуто ризики радіоперехоплення зв'язку, витоку даних через бездротові мережі, логічні та програмні уразливості, а також шкідливе програмне забезпечення. Показано, що компрометація пристрою створює можливість прихованого доступу до мікрофона, повідомлень та інших даних незалежно від захищеності каналу зв'язку. Наголошено на необхідності комплексних заходів захисту та подальших досліджень у цій сфері.

Ключові слова: конфіденційність розмов, технічний захист інформації, мобільні телефони, інформаційна безпека.

Abstract

The paper analyzes the main threats to the confidentiality of communications when using mobile phones. The risks of radio signal interception, data leakage through wireless networks, logical and software vulnerabilities, and malware are considered. It is shown that device compromise enables covert access to the microphone, messages, and other data regardless of channel encryption. The need for comprehensive protection measures and further research in this area is emphasized.

Keywords: confidentiality of communications; technical information protection; mobile phones; information security.

Вступ

Мобільний телефон може становити серйозну загрозу для конфіденційності переговорів, оскільки є складним електронним пристроєм із постійним бездротовим зв'язком, мікрофонами та програмним забезпеченням, яке може бути вразливим до зовнішнього втручання. Навіть у режимі очікування телефон здатний передавати службові дані мережі або активувати окремі модулі зв'язку, що створює потенційну можливість віддаленого доступу до мікрофона чи інших сенсорів у разі компрометації пристрою шкідливим програмним забезпеченням або через спеціалізовані засоби перехоплення. Крім того, всі сучасні смартфони мають модулі Wi-Fi, Bluetooth, GPS та мобільного зв'язку, які можуть використовуватися для визначення місцезнаходження, збору метаданих або передачі інформації третім сторонам. У результаті мобільний телефон може виступати ненавмисним джерелом витоку інформації під час проведення конфіденційних переговорів, особливо якщо не застосовуються відповідні організаційні та технічні заходи захисту.

Результати дослідження

Мобільні телефони настільки глибоко увійшли в наше повсякденне життя, що більшість людей вже не уявляє свого дня без них. Їх беруть із собою на роботу, у відрядження, на наради та зустрічі, використовуючи для планування, обміну повідомленнями та швидкого доступу до інформації. Багато хто робить це автоматично, навіть не замислюючись про потенційні загрози: смартфон, який завжди поруч, може стати каналом витоку конфіденційної інформації, особливо під час ділових переговорів, де кожне слово має значення. У цій зручності ховається серйозна небезпека — непомітне шкідливе програмне забезпечення може перетворити гаджет на джерело витоку даних, а в деяких випадках несанкціонований доступ до інформації можливий і без шкідливих програм.

Розглянемо та класифікуємо усі можливі загрози, що створює мобільний телефон:

1. Пряме перехоплення комунікацій. До цієї категорії належать загрози, пов'язані з можливістю перехоплення сигналів мобільного зв'язку без безпосереднього доступу до самого телефону.

Перехоплення може здійснюватися безпосередньо з радіоканалу між мобільним пристроєм і базовою станцією оператора за допомогою спеціалізованих технічних засобів, зокрема комплексів імітації базових станцій або систем радіомоніторингу. Після перехоплення сигналу можлива його подальша обробка та декодування, особливо у випадках використання застарілих або вразливих алгоритмів шифрування мережі, таких як GSM-шифри A5/1 та A5/2, або під час примусового переведення пристрою у менш захищені режими роботи мережі [1]. Слід зазначити, що застосування подібних технічних засобів зазвичай потребує спеціалізованого обладнання та доступу до відповідної інфраструктури, тому на практиці такі можливості переважно перебувають у розпорядженні державних органів та спеціальних служб, які використовують їх у межах оперативно-розшукової діяльності.

2. Витік даних через бездротові мережі. До цієї категорії належать загрози, пов'язані з передачею інформації через бездротові інтерфейси мобільного телефону, зокрема Wi-Fi, Bluetooth та мобільний інтернет. Під час підключення до незахищених або публічних Wi-Fi мереж існує ризик перехоплення мережевого трафіку за допомогою засобів аналізу пакетів або атак, що може дозволити отримати доступ до переданих даних або облікових записів [2]. Аналогічно, уразливості або неправильна конфігурація Bluetooth-з'єднань можуть створювати можливість перехоплення сигналів, несанкціонованого підключення до пристрою або отримання доступу до окремих даних. Крім того, навіть у разі використання захищених протоколів зв'язку можуть передаватися службові дані та метадані, які дозволяють встановити факт комунікації, її час, інтенсивність або приблизне місцезнаходження користувача, що також може становити ризик для конфіденційності.

3. Логічні та програмні уразливості. До цієї категорії належать загрози, пов'язані з помилками в програмному забезпеченні мобільного пристрою, операційної системи та встановлених додатків. Вразливості можуть виникати через недоліки в коді, неправильну реалізацію механізмів автентифікації, управління правами доступу або обробки даних, що створює можливість для несанкціонованого виконання команд, підвищення привілеїв чи обходу систем безпеки. Використання застарілих версій операційної системи або програм без актуальних оновлень підвищує ризик експлуатації відомих вразливостей [3].

4. Шкідливе програмне забезпечення. До цієї категорії належать програми, спеціально створені для несанкціонованого доступу, прихованого збору або передачі інформації з мобільного пристрою. Серед них — шпигунські модулі (spyware), трояни віддаленого доступу (RAT), кейлогери та інші типи шкідливого коду, які можуть бути встановлені через фішингові повідомлення, заражені додатки або експлуатацію вразливостей системи. Після інфікування такі програми здатні працювати у прихованому режимі, отримувати доступ до мікрофона, камери, списків контактів, повідомлень і файлів, а також передавати зібрані дані на віддалені сервери без відома користувача [4]. У контексті конфіденційних переговорів це створює ризик прихованого запису розмов, витоку службової інформації та повного компрометування пристрою як засобу зв'язку.

У сучасних умовах, шкідливе програмне забезпечення може розглядатися як одна з найбільш небезпечних загроз для конфіденційних переговорів, оскільки воно здатне забезпечити повний контроль над функціями мобільного пристрою незалежно від рівня захисту мережі. Компрометація пристрою дозволяє здійснювати прихований запис аудіо до моменту шифрування або після його розшифрування, що робить неефективними засоби захисту каналу зв'язку. Потенційний витік інформації можливий, як під час звичайних телефонних дзвінків через мобільну мережу (у тому числі у фоновому режимі), так і під час використання месенджерів із наскрізним шифруванням, таких як Viber чи WhatsApp, оскільки шкідливе ПЗ може отримати доступ до мікрофона на рівні операційної системи. Особливо небезпечним є сценарій прихованої активації мікрофона без відома користувача та без явних ознак роботи пристрою. Сучасне шкідливе ПЗ може працювати у фоновому режимі, мінімізувати системні індикатори, приховувати власні процеси та здійснювати аудіозапис навіть без ініціації дзвінка. У такому випадку телефон, який перебуває у приміщенні під час наради або службової зустрічі, може фактично виконувати функцію несанкціонованого акустичного контролю. Це створює ризик витоку інформації не лише під час комунікації, але й у процесі звичайного обговорення в межах приміщення, що суттєво підвищує рівень загрози порівняно з мережевими атаками. Існують реальні приклади високорівневого шпигунського програмного забезпечення (Pegasus, FinFisher, RCS), які демонструють технічну можливість повного прихованого контролю мобільних пристроїв, включаючи запис аудіо, перехоплення комунікацій та передачу даних без відома користувача. Наприклад, за даними міжнародних розслідувань, Pegasus застосовувалося для

цільового стеження за журналістами, правозахисниками, політиками та представниками бізнесу в різних країнах. Його можливості включали прихований доступ до повідомлень, дзвінків, мікрофона, камери та геолокації без відома користувача.

Висновки

Проведений аналіз свідчить, що мобільний телефон у контексті конфіденційних переговорів є потенційним джерелом багаторівневих загроз, які охоплюють як мережевий, так і програмний та організаційний аспекти безпеки. Найбільш критичними серед них є шкідливе програмне забезпечення та логічні уразливості, оскільки саме вони здатні забезпечити повний прихований контроль над пристроєм і створюють можливість витоку інформації незалежно від захищеності каналу зв'язку. У той час як перехоплення радіосигналу або атаки на бездротові мережі потребують спеціалізованих технічних засобів, компрометація самого пристрою дозволяє здійснювати несанкціонований доступ до аудіоінформації, у тому числі під час звичайного перебування телефону в приміщенні. Наявність реальних прикладів високорівневого шпигунського програмного забезпечення підтверджує практичну реалізованість таких загроз та їх використання у цільових атаках.

Таким чином, проблема забезпечення конфіденційності переговорів із використанням мобільних пристроїв потребує подальших наукових досліджень, спрямованих на розроблення та вдосконалення ефективних методів і технічних засобів захисту, а також удосконалення організаційних заходів мінімізації ризиків.

СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ

1. Mobile Security Threats: A Survey on Protection and Mitigation Strategies [Електронний ресурс]. – Режим доступу: https://sciendo.com/article/10.2478/kbo-2020-0127.

2. A Comprehensive Survey on Mobile Browser Security Issues, Challenges and Solutions [Електронний ресурс]. – Режим доступу: https://www.tandfonline.com/doi/abs/10.1080/19393555.2024.2347256.

3. A Survey on Security Threats in Mobile Operating Systems and Existing Solutions [Електронний ресурс]. – Режим доступу: https://www.ijisrt.com/a-survey-on-security-threats-in-mobile-operating-systems-and-existing-solutions.

4. Cybersecurity Concerns on Mobile Phones: A Systematic Review [Електронний ресурс]. – Режим доступу: https://papers.academic-conferences.org/index.php/iccws/article/view/3272.

Катаєв Віталій Сергійович – асистент кафедри менеджменту та безпеки інформаційних систем, Вінницький національний технічний університет, Вінниця, kataev@vntu.net

Vitaliy Kataiev – assistant of the Department of Management and Security of Information Systems; Vinny-tsia National Technical University , Vinnytsia, kataev@vntu.net