Тип работы: Реферат

Предмет: Информатика

СОДЕРЖАНИЕ
Введение 3
1. Основные уязвимости GSM/DCS 4
1.1. Перехват и расшифровка трафика 4
1.2. Атака через поддельную базовую станцию 5
1.3. Атака на сигнализацию SS7 6
2. Пути повышения безопасности GSM/DCS 8
2.1. Меры операторов связи по модернизации инфраструктуры 8
2.2. Индивидуальные меры защиты пользователей 9
2.3. Альтернативные технологии связи 11
Заключение 14
Список литературы 15

Одной из наиболее актуальных уязвимостей стандарта GSM является слабое шифрование, использующееся для защиты передачи данных между мобильными устройствами и базовыми станциями. В частности, уязвимость, известная под идентификатором CVE-2019-17053, касается алгоритма шифрования A5/1, который был применен в первых версиях GSM-сетей для обеспечения конфиденциальности голосовой связи и передачи данных.
A5/1 был разработан в конце 1980-х годов и изначально считался достаточно надежным для своего времени. Однако с развитием вычислительных мощностей и появлением новых технологий, таких как SDR (Software Defined Radio), эта защита стала уязвимой. Проблема заключается в том, что с помощью доступных инструментов и оборудования злоумышленники могут перехватывать и дешифровывать трафик, передаваемый в сети GSM, что представляет собой серьезную угрозу для конфиденциальности и безопасности пользователей.
Злоумышленники, использующие эту уязвимость, могут получить доступ к аудио- и текстовой информации, передаваемой между абонентами. Это может быть использовано для прослушивания разговоров, чтения текстовых сообщений или сбора другой чувствительной информации, что в свою очередь открывает возможности для мошенничества, слежки или даже манипуляций с мобильными сервисами. Важно отметить, что атака может быть выполнена в реальном времени, что значительно повышает ее опасность.[7]
Стратегия злоумышленника для эксплуатации этой уязвимости обычно включает использование SDR-приемников, которые позволяют перехватывать радиосигналы GSM-сети. С помощью таких устройств злоумышленник может обнаружить трафик между мобильным устройством и базовой станцией, а затем применить различные методы дешифрования, например, с использованием известных методов атак, таких как Known Plaintext Attack (KPA). В этом случае атакующий может воспользоваться тем, что часть данных передается в открытом виде (например, служебные сигналы), чтобы найти ключи шифрования и расшифровать другие сообщения.[3]
Для снижения рисков использования этой уязвимости рекомендуется переходить на более защищенные технологии связи, такие как VoLTE (Voice over LTE) или использовать защищенные мессенджеры с end-to-end шифрованием. Также важно, чтобы операторы связи модернизировали свою инфраструктуру и переходили на более современные и безопасные алгоритмы шифрования. Для пользователей важно избегать использования устаревших мобильных устройств, которые могут работать только с GSM-сетями, и по возможности подключаться к более современным сетям с улучшенной защитой.

1.2. Атака через поддельную базовую станцию

Одной из наиболее серьезных угроз для безопасности мобильных пользователей в сети GSM является

возможность атаки с использованием поддельных базовых станций, также известных как IMSI Catchers. Уязвимость, обозначенная CVE-2018-0134, связана с отсутствием аутентификации базовых станций в стандартном протоколе GSM. В результате этого мобильные устройства могут без какой-либо проверки подключаться к фальшивым станциям, контролируемым злоумышленниками.
IMSI Catcher — это устройство, которое имитирует работу настоящей базовой станции сотовой связи. Оно заставляет мобильные устройства подключаться к нему, якобы в качестве настоящей сети, и таким образом злоумышленник получает возможность отслеживать, перехватывать и манипулировать передаваемыми данными. Основным элементом атаки является получение идентификатора IMSI (International Mobile Subscriber Identity), уникального номера, который используется для идентификации абонента в сети GSM. Эта информация может быть использована для дальнейших атак, таких как перехват вызовов и сообщений, а также для реализации так называемой "человек посередине" атаки (MITM), где злоумышленник может прослушивать или изменять передаваемые данные.[6]

Список литературы

1. Бенедиктов, И. В. Современные угрозы в мобильных сетях и их устранение / И. В. Бенедиктов. – Казань : Казанский университет, 2020. – 220 с.
2. Гусев, Д. А. Уязвимости сотовых сетей GSM / Д. А. Гусев. – СПб. : БХВ-Петербург, 2021. – 256 с.
3. Иванов, П. Н. Мобильные сети и их защита от атак / П. Н. Иванов. – Новосибирск : Сибирское университетское издательство, 2023. – 182 с.
4. Карпов, А. В. Протоколы безопасности в мобильных сетях / А. В. Карпов. – М. : Дело, 2022. – 198 с.
5. Панина, Н. К. Мобильные технологии и безопасность данных / Н. К. Панина. – М. : Инфра-М, 2020. – 312 с.
6. Петренко, А. В. Атаки на сотовые сети: теория и практика / А. В. Петренко. – М. : Альфа, 2021. – 288 с.
7. Романенко, И. В. Безопасность мобильных сетей GSM и 3G / И. В. Романенко. – М. : Наука, 2020. – 340 с.