УДК 004.056

РАЗРАБОТКА АЛГОРИТМА ФАЗЗИНГ-ТЕСТИРОВАНИЯ В СЕТИ GSM С ИСПОЛЬЗОВАНИЕМ ГЕНЕТИЧЕСКОГО МЕТОДА

Алексеенко А.В. (ИТМО),
Научный руководитель – ассистент факультета безопасности информационных технологий Есипов Д.А. (ИТМО)

Введение. В сетях GSM широко используется стандарт передачи мультимедийного трафика по интернет-телефонии (VoIP). Так как технология строится на простом механизме передачи данных по IP, это становится потенциальной мишенью для злоумышленников, которые могут запускать различные атаки вида «отказ в обслуживании» (DoS) с целью нарушения связи, что приводит не только к существенной потере доходов VoIP операторов мобильной связи, но и подрывают надежность инфраструктуры VoIP. Основным вкладом этой работы является разработка алгоритма фаззинг тестирования, способного превентивно обнаружить вредоносные данные, которые потенциально могут попасть на контроллер сети GSM. Обзор рынка, опубликованный в 2020 году, показывает, что VoIP-трафик составляет 49,7% от общего объема голосовой связи. В международном телеком-сообществе сложилась формула 4+2, которая означает, что у многих операторов раньше будут поддерживаться сети 4G и 2G (LTE и GSM), пока не разовьются технологии 5G и 6G. Это значит, что актуальность в разработке и поддержке второго поколения связи не падает.

Современные решения по тестированию мультимедийного трафика не предполагают использование обратной связи для подготовки более результативных тестов, чем и будет отличаться представленное исследование от существующих.

Основная часть.

1) Набор данных и тестовый стенд.

В этом разделе мы описываем наши доброкачественные и нечеткие наборы данных сетевого трафика. Мы обсудим архитектуру нашего тестового стенда, который мы использовали для сбора реального медиа-трафика.

2) Алгоритм фаззинг-тестирования.

Мы представим наш процесс фаззинга, который можно настроить для проведения фаззинга с разной скоростью. Генетический метод фаззинга, основанный на концепциях естественного отбора и генетики, предполагает тестирование сервера с помощью мутаций входных данных и алгоритма обратной связи для выявления наиболее результативных тестовых наборов.

3) Эксперименты и результаты.

В этом разделе мы оцениваем производительность фаззера с встроенным в него алгоритмом. Мы измеряем производительность на основе четырех показателей.

Выводы. В этой работе мы представили эффективный алгоритм фаззинг-тестирования компонент мобильной связи второго поколения, который позволил нам обнаружить ранее неизвестные уязвимости в обработке сетевых пакетов данных от мобильных устройств, тем самым увеличив устойчивость инфраструктуры к атакам вида «отказ в обслуживании» (DoS).

Список использованных источников:

1. 3GPP TS 45.005 (2016-08) GSM/EDGE Radio transmission and reception (Release 4).
2. Википедия : сайт. – URL: https://ru.wikipedia.org/wiki/Сотовая_связь (дата обращения: 20.11.2023).
3. Васинев Д.А., Соловьев М.В. Предложения по построению универсального фаззера протоколов // Труды учебных заведений связи. 2023 Т. 9 № 6 С. 59–67. DOI:10.31854/1813-324X-2023-9-6-59-67.