УДК 004.056

МЕТОДИКА АНАЛИЗА ТРАФИКА И ВЕРИФИКАЦИИ ШИФРОВАНИЯ В СОТОВОЙ СЕТИ 4/5G НА ОСНОВЕ ИМИТАТОРА БАЗОВОЙ СТАНЦИИ ЮНИТЕСС

Д.Н. Одинец

Учреждение образования «Белорусский государственный университет информатики и радиоэлектроники», г. Минск, Республика Беларусь

Аннотация. Статья описывает методику анализа трафика и верификации шифрования, реализованную в имитаторе базовой станции ЮНИТЕСС. Метод базируется на спецификациях 3GPP TS 33.401 и TS 35.201–207. Верификация включает два ключевых этапа: проверку корректности процедур аутентификации и генерации ключей, а также валидацию криптографических алгоритмов. Имитатор принудительно согласовывает алгоритмы защиты, вычисляет эталонные значения и сравнивает их с параметрами, полученными от абонентского устройства, что позволяет выявить ошибки реализации и уязвимости в системе безопасности терминалов 4/5G.

Ключевые слова: имитатор базовой станции ЮНИТЕСС; безопасность данных; шифрование; перехват сигнала; аутентификация.

METHOD OF TRAFFIC ANALYSIS AND ENCRYPTION VERIFICATION IN A 4/5G CELLULAR NETWORK BASED ON THE UNITESS SIMULATOR OF BASE STATION

D.N. Adzinets
Educational Institution "Belarusian State University of Informatics and Radioelectronics", Minsk, Republic of Belarus

Abstract. The article describes the method of traffic analysis and encryption verification implemented in the UNITESS base station simulator. The method is based on the 3GPP TS 33.401 and TS 35.201-207 specifications. Verification includes two key stages: verification of the correctness of authentication and key generation procedures, as well as validation of cryptographic algorithms. The simulator forcibly coordinates protection algorithms, calculates reference values and compares them with the parameters received from the subscriber device, which allows you to identify implementation errors and vulnerabilities in the security system of 4/5G terminals.
Keywords: UNITESS base station simulator; data security; encryption; signal interception; authentication.

Введение

Современные устройства с поддержкой GSM, LTE и 5G передают конфиденциальную информацию: телеметрию промышленных объектов, персональные данные, финансовые транзакции, команды управления критической инфраструктурой. В условиях роста киберугроз недостаточно проверить, работает ли модуль связи, необходимо убедиться, что он защищает данные – даже при целенаправленной атаке. Даже если модуль успешно проходит функциональное тестирование, скрытая уязвимость в реализации протоколов безопасности может сделать устройство мишенью для злоумышленников. Выявление таких дефектов на этапе производства – единственный способ избежать репутационных и финансовых потерь после отгрузки.

Методика анализа трафика и верификации шифрования

Для проверки реализации механизмов защиты необходим полный контроль над параметрами сети. Реальные операторские сети не позволяют реализовать требования предложенной методики тестирования.

1. Принудительно включать / выключать конкретные алгоритмы шифрования.
2. Модифицировать сигнальные сообщения «на лету».
3. Эмулировать атаки в изолированной среде.

Имитатор базовой станции ЮНИТЕСС решает эту задачу, предоставляя лабораторную среду с поддержкой полного стека протоколов 3GPP и алгоритмов безопасности: AES, Snow3G и ZUC для шифрования

и проверки целостности. Методика предполагает создание изолированной лабораторной 4/5G сети (без выхода в публичный интернет) и применение ЮНИТЕСС АРМ для автоматизации сценариев и сбора логов.

В процессе тестов имитируются представленные в таблице атаки.

Виды имитируемых атак
Types of simulated attacks

Тип атаки	Метод эмуляции	Критерий прохождения
Downgrade-атака	Имитатор предлагает только устаревшие или незащищенные алгоритмы (например, нулевое шифрование)	Модуль отвергает конфигурацию, если она ниже минимального порога безопасности, заданного в политике устройства
Replay-атака	Повторная отправка ранее записанных зашифрованных пакетов данных	Модуль игнорирует дубликаты благодаря механизмам счетчиков последовательностей (HFN/SQN)
Перехват идентификаторов	Анализ процедуры первичного подключения: передается ли постоянный идентификатор в открытом виде	Модуль использует временные идентификаторы (TMSI/GUTI) или зашифрованный SUCI; IMSI/SUPI не передается в открытом эфире
Атака на хэндовер	Эмуляция передачи контекста безопасности между «сотами» с подменой ключей	Ключи корректно обновляются (Key Derivation), сессия не прерывается, данные не передаются в открытом виде

Для различных классов устройств существуют свои особенности тестирования. Например, для IoT-датчики (умный город, ЖКХ) тестируется защита телеметрии, устойчивость к подмене команд, для промышленных контроллеров: гарантия подлинности команд управления, защита от несанкционированного доступа. Для транспортных терминалов тестируются конфиденциальность геоданных, защита от отслеживания. Для медицинских устройств важно протестировать соответствие требованиям защита персональных данных.

Ключевым преимуществом методики является возможность принудительного выбора алгоритмов шифрования (AES, Snow3G, ZUC), модификации сигнальных сообщений и эмуляции широкого спектра атак, включая downgrade-атаки, повторную передачу пакетов (replay), перехват идентификаторов и подмену ключей при хэндовере. Такой подход позволяет выявить скрытые дефекты реализации протоколов безопасности 3GPP (TS 33.401, TS 35.201–207) на этапе производства или лабораторных испытаний, тем самым предотвращая потенциальные репутационные и финансовые потери, связанные с эксплуатацией уязвимых устройств.

Особую ценность представляет адаптивность методики под различные классы оборудования – от IoT-датчиков до промышленных

контроллеров и медицинской техники, – что подтверждает ее универсальность. Внедрение данной методики в процессы контроля качества позволяет гарантировать не только работоспособность устройств, но и их способность противостоять целенаправленным атакам, обеспечивая конфиденциальность, целостность и подлинность передаваемых данных [1].

Заключение

Предложенная методика анализа трафика и верификации шифрования на базе имитатора базовой станции ЮНИТЕСС представляет собой комплексное решение для оценки защищенности устройств связи стандартов GSM, LTE и 5G. В условиях растущих киберугроз, нацеленных на перехват конфиденциальной информации и нарушение целостности управления критическими объектами, традиционное функциональное тестирование становится недостаточным. Использование имитатора позволяет воссоздать изолированную тестовую среду с полным контролем параметров сети, что недостижимо в условиях реальной операторской инфраструктуры.

Список использованных источников / References

1. Adzinets Dzmitry. Testing GSM/LTE/5G modules in conditions of no or unstable cellular communication. LXXIV International Multidisciplinary Conference "Recent Scientific Investigation". Proceedings of the Conference (12-13 November, 2025). Primedia E-launch LLC, Shawnee, USA. 2025. 122 p., p.47-50.

Сведения об авторе

Одинец Д.Н., канд. техн. наук, доцент, доцент, учреждение образования «Белорусский государственный университет информатики и радиоэлектроники», adzinets@bsuir.by.

Information about the author

Adzinetts D., Dr. Sci. (Tech.), Associate Professor, Associate Professor, Educational Institution "Belarusian State University of Informatics and Radioelectronics", adzinets@bsuir.by.