УДК 004.056

Данилин М.И.

магистр 2 курса

Поволжский государственный университет телекоммуникации и информатики

Россия, г. Самара

АНАЛИЗ АТАКИ IMP4GT МОБИЛЬНОЙ СЕТИ ЧЕТВЕРТОГО ПОКОЛЕНИЯ

Аннотация: в статье рассмотрен анализ атаки IMP4GT на мобильную сеть четвертого поколения. Рассмотрены сценарии атаки. Сделаны выводы о возможных последствиях атаки.

Ключевые слова: LTE, целостность, аутентификация, атака, IMP4GT.

Danilin M. I.

2nd year Master's degree

Volga Region State University of Telecommunications and Informatics

Russia, Samara

Analysis of the IMP4GT attack on the fourth-generation mobile network

Abstract: the article analyzes the IMP4GT attack on the fourth-generation mobile network. Attack vectors are considered. Conclusions are drawn about the possible consequences of the attack.

Keywords: LTE, integrity, authentication, attack, IMP4GT.

LTE (Long Term Evolution) является последним широко распространенным стандартом мобильной связи. В основе безопасности LTE лежит взаимная аутентификация пользовательского оборудования и сети, обеспечение конфиденциальности передаваемого трафика, конфиденциальность местоположения пользователя и многое другое. Нарушение одной из основ безопасности несет угрозу использованию LTE в качестве средства связи.

Атака IMP4GT (IMPersonation Attacks in 4G NeTworks), разработанная объединенной группой исследователей из Рурского и Нью-Йоркского университетов, позволяет злоумышленнику выдавать себя за легитимного пользователя в мобильной сети. Это становится возможным из-за уязвимости в LTE – отсутствие защиты целостности на уровне пользователя. Пользуясь этим, злоумышленник может провести атаку "Человек посередине" (MitM), что позволит ему манипулировать и перенаправлять IP-пакеты. Однако, IMP4GT расширяет атаку эксплуатируя механизм отражения определенных пакетов в IP стеке мобильной операционной системы.

Существует два сценария атаки IMP4GT:

1) восходящее (uplink) олицетворение;
2) нисходящее (downlink) олицетворение.

В сценарии восходящего олицетворения, злоумышленник выдает себя за легитимное устройство в сети. Этот вариант может быть использован для установления TCP/IP-соединения с Интернетом, связанного с личностью жертвы. Тем самым злоумышленник может посещать интернет-сайты используя чужой IP-адрес, а также публиковать разного рода информацию, чтобы скомпрометировать (подставить) других людей.

В сценарии нисходящего олицетворения, злоумышленник имитирует сеть и может установить TCP/IP-соединение с телефоном. При этом злоумышленник обходит межсетевой экран LTE-сети и потенциально может использовать это соединение для развертывания вредоносных программ или фильтрации данных.

Чтобы реализовать атаку на сетевом уровне злоумышленник использует строение IP-стека мобильной операционной системы. Принцип заключается в использовании отражения сообщений, которыми обмениваются пользовательское оборудование и сеть. В IMP4GT используются два типа сообщений отражения:

1) уведомление об отсутствии поддержки транспортных протоколов в операционной системе (недостижимое отражение).

2) сообщения типа ping (отражение ping).

Оба типа сообщений отражения несут в себе полезную нагрузку (копию исходного входящего IP-пакета), но они различаются по длине, скорости и предвидению полезной нагрузки. Исходя из этого в разных частях атаки IMP4GT используются разные сообщения отражения. Для дешифрования сообщений используется недостижимое отражение, а для шифрования – отражение ping.

Реализовав атаку “человек по середине”, злоумышленник использует сообщения отражения для построения оракула шифрования и дешифрования. Как только построение оракула будет закончено, злоумышленник может выдать себя за жертву, используя её IP-адрес.

Для реализации атаки IMP4GT злоумышленнику необходимо находиться непосредственно вблизи жертвы, создать оракул шифрования и дешифрования пакетов данных, иметь специальные навыки и дорогостоящее оборудование.

IMP4GT использует отсутствие защиты целостности наряду с механизмами отражения ICMP. В результате атаки злоумышленник может обойти любой механизм авторизации, учета или межсетевого экрана поставщика. С помощью IMP4GT злоумышленник может подделать любой трафик в Интернет, например, чтобы использовать личность жертвы для загрузки критических материалов. В случаях, когда правоохранительные органы запрашивают личность пользователя для конкретного публичного IP-адреса (законный запрос на раскрытие информации), действия IMP4GT влияют на результаты расследования.

Обеспечение защиты целостности на уровне пользователя является необходимым, чтобы не допустить данной атаки, реализация которой может привести к негативным последствиям, и других возможных атак, которые будут эксплуатировать данную уязвимость.

Использованные источники:

Imp4gt-attacks.net: сайт – 2020. – URL: https://imp4gt-attacks.net/ (дата обращения 29.05.2021)