УДК 004.056

Данилин М.И.

магистр 2 курса

Поволжский государственный университет телекоммуникации и информатики

Россия, г. Самара

ОБЗОР УГРОЗ БЕЗОПАСНОСТИ СТАНДАРТА LTE

Аннотация: в статье рассмотрены существующие угрозы мобильной сети четвертого поколения. Проведен анализ угроз и уровень их актуальности. Сделаны выводы о безопасности стандарта LTE.

Ключевые слова: LTE, атака, злоумышленник, пользовательское оборудование, целостность, безопасность.

Danilin M. I.

2nd year Master's degree

Volga Region State University of Telecommunications and Informatics

Russia, Samara

OVERVIEW OF LTE SECURITY THREATS

Abstract: the article considers the existing threats to the fourth-generation mobile network. The analysis of threats and the level of their relevance is carried out. Conclusions about the security of the LTE standard are made.

Keywords: LTE, attack, attacker, user hardware, integrity, security.

Long Term Evolution (LTE) является последним широко распространенным стандартом мобильной связи и используется сотнями миллионов людей по всему миру. Протокол предлагает высокоскоростной доступ в Интернет и услуги пакетной телефонии и стал неотъемлемой частью нашей повседневной коммуникации. Мы в основном полагаемся на безопасность LTE для различных приложений. Цели безопасности LTE включают, среди прочего, взаимную аутентификацию, конфиденциальность трафика и конфиденциальность местоположения; любой вектор атаки, подрывающий эти цели безопасности, имеет далеко идущие последствия для использования LTE в качестве средства связи.

Ниже представлены различные атаки на сеть радио доступа LTE. Большинство не является специфичными для сети LTE и может использоваться в других сетях.

Атака, использующая интерфернцию

Добавление искусственно созданной интерференции в радиосреду может привести к прекращениею функционирования системы в связи с значительным уровнем сигнала-помехи. Атаки такого типа легко осуществить из-за широкой доступности оборудования, что делает атаку данного типа актуальной. Однако, заметить инерференцию возможно с помощью оборудования мониторинга спектра радиоканала.

Атака, использующая подавление сигнала

Реализуется использованием идентичной частоты с пользовательским оборудованием. Так как беспроводные сети высокой скорости уязвимы к простому подавлению сигнала, радио канал может быть заблокирован из-за использования той-же частоты. В сети LTE, состоящей из множества подсистем, сигнал очень сложен. Если удастся вывести из строя одну подсистему, то вся базовая станция будет выведена из строя. Для реализации данной атаки злоумышленнику не потребуется

дорогостоящее оборудование. Все что потребуется – это, недорогое SDR (Software Defined Radio - программно-определяемая радиосистема), ноутбук и источник питания.

Атака определения местоположения

Определить местоположение пользователя становится возможным отследив C-RNTI (Cell Radio Network Temporary Identifier - временный сетевой идентификатор радиостанции) и сигналы переключения пользователя между базовыми станциями. Так как C-RNTI передается в открытом виде, злоумышленник сможет определить находится ли пользователь, имеющий данный C-RNTI, в этой ячейке или нет. Злоумышленник также имеет возможность связать новый C-RNTI из команды передачи (Handover Command message) со старым C-RNTI, чтобы отследить перемещения жертвы.

Для определения местоположения пользователя также могут использоваться уязвимости сотовых сетей предшествующих поколений, с которыми LTE взаимодействует в роуминге.

Атака, основанная на клонировании USIM

Задача данной атаки - извлечь мастер-ключ, который определяется оператором сети и входит в взаимно однозначное соответствие с IMSI. Извлечение мастер ключа необходимо для клонирования USIM, реализовав атаку на физическую реализацию механизмов, которые выполняют криптографические алгоритмы на карте. Существует способ восстановления мастер-ключа с помощью атаки по энергопотреблению (differential power analysis).

Атака на полосу пропускания

Целью данной атаки является частота, а именно – частота, которую использует пользовательское оборудование для передачи данных. Для злоумышленника представляют интерес отчеты о состоянии буфера (buffer

status report), которые содержат в себе информацию о контроле доступа, распределении нагрузки и планировании передач. Отправив ложный отчет о состоянии буфера базовой станции, злоумышленник может нарушить планируемый сеанс передачи данных.

Атака aLTEr

Цель данной атаки – прослушивание соединения и перенаправление пользователя на мошеннический сайт. Атака реализуется за счет уязвимости стандарта LTE – отсутствие защиты целостности пользовательского уровня. У данной атаки существует два сценария: прослушивание и активная фаза атаки.

В сценарии прослушивания злоумышленник анализирует пакеты, передаваемые пользователем. Анализируя активность пользователя в сети, злоумышленник вычисляет наиболее посещаемы сайты, а также создает шаблоны активности, чтобы провести активную фазу атаки.

Активная фаза атаки является продолжением пассивной фазы. В этом сценарии злоумышленник выдает себя за базовую станцию по отношению к пользовательскому оборудованию. Получив пакеты пользователя, злоумышленник передает их на настоящую базовую станцию, чтобы заменить ответные сообщения базовой станции – перенаправить пользователя на мошеннический сайт. Причина – алгоритм AES-CTR, который выполняет функцию счётчика, но не контролирует целостность пакетов и, соответственно, не позволяет обнаружить подмену шифротекста.

Для реализации атаки злоумышленнику необходимо иметь дорогостоящее оборудование и находиться непосредственно вблизи пользователя.

Атака олицетворения IMP4GT

Цель данной атаки – выдать себя за пользователя в сети по отношению к базовой станции или выдать себя за базовую станцию по отношению к пользователю. Эта атака использует ту же уязвимость, что и атака aLTEr, и дополняет её атакой на сетевом уровне. Атака позволяет злоумышленнику публиковать критические данные, используя IP-адрес жертвы. Злоумышленник, выдавая себя за базовую станцию, обходит брандмауэр поставщика и потенциально может использовать это соединение для развертывания вредоносных программ или фильтрации данных.

Для реализации атаки необходимо дорогостоящее оборудование, наличие специальных знаний у злоумышленника и непосредственное нахождение вблизи жертвы.

LTE сети имеют достаточное количество угроз, однако целесообразность проведения атаки на пользователя не всегда присутствует. Это связано со спецификой атаки, требуемым оборудованием, цена которого значительно превышает выгоду от атаки на произвольного пользователя сети. Отсутствие защиты целостности пользовательского уровня является серьёзной уязвимость, используя которую злоумышленники могут проводить точечные атаки. Обнаружение большего количества уязвимостей и появление новых атак может послужить для обеспечения лучшей защиты в мобильной сети следующего поколения.

Используемые источники:

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

Alter-attack.net: сайт – 2019. – URL: https://alter-attack.net (дата обращения 06.06.2021)