

МОДИФИЦИРОВАННЫЙ МЕТОД ПОСТРОЕНИЯ АЛГОРИТМА АУТЕНТИФИКАЦИИ ПРОТОКОЛА LTE EPS-AKA С ИСПОЛЬЗОВАНИЕМ ВЕКТОРА ЗАПРОСА

Никита Вячеславович КОРМИЛЬЦЕВ^{a,*}, Александр Дмитриевич УВАРОВ^b,
Александр Анатольевич МИХАЙЛОВ^c, Марина Владимировна ТУМБИНСКАЯ^d

^a студент, Казанский национальный исследовательский технический
университет им. А.Н. Туполева – КАИ (КНИТУ-КАИ), Казань, Российская Федерация
kormiltcev@hotmail.com
https://orcid.org/0000-0002-2289-5672
SPIN-код: 1580-1482

^b студент, Казанский национальный исследовательский технический
университет им. А.Н. Туполева – КАИ (КНИТУ-КАИ), Казань, Российская Федерация
obg-96@mail.ru
https://orcid.org/0000-0003-0337-2689
SPIN-код: 7184-4498

^c студент, Казанский национальный исследовательский технический
университет им. А.Н. Туполева – КАИ (КНИТУ-КАИ), Казань, Российская Федерация
Alex-0995@mail.ru
ORCID: отсутствует
SPIN-код: отсутствует

^d кандидат технических наук, доцент кафедры систем информационной безопасности,
Казанский национальный исследовательский технический университет им. А.Н. Туполева –
КАИ (КНИТУ-КАИ), Казань, Российская Федерация
tumbinskaya@inbox.ru
ORCID: отсутствует
SPIN-код: 4414-9302

• Ответственный автор

История статьи:

Получена 31.01.2019
Получена в доработанном
виде 22.02.2019
Одобрена 15.03.2019
Доступна онлайн
15.04.2019

УДК 004.056

JEL: C63, M15

Ключевые слова:

EPS-AKA, LTE, MME,
E-UTRAN, сотовая
безопасность,
аутентификация

Аннотация

Предмет. Разработка модифицированного метода построения алгоритма аутентификации протокола LTE EPS-AKA с использованием вектора запроса в четвертом поколении стандартов связи LTE.

Цели. Изучение возможного решения проблемы получения IMSI в открытом виде во время аутентификации EPS-AKA в сети LTE с использованием инфраструктуры открытых ключей (PKI).

Методология. В работе использованы методы математического и аппаратного моделирования.

Результаты. Предложен модифицированный метод построения алгоритма аутентификации протокола LTE EPS-AKA с использованием вектора запроса на основе корреляции запросов аутентификации UE с серийным номером оборудования (IMEI), который хранится в специальном векторе безопасности (SV) для последних запросов на аутентификацию, полученных и сохраненных в HSS. Таким образом, HSS будет защищен от DoS-атак, которые не устраняются простыми методами защиты, включенными в стандарт LTE.

Выводы. Проведен анализ безопасности существующих 4G сетей, а также их уязвимости к DoS-атакам. Обнаружена серьезная уязвимость в процессе аутентификации, заключающаяся в том, что вектор аутентификации вычисляет непосредственно HSS, даже если мобильное устройство заражено вредоносными ПО или отправка последовательного запроса происходит с использованием поддельных IMSI, что непременно приведет к перегрузке важной части основного сервера HSS и к его возможному отключению.

© Издательский дом ФИНАНСЫ и КРЕДИТ, 2019

Для цитирования: Кормильцев Н.В., Уваров А.Д., Михайлов А.А., Тумбинская М.В. Модифицированный метод построения алгоритма аутентификации протокола LTE EPS-AKA с использованием вектора запроса // Национальные интересы: приоритеты и безопасность. – 2019. – Т. 15, № 4. – С. 784 – 794.
<https://doi.org/10.24891/ni.15.4.784>

Введение

Массовое использование информационных систем породило проблему киберпреступлений. Увеличение скорости передачи данных при быстром перемещении мобильного устройства (UE) и уменьшение стоимости оказания услуг привело к тому, что консорциум 3GPP разработал новые радио-интерфейсы OFDMA и SC-FDMA, используемые в сотовой связи, причем обеспечение безопасности является необходимостью при передаче конфиденциальных данных [1].

Для обеспечения безопасности сети архитектура сетевой безопасности должна основываться на двух принципах. Прежде всего следует создать иерархическую защиту, а затем во время дальнейших разработок необходимо внедрять принципы глубокой обороны. Первая концепция направлена на выполнение политик безопасности для обеспечения отказоустойчивости сети. Глубокая защита, используя полиномиальную политику защиты для управления рисками, повышает безопасность сети. Здесь вступает в силу принцип: *при отказе одной линии защиты, другая линия защиты предотвращает повреждение всей системы*. Система безопасности должна планироваться иерархически – от границы сети до внутренней сети и основных серверов. В настоящей статье предлагается подход к системе защиты сетей LTE/LTE Advanced.

При реализации безопасности необходимо разделить сигналы на управление и потоки пользователя, как указано в общей модели безопасности ITU-T X805 [2]. Каждая рассматриваемая плоскость состоит из сетевых устройств, соединений и сетевых приложений. С помощью модели иерархической архитектуры безопасности мы имеем возможность анализировать угрозы безопасности сетей 4G LTE и предоставлять соответствующие политики и методы для

решения проблем сетевой безопасности. Управление безопасностью обеспечивают такие механизмы, как контроль политики безопасности, а также сбор событий, анализ и составление отчетов.

Сетевая архитектура 4G

Long Term Evolution (LTE) – новый стандарт сотовой связи, основанный на стандарте 3G и определяющий упрощенную сетевую модель на основе IP [3]. Начиная с данного стандарта в сети радиодоступа появляется новый компонент – усовершенствованная базовая станция (eNB), обрабатывающая все требования по радио-интерфейсу самостоятельно в отличие от BTS/NodeB сетей 2G/3G, которым требуются определенные стандартные контроллеры BSC/RNC. Также были добавлены новые прямые интерфейсы связи между базовыми станциями и интерфейсы X2, которые обеспечивают прямую связь и передачу обслуживания на основе IP между двумя или более eNodeB, а также перенаправление PDU на одноранговые узлы туннеля. Данный стандарт также предлагает возможность прямой связи между сетевыми объектами, которые принадлежат двум разным абонентам, тем самым достигая одной из главных целей – определения открытых интерфейсов для всех абонентов.

MME отвечает за связь NAS с межсетевым узлом, расположенным между сетями доступа 3G, и интерфейсом S3. Также MME хранит список всех зон отслеживания для UE и выбирает S-GW и P-GW для абонента.

Помимо всех функций, определенных в стандарте LTE, в данной статье будут рассмотрены методы аутентификации и авторизации пользователя. Важным фактом является то, что пользовательский трафик после аутентификации идет не через MME, а непосредственно направляется в S-GW и PGW. Если злоумышленник захочет

выполнить перехват пакетного трафика, он должен подключиться именно к этим точкам. S-GW является завершающей стадией интерфейса передачи пакетных данных в направлении E-UTRAN. Когда мобильные устройства перемещаются между базовыми станциями, S-GW выполняет функцию привязки к местности. Это означает, что пакеты маршрутизируются как во внутренней, так и в междугородней EUTRAN. P-GW похож на S-GW, разница заключается в том, что он представляет собой шлюз для внешних фиксированных и мобильных сетей передачи данных. Он также отвечает за выполнение определенных правил оператора, предназначенных для распределения ресурсов.

Сервер HSS – это сервер, объединяющий Home Location Register (HLR) и центр аутентификации (AuC), присутствующие в сетях 2G и 3G. HLR состоит из базы данных, которая хранит информацию о профиле пользователя и номер мобильного телефона (MSISDN) [4]. AuC HSS – это часть сервера, отвечающая за создание вектора аутентификации (AV), который используется для взаимной аутентификации между абонентом и сетью, шифрованием и защитой целостности во время передачи по радиоканалу.

В последние годы в сеть был внедрен шлюз безопасности (Se-GW) для обеспечения защиты основной сети и зашифрованного трафика IPSEC между eNodeB и базовой сетью. PCRF (*Policy and Charging Rules Function*) Server отвечает за управление каждым абонентским сеансом и правилами его учета. По сравнению с UMTS PCRF он представляет собой комбинацию функций решения политики сеанса связи (PDF) и функций тарификации (CRF). Основные компоненты и интерфейсы сети LTE, используемые для установления соединений, представлены на рис. 1 [5].

Сравнительный анализ сетевой безопасности поколений стандартов связи

В настоящее время в зависимости от скорости передачи данных, количества и качества предоставляемых услуг можно выделить

четыре основных поколения стандартов сетей сотовой связи. Стоит добавить, что сейчас активное развитие получает пятое поколение стандарта, но из-за малой распространенности в данной статье рассмотрен не будет. Каждое из поколений характеризуется особенностями реализации механизмов обеспечения безопасности (табл. 1) [6].

Сетевая безопасность LTE

В LTE применяется метод аутентификации EPS-AKA (*Evolved Packet System – Authorization and Key Agreement*), представляющий собой доработку алгоритма 3G AKA (UMTS AKA), и, естественно, не являющийся совершенно новым методом аутентификации [7]. Основной причиной выбора такого подхода послужила хорошая совместимость алгоритма с существующими технологиями, а также низкая стоимость реализации для сетей 4G.

Механизм безопасности AKA основан на секретном ключе, разделяемом между USIM-картой (*Universal Identifier Module*) и AuC (центром аутентификации). Для обеспечения конфиденциальности данных пользователей во время аутентификации для каждого абонента генерируются разные ключи [8]. В ходе разработки протокола для удовлетворения новых требований безопасности стандарту 4G были поставлены следующие цели:

- полная взаимная аутентификация в сети между MS и LTE;
- ключи для шифрования (CK) и проверки целостности (IK), генерируемые USIM в мобильном устройстве пользователя, не передаются по радиоинтерфейсу;
- максимально возможное разделение ключей;
- MME получает от HSS только KASME, а не конкретные ключи (IK и CK);
- шифрование на уровне AS (сигнализация и данные) и NAS (Non Access Stratum);
- защита целостности как для AS, так и для NAS.

Аутентификация в LTE, отображенная на рис. 2, происходит следующим образом:

- UE отправляет в MME запрос Attach Request (содержащий IMSI, параметры безопасности, набор ключей KSI-ASME) [9];
- MME перенаправляет запрос аутентификации в HSS, добавляя к нему идентификатор сети сервера (SNID) и тип сети (проводная или радиосеть);
- домашний сервер абонентов (HSS) аутентифицирует идентификатор сети службы (SNID) и, получая ключ безопасности от UE, вычисляет параметр с выбранным порядковым номером (SQN) и случайным числом (RAND), которое генерируется вектором аутентификации AV. Данный вектор состоит из четырех параметров: XRES (ожидаемый ответ от UE), токена аутентификации (AUTN), RAND и KASME;
- HSS отправляет AV в MME;
- MME отправляет запрос аутентификации в UE, который включает такие параметры, как RAND, AUTN и KSI-ASME. Последний параметр используется UE для генерации K-ASME, идентичного тому, который используется в HSS;
- UE аутентифицирует MME и, следовательно, сеть. Мобильное устройство, используя f1 для генерации XMAC, сравнивает его с MAC в полученном AUTN;
- UE использует f2 для вычисления RES, а также генерирует СК с использованием f3 (RAND) и IK с использованием f4 (RAND);
- UE отправляет ответ аутентификации RES в MME;
- MME сравнивает UE RES с HSS XRES и, если они совпадают, UE становится успешно аутентифицированным. Если они отличаются друг от друга, MME отбрасывает соединение с UE.

Исходя из перечисленного, протокол аутентификации EPS-AKA можно разделить на две фазы. Сначала происходит генерация и

распределение информации об аутентификации от HSS к MME, а уже затем – процесс взаимной аутентификации между UE и MME [10].

И все же приведенный механизм аутентификации EPS-AKA имеет ряд уязвимостей для нескольких видов как активных, так и пассивных атак из-за отправления IMSI в незащищенном виде, что влечет за собой нарушение конфиденциальности и возможность применения злоумышленником DoS-атаки. При этом стоит отметить, что DoS-атака может быть направлена как на MME, так и на HSS. Для подавления последнего, злоумышленник может постоянно отправлять запрос на идентификацию посредством отправки на HSS случайно сгенерированные поддельные IMSI [11]. Такие атаки обойдутся относительно недорого, стоимость оборудования колеблется от 1 300 до 3 900 долл. США (если пренебречь юридическими последствиями).

В 2012 г. авторы работы [12] продемонстрировали такой вид атаки, в результате которой были представлены доказательства возможности прослушивания конфиденциальной информации абонентов. Результаты исследований уязвимостей 4G-сетей 50 мировых операторов, работающих в России, Европе и Азии, приведенных экспертами Positive Technologies, показали что в 80% случаев удалось доказать успешность проведения атак, направленных на сбой в работе, в 77% – возможность перехвата SMS и голосовых вызовов, определения местоположения и в 67% – успешность кражи денег со счетов абонентов.

В настоящее время 4G LTE представляет собой гетерогенную сеть, которая благодаря коммутации пакетов может быть легко интегрирована в другие беспроводные сети, например wi-fi, WIMAX и UMTS. Именно поэтому при таких возможностях развития данной технологии, обеспечение безопасности не может проходить с использованием одинакового ключа асимметричного шифрования сообщений, посылаемых мобильным устройством и HSS. Кроме того,

асимметричное шифрование само по себе не может обеспечить необходимую конфиденциальность и доступность на основании того факта, что при компроментации закрытого ключа HSS посредством атаки с использованием ложной базовой станции станет доступна конфиденциальная информация абонентов.

Совершенствование алгоритма протокола LTE EPS-AKA с вектором безопасности (EPS-AKASV)

Злоумышленник может использовать легальное UE для постоянной отправки поддельных IMSI для перегрузки HSS/AuC, что, несомненно, будет потреблять вычислительную мощность и переполнять буфер памяти. Кроме того, в зависимости от количества атак и технических характеристик аппаратного и программного обеспечения HSS данная атака может привести к отключению HSS от обслуживания через определенный промежуток времени.

Нами предлагается подход к совершенствованию использования аутентификации EPS-AKA с вектором безопасности (SV), в котором HSS сначала сравнивает запросы аутентификации с одного и того же аппаратного адреса UE прежде чем вычислять вектор аутентификации. Физический адрес UE будет сохранен в SV и если в векторе безопасности будет найден новый запрос, HSS/AuC отменит запрос от UE в течение предопределенного периода времени. Эта концепция гарантирует, что устройство, которое пытается провести DoS-атаку, не будет перегружать HSS/MME [6].

Вектор безопасности будет иметь длину, равную 300 значениям физических адресов UE, чтобы сохранить данные в буфер HSS и не запрашивать дополнительные мощности при проверке того, существует ли еще новое значение IMEI в вычисленных запросах. Проверка IMEI вычисляется, используя две функции FOR и IF, чтобы проверить, находится ли новый IMEI в (SV) [13].

Таблица 1

Сравнительный анализ сетевой безопасности поколений стандартов связи

Table 1

A comparative analysis of the network security of communication standard generations

Поколение стандартов сетей сотовой связи	Особенности механизма аутентификации	Уязвимости информационной безопасности	Отличительные особенности защиты информации от предшествующих поколений стандартов
1G	На начальном этапе развития сетей при появлении таких технологий, как AMPS/D-AMPS, NMT-450) защита от НСД осуществлялась посредством использования двух индикаторных номеров, которые присваиваются каждому абоненту: ESN (электронный серийный номер от фирмы изготовителя) и MIN (мобильный идентификационный номер, который присваивается оператором). Весь механизм аутентификации основывается на приеме базовой станцией на определенной частоте идентификаторов ESN и MIN	Уязвимость заключается в простоте перехвата данных из эфира с помощью сканера совместно с простой расшифровкой, что привело к массовому клонированию телефонных станций. Конфиденциальность самой связи полностью исключалась, потому что сигналы в эфире передавались с использованием частотной модуляции и прослушивались в эфире с помощью обычного ЧМ-приемника	Поскольку это первый появившийся стандарт сотовой связи, необходимо отметить, что для устранения заявленной уязвимости были внедрены криптографические технологии аутентификации пользователей: A-KEY и SIS, основанные на методе запрос/ответ. BS посылает запрос, а телефон, обработав его, выдает зашифрованный ответ. При этом, если полученный ответ верный, то BS допускает пользователя в сеть. Поскольку теперь ключ не передавался в эфире, клонирование телефонов стало затруднено

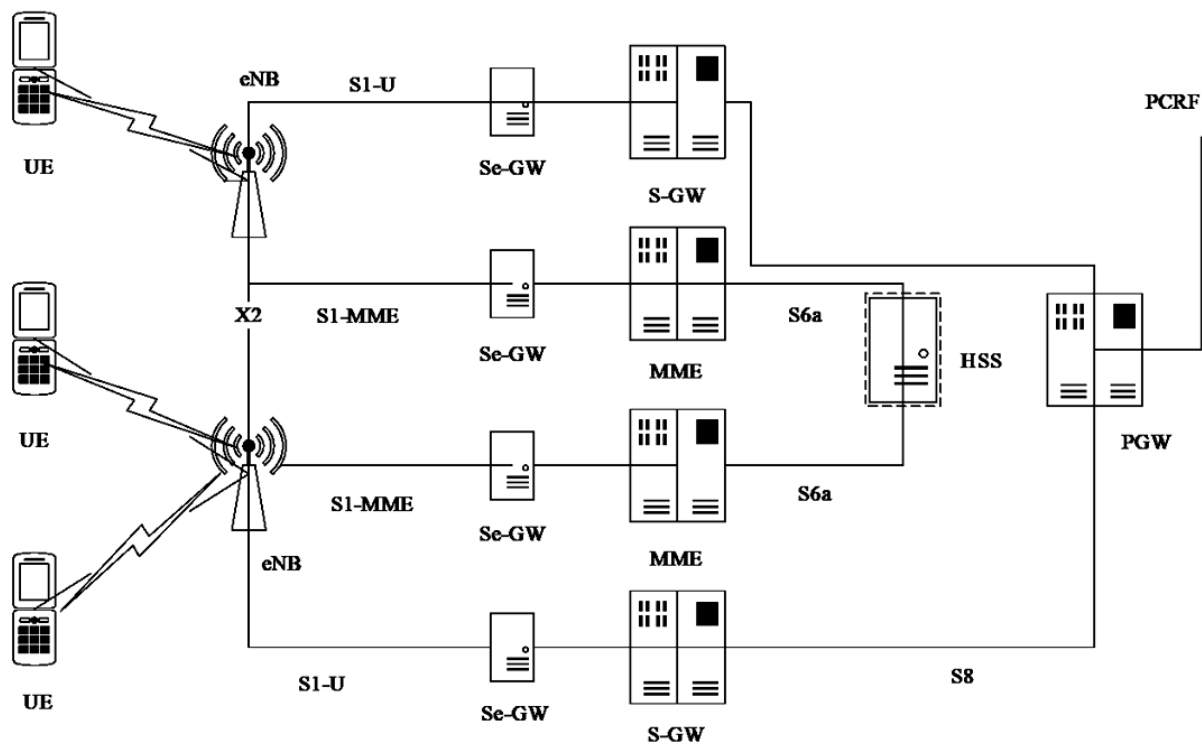
2G	Принцип аутентификации в сетях 2G (GSM) аналогичен реализованному в технологиях A-KEY и SIS и основан на механизме аутентификации «запрос/ответ» с использованием шифрования	Детальный анализ 2G-сетей позволяет выявить ряд существенно уязвимых мест подсистемы безопасности, таких как малая длина криптографических ключей и заложенная команда отключения режима шифрования. Также в сетях не предусмотрена взаимная аутентификация, в результате чего абонент может подключиться к поддельной базовой станции, отсутствуют процедуры, позволяющие BS отслеживать параметры абонентов при роуминге. В дополнение к этому система безопасности не обладает необходимой функциональной гибкостью и не позволяет наращивать криптостойкость	Отличия заключаются в том, что параметры аутентификации перестали быть привязаны к мобильному устройству, а стали храниться в отдельном аутентификационном модуле – SIM-карте. Здесь же хранятся алгоритмы шифрования A3 и A8. При переходе к сетям стандарта GPRS, позиционируемым в качестве сетей сотовой связи промежуточного поколения (2.5G), впервые была реализована система защиты каждой из точек сети от внешних атак. В сетях GPRS используются более криптостойкие алгоритмы семейства GPRS-A5, при этом ключи шифрования не закреплены за мобильным устройством, а выбираются в процессе аутентификации
3G	Аутентификация пользователя в UMTS так же, как и в сети GSM, осуществляется с помощью шифрования с общим ключом по протоколу типа «клик-отзыв», аутентифицирующая сторона посылает аутентифицируемой стороне случайное число, которое зашифровывает его по определенному алгоритму с помощью общего ключа и возвращает результат обратно	Существует два способа получения IMSI нужного устройства и перехвата его координат при помощи фемтосоты, компактной носимой базовой станции. В первом случае удастся перехватить пару IMSI/TMSI во время обмена между устройством и базовой станцией. Во втором случае – передачу параметров аутентификации и секретного ключа сессии, после чего перенаправить этот сигнал на все находящиеся в зоне доступа устройства, включая атакуемое. Сообщение об ошибке при синхронизации обнаруживает нужное устройство, что делает возможным получение данных о местонахождении нужного абонента, не задействовав при этом оператора сотовой связи	В 3G в целях безопасности не применяется постоянный идентификатор устройства (IMSI), он заменен на периодически меняющийся временный (TMSI)

Источник: авторская разработка

Source: Authoring

Рисунок 1
Модель сетевой архитектуры LTE

Figure 1
The LTE network architecture model

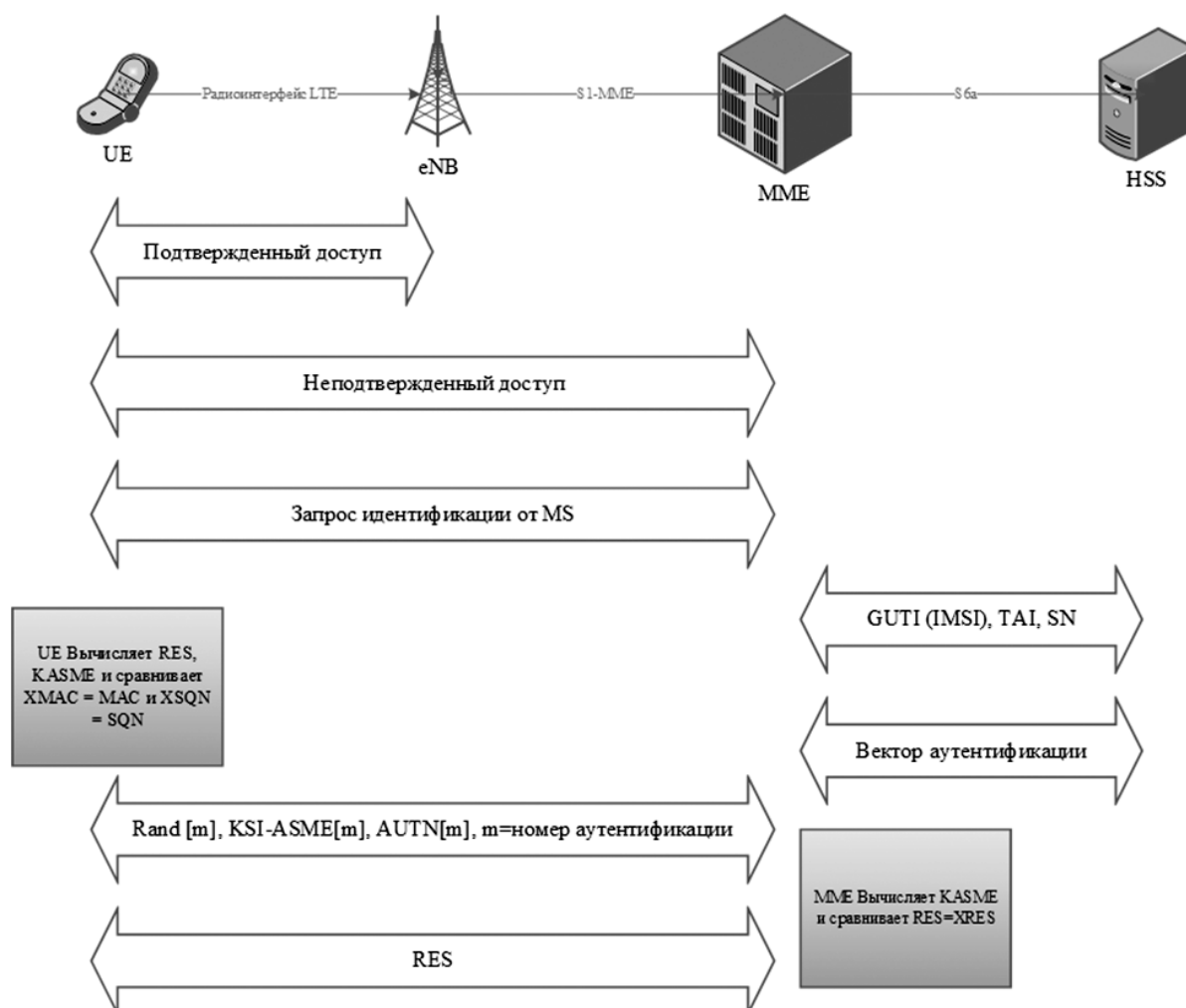


Источник: авторская разработка

Source: Authoring

Рисунок 2
Процесс аутентификации EPS-AKA

Figure 2
The EPS-AKA authentication process



Источник: авторская разработка

Source: Authoring

Список литературы

1. Лапсарь А.П., Лапсарь С.А. Обеспечение безопасности инновационных разработок в условиях конкурентного противостояния // Финансы и кредит. 2017. Т. 23. Вып. 1. С. 49–62. URL: <https://doi.org/10.24891/fc.23.1.49>
2. Кормильцев Н.В., Уваров А.Д., Корнилов Г.С., Перухин М.Ю. Оптимизация процесса аутентификации для защиты конфиденциальных данных пользователей при подключении к сети LTE // Вестник Технологического университета. 2018. Т. 21. № 3. С. 134–138.
3. Казарин О.В. Многосторонние конфиденциальные вычисления в задаче о предотвращении столкновений // Вестник компьютерных и информационных технологий. 2017. № 6. С. 50–56. URL: <https://doi.org/10.14489/vkit.2017.06.pp.050-056>

4. *Кормильцев Н.В., Уваров А.Д.* Методы создания IMSI-ловушки для перехвата GSM-пакетов // Вестник современных исследований. 2018. № 3-2 (18). С. 137–139.
URL: <http://orcacenter.ru/journals/modern-research/mr.2018.03.02.pdf>
5. *Корионов И.П., Орлов В.Г.* Пользовательские аспекты безопасности в сетях LTE // Телекоммуникации и информационные технологии. 2017. № 2. С. 16–21.
URL: <http://www.srd-mtuci.ru/attachments/article/249/%D0%A2%D0%98%D0%A2-2-2017.pdf>
6. *Петренко А.А., Петренко С.А.* Способ повышения устойчивости LTE-сети в условиях деструктивных кибератак // Вопросы кибербезопасности. 2015. № 2. С. 36–42.
URL: <https://cyberleninka.ru/article/n/sposob-povysheniya-ustoychivosti-lte-seti-v-usloviyah-destruktivnyh-kiberatak>
7. *Бармина С.С., Таджикибаева Ф.М., Тумбинская М.В.* Корреляционный анализ и прогнозирование SYN-ФЛУД атак // Прикладная информатика. 2018. Т. 13. № 4. С. 93–102.
URL: <https://publications.hse.ru/mirror/pubs/share/direct/226449553>
8. *Степунин А.Н., Николаев А.Д.* Мобильная связь на пути к 6G. Вологда: Инфра-Инженерия, 2017. Т. 1. С. 23–45.
9. *Ермаков С.А., Коленбет Н.С., Юрасов В.Г., Батаронов И.Л.* Архитектура системы безопасности в сотовых сетях стандарта LTE // Информация и безопасность. 2014. Т. 17. № 4. С. 626–629.
10. *Листопад М.Е., Коротченко С.Е.* Совершенствование методики оценки системы информационной безопасности в России // Национальные интересы: приоритеты и безопасность. 2017. Т. 13. Вып. 6. С. 1162–1175. URL: <https://doi.org/10.24891/ni.13.6.1162>
11. *Терентьев А.М.* Выбор адекватных средств информационной защиты персонального компьютера в России // Национальные интересы: приоритеты и безопасность. 2012. Т. 8. Вып. 33. С. 37–42. URL: <https://cyberleninka.ru/article/n/vybor-adekvatnyh-sredstv-informatsionnoy-zaschity-personalnogo-kompyutera-v-rossii>
12. *Ревенков П.В., Бердюгин А.А.* Кибербезопасность в условиях Интернета вещей и электронного банкинга // Национальные интересы: приоритеты и безопасность. 2016. Т. 12. Вып. 11. С. 158–169. URL: <https://cyberleninka.ru/article/n/kiberbezopasnost-v-usloviyah-interneta-veschey-i-elektronnogo-bankinga>
13. *Асирян В.М., Шишкин М.О., Степанов М.С.* Оценка ресурса соты сети LTE при обслуживании эластичного трафика // Телекоммуникации и информационные технологии. 2018. Т. 5. № 1. С. 76–82.
URL: <http://srd-mtuci.ru/attachments/article/249/%D0%A2%D0%98%D0%A2-1-2018.pdf>

Информация о конфликте интересов

Мы, авторы данной статьи, со всей ответственностью заявляем о частичном и полном отсутствии фактического или потенциального конфликта интересов с какой бы то ни было третьей стороной, который может возникнуть вследствие публикации данной статьи. Настоящее заявление относится к проведению научной работы, сбору и обработке данных, написанию и подготовке статьи, принятию решения о публикации рукописи.

A MODIFIED METHOD TO DESIGN THE LTE AUTHENTICATION PROTOCOL EPS-AKA ALGORITHM USING THE QUERY VECTOR

Nikita V. KORMIL'TSEV^a, Aleksandr D. UVAROV^b,
Aleksandr A. MIKHAILOV^c, Marina V. TUMBINSKAYA^d

^a Kazan National Research Technical University named after A.N. Tupolev – KAI (KNRTU-KAI),
Kazan, Republic of Tatarstan, Russian Federation
kormiltcev@hotmail.com
<https://orcid.org/0000-0002-2289-5672>

^b Kazan National Research Technical University named after A.N. Tupolev – KAI (KNRTU-KAI),
Kazan, Republic of Tatarstan, Russian Federation
obg-96@mail.ru
<https://orcid.org/0000-0003-0337-2689>

^c Kazan National Research Technical University named after A.N. Tupolev – KAI (KNRTU-KAI),
Kazan, Republic of Tatarstan, Russian Federation
Alex-0995@mail.ru
ORCID: not available

^d Kazan National Research Technical University named after A.N. Tupolev – KAI (KNRTU-KAI),
Kazan, Republic of Tatarstan, Russian Federation
tumbinskaya@inbox.ru
ORCID: not available

• Corresponding author

Article history:

Received 31 January 2019
Received in revised form
22 February 2019
Accepted 15 March 2019
Available online
15 April 2019

JEL classification: C63,
M15

Keywords: EPS-AKA,
LTE, MME, E-UTRAN,
mobile security,
authentication

Abstract

Subject This article deals with the development of a modified method of the LTE authentication protocol EPS-AKA algorithm design using the query vector in the fourth generation of LTE communication standards.

Objectives The article aims to explore the possibility of solving the problem of obtaining international mobile subscriber identity (IMSI) in the clear during EPS-AKA authentication in the LTE network using Public Key Infrastructure (PKI).

Methods For the study, we used the methods of mathematical and hardware modeling.

Results We offer a modified method to develop the LTE authentication protocol EPS-AKA algorithm using the query vector based on the correlation of UE authentication requests with the international mobile equipment identity (IMEI), which is stored in a special security vector (SV) for the latest authentication requests received and stored in the HSS. Thus, the HSS can be protected from DoS attacks, which are not eliminated by the conventional protection methods included in the LTE standard.

© Publishing house FINANCE and CREDIT, 2019

Please cite this article as: Kormil'tsev N.V., Uvarov A.D., Mikhailov A.A., Tumbinskaya M.V. A Modified Method to Design the LTE Authentication Protocol EPS-AKA Algorithm Using the Query Vector. *National Interests: Priorities and Security*, 2019, vol. 15, iss. 4, pp. 784–794.
<https://doi.org/10.24891/ni.15.4.784>

References

1. Lapsar' A.P., Lapsar' S.A. [Safety of innovation under competitive struggle]. *Finansy i kredit = Finance and Credit*, 2017, vol. 23, iss. 1, pp. 49–62. (In Russ.)
URL: <https://doi.org/10.24891/fc.23.1.49>
2. Kormil'tsev N.V., Uvarov A.D., Kornilov G.S., Perukhin M.Yu. [Optimizing the authentication process protecting confidential user data when connecting to the LTE network]. *Vestnik Tekhnologicheskogo universiteta = Herald of Kazan Technological University*, 2018, vol. 21, no. 3, pp. 134–138. (In Russ.)

3. Kazarin O.V. [Multi-party secure computation in the problem of collisions prevention]. *Vestnik komp'yuternykh i informatsionnykh tekhnologii = Herald of Computer and Information Technologies*, 2017, no. 6, pp. 50–56. (In Russ.)
URL: <https://doi.org/10.14489/vkit.2017.06.pp.050-056>
4. Kormil'tsev N.V., Uvarov A.D. [Methods to create a IMSI trap to intercept GSM packets]. *Vestnik sovremennykh issledovaniy*, 2018, no. 3-2 (18), pp. 137–139. (In Russ.)
URL: <http://orcacenter.ru/journals/modern-research/mr.2018.03.02.pdf>
5. Korionov I.P., Orlov V.G. [User-defined security aspects of LTE networks]. *Telekommunikatsii i informatsionnye tekhnologii = Telecommunications and Information Technologies*, 2017, no. 2, pp. 16–21. URL: <http://www.srd-mtuci.ru/attachments/article/249/%D0%A2%D0%98%D0%A2-2-2017.pdf> (In Russ.)
6. Petrenko A.A., Petrenko S.A. [Method for increasing the LTE-network stability in destructive cyber attacks]. *Voprosy kiberbezopasnosti = Cybersecurity Issues*, 2015, no. 2, pp. 36–42.
URL: <https://cyberleninka.ru/article/n/sposob-povysheniya-ustoychivosti-lte-seti-v-usloviyah-destruktivnyh-kiberatak> (In Russ.)
7. Barmina S.S., Tadzhibaeva F.M., Tumbinskaya M.V. [Correlation analysis and forecasting of SYN-flood attacks]. *Prikladnaya informatika = Journal of Applied Informatics*, 2018, vol. 13, no. 4, pp. 93–102. URL: <https://publications.hse.ru/mirror/pubs/share/direct/226449553> (In Russ.)
8. Steputin A.N., Nikolaev A.D. *Mobil'naya svyaz' na puti k 6G. V 2-kh tomakh* [Mobile communication on the way to 6G. In two volumes]. Vologda, Infra-Inzheneriya Publ., 2017, vol. 1, pp. 23–45. (In Russ.)
9. Ermakov S.A., Kolenbet N.S., Yurasov V.G., Bataronov I.L. [Security architecture in LTE cellular networks]. *Informatsiya i bezopasnost' = Information and Security*, 2014, vol. 17, no. 4, pp. 626–629. (In Russ.)
10. Listopad M.E., Korotchenko S.E. [Improving the method for evaluation of the information security system in Russia]. *Natsional'nye interesy: priority i bezopasnost' = National Interests: Priorities and Security*, 2017, vol. 13, iss 6, pp. 1162–1175. (In Russ.)
URL: <https://doi.org/10.24891/ni.13.6.1162>
11. Terent'ev A.M. [Selecting adequate means of information protection of personal computer in Russia]. *Natsional'nye interesy: priority i bezopasnost' = National Interests: Priorities and Security*, 2012, vol. 8, iss. 33, pp. 37–42. URL: <https://cyberleninka.ru/article/n/vybor-adekvatnyh-sredstv-informatsionnoy-zaschity-personalnogo-kompyutera-v-rossii> (In Russ.)
12. Revenkov P.V., Berdyugin A.A. [Cybersecurity in the Internet of things and electronic banking]. *Natsional'nye interesy: priority i bezopasnost' = National Interests: Priorities and Security*, 2016, vol. 12, iss. 11, pp. 158–169. URL: <https://cyberleninka.ru/article/n/kiberbezopasnost-v-usloviyah-interneta-veschey-i-elektronnogo-bankinga> (In Russ.)
13. Asiryan V.M., Shishkin M.O., Stepanov M.S. [Assessment of the resource cell of the LTE network during the maintenance of the elastic traffic]. *Telekommunikatsii i informatsionnye tekhnologii = Telecommunications and Information Technologies*, 2018, vol. 5, no. 1, pp. 76–82.
URL: <http://srd-mtuci.ru/attachments/article/249/%D0%A2%D0%98%D0%A2-1-2018.pdf> (In Russ.)

Conflict-of-interest notification

We, the authors of this article, bindingly and explicitly declare of the partial and total lack of actual or potential conflict of interest with any other third party whatsoever, which may arise as a result of the publication of this article. This statement relates to the study, data collection and interpretation, writing and preparation of the article, and the decision to submit the manuscript for publication.